PHILIPP JAUD

Personal Data as an Economic Asset

Internet und Gesellschaft
35

Mohr Siebeck

Internet und Gesellschaft

Schriften des Alexander von Humboldt Institut
für Internet und Gesellschaft

Herausgegeben von

Jeanette Hofmann, Matthias C. Kettemann,
Björn Scheuermann, Thomas Schildhauer
und Wolfgang Schulz

35

Philipp Jaud

Personal Data as an Economic Asset

Compatibility with the EU Charter of Fundamental Rights

Mohr Siebeck

Philipp Jaud, born 1997; law studies at the Universities of Innsbruck (Austria) and Padua (Italy); doctoral scholarship at the University of Innsbruck; 2023 dissertation; associate at a law firm in Innsbruck.

Open access funded by the Fachinformationsdienst (FID) interdisziplinäre Rechtsforschung in Berlin.

ISBN 978-3-16-163406-2 / eISBN 978-3-16-163407-9
DOI 10.1628/978-3-16-163407-9

ISSN 2199-0344 / eISSN 2569-4081 (Internet und Gesellschaft)

The Deutsche Nationalbibliothek lists this publication in the Deutsche Nationalbibliographie; detailed bibliographic data are available at *https://dnb.dnb.de*.

Published by Mohr Siebeck Tübingen, Germany, 2024. www.mohrsiebeck.com

The book was printed on non-aging paper by Laupp & Göbel in Gomaringen and bound by Buchbinderei Nädele in Nehren.

Printed in Germany.

Preface

With profound gratitude, I introduce this book, a synthesis of rigorous research and academic commitment. The aim of this work is to contribute to the ongoing discourse surrounding the intricate relationship between personal data, economic dynamics and fundamental rights.

The motivation behind this exploration stems from a recognition of the evolving role of personal data in our digital landscape. As personal data transforms into a commodity, it becomes crucial to scrutinise the compatibility of these practices with the principles outlined in the EU Charter of Fundamental Rights.

This work seeks to provide insights into the nuanced interplay between the economic value assigned to personal data and the safeguards enshrined in the EU Charter of Fundamental Rights. While not exhaustive, the scope of this exploration covers legal, societal and economical dimensions, acknowledging the multifaceted nature of the subject.

It is crucial to acknowledge the inherent limitations of such an endeavour. The dynamic nature of technology, legal frameworks and societal attitudes implies that this work offers a snapshot rather than a comprehensive map of the entire landscape. As personal data continues to evolve, ongoing discussions and adaptations will be necessary.

I express my deepest appreciation to Mohr Siebeck for providing an invaluable platform to disseminate this research. Their editorial proficiency and research prowess have greatly enhanced the final presentation of this work.

The University of Innsbruck has been a crucial supporter throughout my academic endeavors. The doctoral scholarship from the University's Emerging Scholars Program enabled me to dedicate a focused year to research, laying the groundwork for this book.

Gratitude extends to Prof. Matthias C. Kettemann and Prof. Malte Kramme for their insightful instructions and rigorous examination of my dissertation. Their expertise has been instrumental in shaping the intellectual foundation of this book.

Prof. Bernardo Cortese from the University of Padova deserves acknowledgment for sparking my passion for EU law. His guidance and encouragement have been pivotal in shaping the transnational perspective of this work.

A special note of gratitude is reserved for Prof. Clara Rauchegger. Her unwavering support, mentorship and tireless advocacy for my academic pursuits have played a crucial role in my growth as a legal practitioner. This book stands as a

testament to her commitment to fostering intellectual curiosity and academic excellence.

Finally, heartfelt thanks to my family and my dear Danijela for their unwavering support and understanding throughout this challenging yet rewarding journey. You have been my constant sources of inspiration.

May this book contribute meaningfully to the academic discourse and serve as a valuable resource for those navigating the intricate landscape of personal data, economics and fundamental rights within the EU.

Innsbruck, January 2024 Philipp Jaud

Summary of the contents

Table of contents

Abbreviations

ABGB	Austrian Civil Code
B2C	Business-to-Consumer
BGB	German Civil Code
BGH	German Federal Court of Justice
BVerfG	German Federal Constitutional Court
CAI	Institute of Chartered Accountants of Ireland
CEO	Chief Executive Officer
Charter	Charter of Fundamental Rights of the European Union
CJEU	Court of Justice of the European Union
CVV	Card Verification Value
DCD	Digital Content Directive
DPD	Data Protection Directive
DSB	Austrian Data Protection Authority
DSG	Austrian Data Protection Law
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
ed.	editor
eds.	editors
e.g.	example given
et al.	et alii
etc.	et cetera
EU	European Union
GDPR	General Data Protection Regulation
GPDP	Garante per la protezione dei dati personali
ibid	ibidem
ICO	Information Commissioner's Office
i.e.	id est
IP	Internet Protocol
ODD	Open Data Directive
OECD	Organisation for Economic Co-Operation and Development
OLG	Oberlandesgericht
p.	page
pp.	pages
para.	paragraph
paras.	paragraphs
TEU	Treaty on European Union
TFEU	Treaty on the Functioning of the European Union

URL	Uniform Resource Locator
US	United States
VAT	Value-Added Tax
VFGH	Austrian Constitutional Court
WIFI	Wireless Fidelity
WP29	The Article 29 Data Protection Working Party
WP136	Article 29 Working Party opinion 4/2007 on the concept of personal data, 20 June 2007
WP217	Article 29 Data Protection Working Party opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, 14 November 2014

I. Introduction

1. Aims and objectives

This work primarily examines personal data as an economic asset under EU law. In this regard, personal data as an economic asset is analysed mainly in the light of the Charter[1]. Furthermore, this work seeks to address the question of whether and to what extent the use of personal data as an economic asset can be compatible with the Charter and to what extent personal data can be used as an economic asset at all.

As well as this main aim, this work discusses fundamental questions about personal data as an economic asset. It intends to introduce the concept of personal data as an economic asset. Moreover, the value of personal data and their economic exploitation are explored. The rights to personal data and the allocation of personal data as an economic asset are analysed. EU regulation of personal data as an economic asset is also discussed. This should give a concise analysis of the notion 'personal data as an economic asset'.

Moreover, this work aims to examine the applicability of the Charter to the use of personal data as an economic asset. Facilitations and limits set by the Charter on the use of personal data as an economic asset are outlined.

2. Background

In recent years, the business practice that people do not have to pay a price for digital content or digital services, but rather provide personal data in exchange for digital content or services, has become more and more established. Often content or services are then perceived by users as free. However, they are not free, as companies accumulate large amounts of personal data that are used as an economic asset in return. *Cohen* argues that the purpose of this business practice is

'to produce tractable, predictable citizen-consumers whose preferred modes of self-determination play out along predictable and profit-generating trajectories'.[2]

---

[1] Charter of Fundamental Rights of the European Union [2012] OJ C 326/391.

[2] J.E. Cohen, 'What Privacy Is For', 126 *Harvard Law Review* (2013), p. 1917.

In this regard, *Zuboff* coined the notion of 'surveillance capitalism'.[3]

In order to grant certain rights in these cases to persons who provide personal data in return for digital content or digital services, the DCD[4] was adopted by the EU. The DCD applies not only if the consumer pays a price for the digital content or digital service, but also if the consumer supplies personal data in return.[5] Article 3 (1) DCD states that its provisions apply where 'the consumer pays or undertakes to pay a price' and

> '[…] shall also apply where the trader supplies or undertakes to supply digital content or a digital service to the consumer, and the consumer provides or undertakes to provide personal data to the trader […]'.

It was criticised early in the legislative process of the DCD that personal data was treated as a counterperformance for digital content or services. The EDPS was critical of the treatment of the fundamental right to data protection almost as a mere economic asset.[6] The EDPS even went so far as to compare the market for personal data to the market of organ trafficking.[7] This comparison may seem extreme, but it illustrates the need for academic discussion on this issue. The question to what extent a fundamental right can be 'traded' is of utmost relevancy not only because of the existing business practice of large online companies, but also through Article 3 DCD.

Some aspects of the use of personal data as an economic asset have been addressed in the literature.[8] *Langhanke's* work should be emphasised here as the first German-language monograph on the topic after the adoption of the GDPR[9], in which she outlines approaches for the contractual classification of the phenomenon of 'paying with data'.[10] However, it needs to be further explored to

---

[3] See S. Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (PublicAffairs, 2019).

[4] Directive 2019/770/EU of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services, [2019] OJ L 136/1.

[5] Art 3 (1) Directive 2019/770/EU.

[6] European Data Protection Supervisor, *Opinion 4/2017 of European Data Protection Supervisor on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content*, 14 March 2017.

[7] Ibid, p. 7.

[8] See for example, G. Versaci, 'Personal Data and Contract Law: Challenges and Concerns about the Economic Exploitation of the Right to Data Protection', 14 *European Review of Contact Law* (2018). See also regarding data protection law in general, without reference to the Charter, M. Durovic and M. Montanaro, 'Data Protection and Data Commerce: Friends or Foes?', 17 *European Review of Contract Law* (2021).

[9] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/ 46/ EC (General Data Protection Regulation) [2016] OJ L199/1.

[10] C. Langhanke, *Daten als Leistung – Eine rechtsvergleichende Untersuchung zu Deutschland, Österreich und der Schweiz* (Mohr Siebeck 2018).

what extent the fundamental right to data protection is compatible with transactions of personal data as an economic asset. This question has not been clarified and even in recent literature, for example, 'trading' with personal data is considered to be in conflict with the Charter.[11] Therefore, this work explores the concept of personal data as an economic asset.

The concept of data as economic asset received a lot of scientific attention from the first proposals of the DCD. On the one hand, the focus of the academic discourse in the German-speaking area was and still is on fundamental questions that relate to private autonomy, the relationship between data protection and contract law as well as the civil and contractual classification of data trading.[12] For example, *Sattler* proposes a model that enables the synchronisation of data protection and contract law.[13] However, some fundamental questions on this issue are yet to be explored in detail. In the Anglo-Saxon literature, property rights aspects in particular have been discussed.[14] At EU policy level, the notion of control over personal data was particularly prominent.[15]

On the other hand, less attention was paid to the question of the extent to which the fundamental right to data protection may be used as a mere economic asset. The commercialisation of the fundamental right to data protection, if one compares it with other personality rights, is not excluded per se.[16] But the requirements that must be fulfilled in order to meet the Charter's criteria must be answered in more detail. Therefore, this work seeks to address the question of whether and to what extent the use of personal data as an economic asset can be compatible with the Charter.

Moreover, the core question of the work, to what extent personal data can be used as an economic asset, is particularly topical not only due to the existing business practises of large online companies, but also due to the DCD, which had

---

[11] See B. Custers and G. Malgieri, 'Priceless data: why the EU fundamental right to data protection is at odds with trade in personal data', 45 *Computer Law & Security Review* (2022), pp. 1–11.

[12] See for example, N. Forgò and B. Zöchling-Jud, *Das Vertragsrecht des ABGB auf dem Prüfstand: Überlegungen im digitalen Zeitalter* (MANZ'sche Verlags- und Universitätsbuchhandlung, 2018); A. Metzger, 'A Market Model for Personal Data: State of the Play under the New Directive on Digital Content and Digital Services', in S. Lohsse et al. (eds.), *Data as Counterperformance – Contract Law 2.0?* (Münster Colloquia on EU Law and the Digital Economy V, 2020).

[13] A. Sattler, *Informationelle Privatautonomie – Synchronisierung von Datenschutz- und Vertragsrecht* (Mohr Siebeck, 2022).

[14] See for example, P.M. Schwartz, 'Property, Privacy, and Personal Data', 117 *Harvard Law Review* (2004), pp. 2056–2128; N. Purtova, 'The illusion of personal data as no one's property', 7 *Law, Innovation and Technology* (2015), pp. 40–81.

[15] C. Lazaro and D. Le Métayer, 'Control over Personal Data: True Remedy or Fairy Tale?', 12 *SCRIPTed* (2015), p. 19.

[16] See for example, G. Versaci, 'Personal Data and Contract Law: Challenges and Concerns about the Economic Exploitation of the Right to Data Protection' (*supra* Chapter I. note 8).

to be implemented in national law by the beginning of 2022.[17] As a result, since 1 January 2022, national provisions have been in force in all Member States that deal, inter alia, with personal data in return for digital content and services and their legal consequences. Fundamental rights aspects of this issue have not been sufficiently considered in the scientific literature so far.

This work deals with the above-mentioned questions in order to contribute to the legal discussion and development of the concept 'data as an economic asset' and its compatibility with the Charter.

3. Methodology

This work relies on doctrinal analysis, the traditional method of legal research.[18] It aims to systematise and rationalise the legal rules, principles, standards and procedures that apply to personal data as an economic asset. For this purpose, EU primary law is examined, with particular focus on the Charter. This is done by using the interpretation methods of grammatical, historical, systematic and teleological interpretation, with particular emphasis on the latter.

To answer the research questions, the Charter, as a primary source, is of particular importance. In addition, several instruments of EU secondary law – such as the GDPR and DCD – are analysed insofar as they are relevant for personal data as an economic asset. The case law of the CJEU guides the interpretation of these sources of primary and secondary EU law.

Economic perspectives are also applied to discuss the value of personal data. Different methods, including empirical studies, are presented to assess the value of personal data. How companies use, share and value personal data in the data-driven economy is illustrated with real-life examples. Contract law considerations concerning personal data as an economic asset would go beyond the scope of this work and are therefore not addressed.

4. Structure

Following this introductory chapter, Chapter II. explores the definition of personal data. The concept of personal data is often taken for granted. However, the answer to the question of what exactly is meant by personal data is of fundamental importance for the analysis that is conducted in the subsequent chapters. A clear understanding of the term 'personal data' is obtained here by examining the meaning of 'personal data' in the GDPR and by analysing the relevant case law of the CJEU.

---

[17] See Article 24 DCD.

[18] See for an outline of legal research methodology: L. Cahillane and J. Schweppe (eds.), *Legal Research Methods: Principles and Practicalities* (Clarus Press, 2016).

Chapter III. examines the value of personal data. The term 'economic asset' suggests that data is ascribed a certain material value. In view of the numerous tech companies that generate their revenue from personal data, this value should not be underestimated. Different methods are presented and applied to assess how personal data are used, shared and valued. It will be shown that personal data, such as names, addresses, age, have a monetary value.

After establishing the concept of 'personal data as an economic asset', Chapter IV. aims to examine how and by whom personal data can be used as an economic asset. Different approaches on how rights to personal data may be designed are critically appraised. Emphasis is placed on EU data protection law. It will be argued that EU data protection law gives data subjects numerous rights, allowing them to control and dispose of their personal data.

Chapter V. provides an overview of EU instruments that deal with the data economy and data as an economic asset. The chapter gives an overview of EU legal instruments regarding data, with particular focus on the DCD. It is argued that the EU recognises that (personal) data can be an economic asset.

Before this work turns to the question of whether and, if so, under which conditions the concept of personal data as an economic asset is compatible with the Charter, it is necessary to clarify under what circumstances the Charter is applicable to personal data as an economic asset. To establish this fundamental premise, Chapter VI. examines the EU and its Member States as Addressees of the Charter. The Chapter then turns to horizontal effect of the Charter. It will be shown when the Charter can be applied in the context of personal data as an economic asset.

Article 8 of the Charter establishes an autonomous fundamental right to data protection and therefore merits a detailed analysis in the context of personal data as an economic asset. Thus, the scope of application and protection of Article 8 of the Charter are described in Chapter VII. This is followed by an examination of the requirements of lawful data processing and thus the use of personal data as an economic asset. It will be established that the economic use of personal data is not per se incompatible with Article 8 of the Charter.

As the fundamental right to data protection is not limitless, Chapter VIII. discusses the limitations of this right. Special consideration is given to Article 52 of the Charter, which provides conditions for limitations of rights of the Charter. The conditions under which the use of personal data as an economic asset meets the criteria of Article 52 of the Charter are examined. Then, fundamental rights and interests in the use of personal data as an economic asset, which can limit the fundamental right to data protection, are outlined.

Chapter IX. summarises the main findings of the work.

II. Definition of personal data

The aim of this chapter is to define personal data. This definition is necessary in order to be able to examine the notion of personal data as an economic asset in subsequent chapters. The definition of personal data serves to delineate which information falls within the scope of personal data and which information does not.[1] The GDPR, which has been comprehensively governing the data protection regime of the EU since May 2018, is of considerable significance in this regard. The GDPR is relevant not only because of its extensive regulatory scope, but also because it contains a legal definition of personal data.

The definition of personal data in the GDPR includes four key elements. While these four building blocks are tightly interconnected and build on one another,[2] they will be analysed individually for the purpose of this chapter. Section 1 below reflects the legal definition of the GDPR and the Opinion of the WP29. Section 2 examines the first element of the definition ('any information') and Section 3 the second one ('relating to'). Section 4 looks at the third element ('an identified or identifiable'), while Section 5 turns to the fourth one ('natural person'). On the basis of these four components, a clear understanding of the term 'personal data' is obtained by examining the meaning of 'personal data' in the GDPR and by analysing the relevant case law of the CJEU.

1. Legal definition and WP29 Opinion

Article 4 (1) GDPR defines personal data as follows:

'Personal data means 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, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;'[3]

---

[1] C. Bergauer, 'Art 4 Z 1 personenbezogene Daten' in D. Jahnel (ed.), *DSGVO Datenschutz-Grundverordnung* (Jan Sramek Verlag, 2021), para. 5; D. Jahnel and C. Bergauer, *Teil-Kommentar zur DS-GVO* (Jan Sramek Verlag, 2018), p. 25.

[2] Article 29 Working Party opinion 4/2007 on the concept of personal data, 20 June 2007 ('WP136'), p. 6.

[3] See Article 4 (1) GDPR.

It is already evident from the first reading of this definition that personal data is defined broadly and comprehensively.[4] The definition closely follows that of the DPD[5]:[6]

'personal data shall mean any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;'[7]

The DPD was replaced by the GDPR. The European Commission's adjusted proposal of the DPD stated that

'the amended proposal meets Parliament's wish that the definition of "personal data" should be as general as possible, so as to include all information concerning an identifiable individual'.[8]

This wish was also considered by the Council.[9]

According to Article 1 (1) GDPR, it is one of the objectives of the GDPR to protect the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.[10] With this purpose in mind, it seems clear why the European lawmaker has adopted such a broad definition of personal data.[11] The concept of personal data is intended to ensure individuals the utmost protection of their rights.

The WP29 adopted a similarly broad definition. The WP29 was an autonomous European working party which has addressed issues regarding the protection of privacy and personal data until 25 May 2018 (the entry into force of the GDPR).[12] Although the WP29 was replaced by the EDPB, its opinions are still

---

[4] A. Klabunde, 'Art. 4 Begriffsbestimmungen' in E. Ehmann and M. Selmayr (eds.), *DS-GVO Datenschutz-Grundverordnung* (2nd edition, C.H. Beck, 2018), para. 7; F. Costa-Cabral and O. Lynskey, 'Family ties: The intersection between data protection and competition in EU law', 54 *Common Market Law Review* (2017), p. 16; F. Costa-Cabral and O. Lynskey, 'The Internal and External Constraints of Data Protection on Competition Law in the EU', *LSE Law, Society and Economy Working Papers* (2015), p. 5; see also, Case C-434/16 *Nowak,* EU:C:2017:994, para. 34.

[5] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31.

[6] A. Klabunde, 'Art. 4 Begriffsbestimmungen' (*supra* Chapter II. note 4), para. 8.

[7] See Article 2 (a) DPD; A. Klabunde, 'Art. 4 Begriffsbestimmungen' (*supra* Chapter II. note 4), para. 8.

[8] Amended proposal for a Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data, COM (92) 422 final, p. 9.

[9] Common position (EC) No 1/95, adopted by the Council on 20 February 1995, OJ NO C 93 of 13.4.1995, p. 20.

[10] See Article 1 (1) GDPR.

[11] This broad definition also corresponds to the view repeatedly expressed by the CJEU, e.g. Case C-434/16 *Nowak* (*supra* Chapter II. note 4), para. 33.

[12] See European Data Protection Board, *Article 29 Working Party,* https://edpb.europa.eu/our-work-tools/article-29-working-party_en (accessed 31 January 2024).

considered of importance. The EDPB has endorsed the WP29 guidelines concerning the GDPR.[13] Moreover, the European Commission still references the WP29 opinions on its homepage.[14]

One of these referenced documents is the WP136. Although it is not legally binding, the WP136 has undoubted significance and offers detailed guidelines on how the concept of personal data should be interpreted.[15] While this opinion was issued on the DPD, it is still relevant today since, as stated above, the GDPR closely follows the DPD. This view was also expressed by Advocate General *Kokott* in her opinion on the *Nowak* case.[16]

The WP136 provides a broad definition of personal data, emphasising the fact that this definition should not be overinterpreted but that the understanding of the concept of personal data should also not be unduly limited.[17] The WP136 divides the definition of personal data into four key elements.[18] The structure of this chapter reflects this approach.

2. 'Any information'

The phrase 'any information' in Article 4 (1) GDPR is very general and suggests a broad interpretation.[19] The WP136 notes that the phrase 'any information' in the GDPR indicates the legislator's eagerness to develop a wide definition of personal data.[20] It is worth noting that information, not data, is mentioned and no distinguishing features are specified.[21] The insufficient differentiation between

---

[13] See European Data Protection Board, *Endorsement of GDPR WP29 guidelines by the EDPB,* 25 May 2018, https://edpb.europa.eu/news/news/2018/endorsement-gdpr-wp29-guidelines-edpb_de (accessed 31 January 2024).

[14] See for example, European Commission, *What is personal data?,* https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en (accessed 31 January 2024), which references the WP29 opinion 4/2007 on the concept of personal data.

[15] N. Purtova, 'The law of everything. Broad concept of personal data and future of EU data protection law', 10 *Law, Innovation and Technology* (2018), p. 43.

[16] Opinion of Advocate General Kokott in Case C-434/16 *Nowak*, EU:C:2017:582, para. 3.

[17] WP136 (*supra* Chapter II. note 2), p. 5.

[18] Ibid, p. 6.

[19] C. Bergauer, 'Begriff und Kategorien' in R. Knyrim (ed.), *Datenschutz-Grundverordnung* (Manz, 2016), p, 50; D. Jahnel and C. Bergauer, *Teil-Kommentar zur DS-GVO* (*supra* Chapter II. note 1), p. 26; C. Bergauer, 'Art 4 Z 1 personenbezogene Daten' (*supra* Chapter II. note 1), para. 9.

[20] WP136 (*supra* Chapter II. note 2), p. 6.

[21] M. Finck and F. Pallas, 'They who must not be identified – distinguishing personal from non-personal data under the GDPR', 10 *International Data Privacy Law* (2020), p. 13; N. Purtova, 'The law of everything. Broad concept of personal data and future of EU data protection law' (*supra* Chapter II. note 15), p. 49; L. A. Bygrave, 'Information Concepts in Law: Generic Dreams and Definitional Daylight', 35 *Oxford Journal of Legal Studies* (2015),

data and information, given that data does not necessarily equal information, can be viewed critically.[22] However, a further discussion of the differences between the two concepts would go beyond the scope of this work.

The nature of the information can be both objective and subjective to be considered 'personal data' under Article 4 (1) GDPR.[23] Therefore, not only objective facts, such as a person's age, are included, but also subjective opinions on the consumer behaviour of an individual.[24] Moreover, it does not matter whether the information is true or false, accurate or inaccurate, for it to be considered 'personal data'.[25]

There are no specific criteria regarding the content of the information. The definition of 'personal data' contains both information relating to the private and family life on an individual and information relating to any type of public behaviour by the individual,[26] such as employment affairs or the political or leisure activities of the individual.[27] The GDPR itself mentions data processing in the context of employment[28] and data revealing political beliefs.[29] The CJEU also ruled in the *Lindqvist* case that working conditions and hobbies are included in the term 'personal data'.[30] The fact that the concept of 'personal data' includes not only data concerning private and family life is also in line with the Charter since the protection of personal data is specifically enshrined in Article 8 of the Charter and this is independent of Article 7, which protects private and family life.[31]

The format or medium on which the information is held is not relevant according to the WP29, which cites alphabetic, numeric, graphic, photographic and audio information as examples.[32] For example, an email or a drawing of a child

---

p. 96; C. Bergauer, 'Begriff und Kategorien' (*supra* Chapter II. note 19), p. 43; W. Ziebarth, 'Artikel 4 Begriffsbestimmungen' in G. Sydow (ed.), *Europäische Datenschutzgrundverordnung* (2nd edition, Nomos Verlag, 2018), para. 8; C. Bergauer, 'Art 4 Z 1 personenbezogene Daten' (*supra* Chapter II. note 1), para. 9.

[22] See already on the DPD, M. Albers, *Informationelle Selbstbestimmung* (Nomos Verlag, 2005), p. 318.

[23] WP136 (*supra* Chapter II. note 2), p. 6.

[24] A. Klabunde, 'Art. 4 Begriffsbestimmungen' (*supra* Chapter II. note 4), para. 9; C. Bergauer, 'Begriff und Kategorien' (*supra* Chapter II. note 19), p. 51.

[25] WP136 (*supra* Chapter II. note 2), p. 6; D. Jahnel and C. Bergauer, *Teil-Kommentar zur DS-GVO* (*supra* Chapter II. note 1), p. 27.

[26] See Case C-465/00 *Österreichischer Rundfunk*, EU:C:2003:294, paras. 73, 74; Case C-615/13 P *ClientEarth*, EU:C:2015:489, para. 30; European Union Agency for Fundamental Rights and Council of Europe, *Handbook on European data protection law*, (Publications Office of the European Union, 2018), p. 86.

[27] WP136 (*supra* Chapter II. note 2), p. 6.

[28] See Article 88 GDPR.

[29] See Article 9 (1) GDPR.

[30] Case C-101/01 *Lindqvist*, EU:C:2003:596, para. 24.

[31] See Articles 7 and 8 of the Charter.

[32] See WP136 (*supra* Chapter II. note 2), p. 8; A. Klabunde, 'Art. 4 Begriffsbestimmun-

can contain personal data.[33] Furthermore, the CJEU has already ruled in several cases that images taken of a person with a camera are to be understood as personal data.[34]

The CJEU clarified the meaning of 'any information' in the *Nowak* case. Mr. Nowak was a trainee accountant and had failed a CAI exam for the fourth time when he requested to see his exam paper.[35] However, CAI refused to release his exam paper to him on the grounds that it did not contain any personal data.[36] Mr. Nowak then turned to the Data Protection Commissioner, who also informed him that an examination script was not personal data and that it was a vexatious complaint.[37] Mr. Nowak went through the entire process of appeal until finally the Irish Supreme Court had doubts as to whether an examination paper falls under the term 'personal data' and thereupon referred this question, among others, to the CJEU for a preliminary ruling.

The CJEU found that:

> 'The use of the expression "any information" in the definition of the concept of "personal data" […] reflects the aim of the EU legislature to assign a wide scope to that concept, which is not restricted to information that is sensitive or private, but potentially encompasses all kinds of information, not only objective but also subjective, in the form of opinions and assessments […].'[38]

This interpretation is consistent with the broad approach in the WP136 that any information can be personal data, irrespective of its nature or content.[39] Following this wide-ranging interpretation, the CJEU ruled that an examinee's written answers in a job-related examination and any comments the examiner may make on those answers are 'personal data'. However, the examination questions do not constitute personal data of the examinee.[40] A more detailed analysis of the *Nowak* case will be conducted in Section 3. b) below, which focuses on the second element of the definition of personal data ('relating to').

---

gen' (*supra* Chapter II. note 4), para. 9; C. Bergauer, 'Begriff und Kategorien' (*supra* Chapter II. note 19), p. 50; D. Jahnel and C. Bergauer, *Teil-Kommentar zur DS-GVO* (*supra* Chapter II. note 1), p. 27; W. Ziebarth, 'Artikel 4 Begriffsbestimmungen' (*supra* Chapter II. note 21), para. 8; C. Bergauer, 'Art 4 Z 1 personenbezogene Daten' (*supra* Chapter II. note 1), para. 11.

[33] WP136 (*supra* Chapter II. note 2), p. 8.

[34] See for example, Case C–212/13 *Ryneš*, EU:C:2014:2428, para. 22; Case C-345/17 *Buivids*, EU:C:2019:122, para. 31.

[35] Case C-434/16 *Nowak* (*supra* Chapter II. note 4), para. 19.

[36] Ibid, para. 20.

[37] Ibid, para. 23.

[38] Ibid, para. 34.

[39] N. Purtova, 'The law of everything. Broad concept of personal data and future of EU data protection law' (*supra* Chapter II. note 15), p. 66.

[40] Case C-434/16 *Nowak* (*supra* Chapter II. note 4), para. 58.

3. 'Relating to'

The second element of the definition of personal data in Article 4 (1) GDPR is that it 'relates to' a natural person. The WP29 states that this key element of the concept of personal data is essential, as it is crucial to figure out exactly which connections matter and how to differentiate them.[41] Fundamentally, information 'relates to' a person if it is 'about' that person.[42] When examining this element, all the specifics of the case need to be considered.[43]

The connection can be quickly established in many circumstances. For example, a name and surname[44] and an address[45] are evidently 'related to' an individual. However, the WP136 refers to a number of other situations in which it is not as apparent as in the examples mentioned above to determine that information 'relates to' a person. In some constellations, the data primarily relate to objects and not to individuals, but since these objects normally belong to an individual, one can indirectly draw conclusions about the person behind the object by analysing the information about the object. For example, at first glance, the value of a house may seem to merely 'relate to' an object, but it could be used to infer the real estate tax liability of the owner.[46] Another example is the inspection of a car in a garage, where data about the car, mileage, registration and any damage are collected, which can then be linked to the owner of the car.[47] In these situations, an indirect connection between individuals owning or otherwise interacting with objects can be established and seemingly the WP29 finds this indirect relationship to be sufficient.[48]

Information can 'relate to' an individual in 'content', 'purpose' or 'result', which means that information 'relating to' a natural person contains but is larger than information 'about' that person.[49] In situations where information is provided 'about' an individual, irrespective of its intention or the effect it has on the individual, the 'content' element is involved.[50] For example, the criminal record

---

[41] WP136 (*supra* Chapter II. note 2), p. 9.

[42] Ibid.

[43] Ibid, p. 10.

[44] See Case C-101/01 *Lindqvist* (*supra* Chapter II. note 30), para. 24; Case C-73/07 *Satakunnan Markkinapörssi und Satamedia*, EU:C:2008:727, para. 35; Case C-28/08 P *Bavarian Lager*, EU:C:2010:378, para. 68.

[45] See Case C-553/07 *Rijkeboer*, EU:C:2009:293, para. 42.

[46] WP136 (*supra* Chapter II. note 2), p. 9; A. Klabunde, 'Art. 4 Begriffsbestimmungen' (*supra* Chapter II. note 4), para. 10.

[47] WP136 (*supra* Chapter II. note 2), p. 10.

[48] N. Purtova, 'The law of everything. Broad concept of personal data and future of EU data protection law' (*supra* Chapter II. note 15), p. 54.

[49] WP136 (*supra* Chapter II. note 2), p. 10; N. Purtova, 'The law of everything. Broad concept of personal data and future of EU data protection law' (*supra* Chapter II. note 15), p. 54; A. Klabunde, 'Art. 4 Begriffsbestimmungen' (*supra* Chapter II. note 4), para. 10.

[50] WP136 (*supra* Chapter II. note 2), p. 10.

of an individual certainly 'relates to' that person. Furthermore, an entry into a register of foreign nationals,[51] the communication of an individual's income to a third party[52] and tax information[53] 'relate to a person' and constitute personal data.

Nonetheless, information can also 'relate to' a person when it is not about that person. This so-called 'purpose' aspect can occur if the data are used or might be used for the purpose of determining, discussing or affecting the status or actions of a person.[54] The WP136 gives the example of a call log of a telephone inside a company office which provides information about the calls that have been made from that telephone connected to a certain line and can consequently, for different purposes, be related to the company, the employee or the cleaning staff.[55] Another example is the data contained in the record of working time, including the daily work periods and rest periods.[56]

Even without a 'content' or 'purpose' element, information may 'relate to' a person, as its processing may 'result' in having an impact on the rights and interests of that person.[57] The WP136 states that the probable result does not have to affect the individual significantly.[58] This means that the information also 'relates to' a person if the result may have a minimal impact on that person.[59] It is already sufficient if the person is treated differently than other persons due to the result of this data and information processing.[60] The WP136 illustrates this 'result' element by describing a satellite location system set up by a taxi service. This system makes it possible to assess the location of available taxis in real time and thereby enables the tracking of taxi drivers and can have a direct effect on these persons and, as such, the data may also 'relate to' natural persons.[61]

It is clear from the above that the WP29 also interprets the term 'relating to' broadly. This becomes all the more evident when one considers that the elements 'content', 'purpose', 'result' are not to be interpreted cumulatively, but alternatively.[62] Limiting the interpretation of 'relating to' to information 'about' an individual would serve little purpose, as it is not clear why protection should be

---

[51] See Case C-524/06 *Huber*, EU:C:2008:724, para. 43.

[52] See Case C-465/00 *Österreichischer Rundfunk* (*supra* Chapter II. note 26), paras. 73, 74.

[53] See Case C-201/14 *Bara*, EU:C:2015:638, para. 29.

[54] WP136 (*supra* Chapter II. note 2), p. 10; A. Klabunde, 'Art. 4 Begriffsbestimmungen' (*supra* Chapter II. note 4), para. 10.

[55] WP136 (*supra* Chapter II. note 2), p. 10.

[56] See Case C-342/12 *Worten*, EU:C:2013:355, para. 19.

[57] WP136 (*supra* Chapter II. note 2), p. 10; A. Klabunde, 'Art. 4 Begriffsbestimmungen' (*supra* Chapter II. note 4), para. 10.

[58] WP136 (*supra* Chapter II. note 2), p. 10.

[59] N. Purtova, 'The law of everything. Broad concept of personal data and future of EU data protection law' (*supra* Chapter II. note 15), p. 54.

[60] WP136 (*supra* Chapter II. note 2), p. 11.

[61] Ibid.

[62] Ibid.

triggered by the processing of information 'about' an individual but not when the information is processed with the aim of affecting or judging an individual.[63] Furthermore, *Purtova* points out that, as the world becomes more digital and connected through technology, almost any information can be used to learn something about a person or it can impact a person.[64] In my opinion, this very fact speaks in favour of a broad interpretation of 'relating to'. Everyday life is shaped by digital technologies, whether at work or in our leisure time. Almost everywhere, information is processed that is related to one's own person. It is therefore important that information which only on closer inspection shows a relation to a person is also covered by the definition of personal data. As a result, the respective data protection regulations are applicable and the processing of the information occurs according to specified rules. This broad interpretation covers borderline cases and thus sufficiently protects fundamental rights. And this is, after all, one of the main objectives of the GDPR and privacy laws.

a) YS case

The CJEU shed light on the concept of 'personal data' and in particular the element 'relating to' in the *YS* case.[65] The CJEU's decision stems from the applications of various third-country nationals who had applied for a temporary residence permit in the Netherlands. These applications were rejected in one case[66] and granted in two others,[67] but without further justification. In all cases, the parties, based on the right to information under data protection law, requested that the so-called 'minute' (draft notice) be sent to them, but this was refused.[68] The caseworker responsible for processing an application for a residence permit prepares a draft decision, which is submitted to a senior caseworker of that service for evaluation.[69] The caseworker attaches a document explaining to the senior caseworker the reasons on which his or her draft decision is based (the minute).[70] The minute is part of the preliminary process at that authority, but not the final decision.[71] The minute generally contains, among other things, information about the applicant such as name, date of birth, nationality, religion and language.[72] In addition, the minute contains an evaluation of the information in

[63] N. Purtova, 'The law of everything. Broad concept of personal data and future of EU data protection law' (*supra* Chapter II. note 15), p. 79.
[64] Ibid, p. 56.
[65] Case C-141/12 *YS*, EU:C:2014:2081.
[66] Ibid, para. 18.
[67] Ibid, paras. 23 and 27.
[68] Ibid, paras. 20, 25 and 28.
[69] Ibid, para. 13.
[70] Ibid.
[71] Ibid.
[72] Ibid, para. 14.

view of the applicable legal provisions, which is referred to as a 'legal analysis'.[73] The question of whether the legal analysis contained in the minute constitutes personal data was referred to the CJEU for a preliminary ruling.

The CJEU first clarified that the data relating to the respective applicants contained in the legal analysis, such as their names, are personal data.[74] However, it was disputed how to deal with the remaining part of the legal analysis. There were essentially three positions on this matter. According to the broad interpretation, the entire legal analysis should fall under the concept of personal data insofar as it relates to a specific natural person.[75] According to a mediating view, a distinction should be made according to the extent to which the legal analysis is based on specific information about a particular person, since 'only an abstract legal interpretation' should not be included under the term 'personal data'.[76] Pursuant to the restrictive view, the legal analysis *per se* should not fall under the concept of personal data.[77]

The CJEU adopted a rather restrictive view. Although the data contained in the legal analysis about the person applying for a residence permit, such as the name, are personal data,[78] this classification does not apply to the analysis as such[79]. The CJEU justified this decision by stating that the right to information under EU data protection law in particular is intended to give data subjects the opportunity to ascertain whether their personal data is being processed correctly and in a permissible manner.[80] If this right to access would be extended to the entire legal analysis, this would no longer be compatible with the objective of protecting the privacy of the data subject.[81]

Thus, the CJEU did not follow the broad interpretation of the WP129 in the *YS* case. It did not define the term 'personal data' in isolation, but rather functionally with regard to the resulting rights. In addition to information directly relating to a person (e.g. name, age, nationality, etc.), the actual circumstance (e.g. the denial of a residence permit) can also constitute personal data, as it describes personal or factual circumstances relating to a specific person. This means that a differently weighted interpretation of the concept of 'personal data' remains possible in a distinct constellation. This is precisely what happened as the CJEU interpreted the building block 'relating to' broadly in the *Nowak* case.[82]

---

[73] Ibid.
[74] Ibid, para. 38.
[75] Ibid, para. 35.
[76] Ibid.
[77] Ibid, para. 36.
[78] Ibid, para. 38.
[79] Ibid, para. 39.
[80] Ibid, para. 44.
[81] Ibid, para. 46.
[82] See Subsection II.2. for a description of the dispute in the main proceedings.

b) Nowak case

As noted above, the CJEU emphasised in the *Nowak* case that the term 'personal data' was not limited to sensitive or private information, but potentially encompasses all types of information, both objective and subjective, in the form of opinions or assessments, provided that it is information 'relating to' the individual at issue.[83] The latter condition is fulfilled if the information is linked to a specific person due to its content, purpose or effects.[84] The written answers of an examinee in a job-related examination represent such information that is linked to his person.[85] Indeed, the content of these answers reflects the examinee's level of knowledge and competence in a particular area, as well as his thought process, judgment and critical thinking.[86] Furthermore, the collection of these answers is aimed at assessing the professional skills of the examinee and his suitability to perform the profession in question.[87] Finally, the use of that information, reflected in particular in the success or failure of the examinee in the examination at issue, may affect his rights and interest to the extent that it may determine or influence his chances of entering the desired profession or obtaining the desired employment.[88]

As for the examiner's comments on the examinee's answers, the CJEU notes that, just like the candidates answers in the exam, they represent information relating to the examinee.[89] Thus, the content of the notes expresses the examiner's assessment of the examinee's individual performance in the examination and, in particular, of the examinee's knowledge and competence in the field in question.[90]

The CJEU interprets the term 'relating to' almost identically to the WP136, which mentions the alternative conditions of content, purpose and result. The CJEU chooses the wording content, purpose or effect.[91] The answers and comments are information about the candidate. The purpose is to assess the professional skills and as a result they may impact the examinee's professional career.[92] The CJEU justifies this, inter alia, by stating that written answers given by the candidate in a professional examination and any comments made on them by the

---

[83] Case C-434/16 *Nowak* (*supra* Chapter II. note 4), para. 34; see also Case C-487/21 *Österreichische Datenschutzbehörde*, EU:C:2023:369, para. 23.

[84] Case C-434/16 *Nowak* (*supra* Chapter II. note 4), para. 35; see also Case C-487/21 *Österreichische Datenschutzbehörde* (*supra* Chapter II. note 83), para. 24.

[85] Case C-434/16 *Nowak* (*supra* Chapter II. note 4), para. 36.

[86] Ibid, para. 37.

[87] Ibid, para. 38.

[88] Ibid, para. 39.

[89] Ibid, para. 42.

[90] Ibid, para. 43.

[91] Ibid, para. 44.

[92] N. Purtova, 'The law of everything. Broad concept of personal data and future of EU data protection law' (*supra* Chapter II. note 15), p. 71.

examiner are open to review and may be corrected or deleted and that this serves the purpose of guaranteeing the protection of the right to privacy of the examinee.[93] Here, too, the CJEU takes the circumstances of the case into account. In contrast to the *YS* case, this broad interpretation is understood to be in line with the objective of securing the right to privacy.[94] Since the *Nowak* ruling was issued more recently, one may argue that it acts as an adjustment in favor of a broader interpretation of the term 'relating to'.

4. 'Identified or identifiable'

The third element of the definition of personal data according to the GDPR is that information must relate to a natural person who is 'identified or identifiable'.[95] A person is 'identified' if he or she can be distinguished from other people in a group, and he or she is 'identifiable' if he or she has not yet been identified, but it would be possible to do so.[96] This definition seems very broad, especially as it would appear possible with modern technologies to be able to identify any person.[97]

In order to be able to identify persons, so-called 'identifiers' are used. These are pieces of information that are characteristic of a specific person, such as name, address, fingerprints, etc.[98] The GDPR itself gives examples of possible identifiers in Article 4 (1):

'[…] an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;'[99]

This definition, in contrast to the one given by the DPD, includes genetic identifiers and thus responds to technological development.[100]

---

[93] Case C-434/16 *Nowak* (*supra* Chapter II. note 4), para. 56.

[94] The CJEU explicitly addresses this contrast with the *YS* case in paragraph 56 of the *Nowak* judgment.

[95] Article 4 (1) GDPR.

[96] WP136 (*supra* Chapter II. note 2), p. 12; European Union Agency for Fundamental Rights and Council of Europe, *Handbook on European data protection law* (*supra* Chapter II. note 26), p. 89.

[97] See P. M. Schwartz and D. J. Solove, 'The PII Problem: Privacy and a New Concept of Personally Identifiable Information', 86 *New York University Law Review* (2011), p. 1875; P. M. Schwartz and D. J. Solove, 'Reconciling Personal Information in the United States and European Union', 102 *California Law Review* (2014), p. 892, who argue that the EU's approach is more in line with technology than the United States' approach.

[98] WP136 (*supra* Chapter II. note 2), p. 12.

[99] See Article 4 (1) GDPR.

[100] W. G. Voss and K. A. Houser, 'Personal Data and the GDPR: Providing a Competitive Advantage for U.S. Companies', 56 *American Business Law Journal* (2019), p. 315; A. Klabunde, 'Art. 4 Begriffsbestimmungen' (*supra* Chapter II. note 4), para. 15.

Usually, people are identified or identifiable directly by their names,[101] although occasionally additional information is needed to avoid confusion.[102] Common or homonymous names require additional identifiers to uniquely individualise a person.[103] For example, many people have the first name Joe. But if one combines this first name with additional information like a last name or an address, one may identify a specific person. In this way, it is also possible to identify people indirectly.[104] Even if a person is initially considered unidentifiable, he or she may still be identifiable if additional information is obtained.[105] This principle is also supported by the GDPR, as it stipulates that individuals can be identified with 'one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person'.[106] It is not necessary to learn a person's name in order to identify them.[107] A passport number or license plate may be sufficient for this purpose.[108] The CJEU ruled in this sense in the *Lindqvist* case where it found that

'referring, on an internet page, to various persons and identifying them by name or by other means, for instance by giving their telephone number or information regarding their working conditions and hobbies, constitutes the processing of personal data […]'.[109]

Recital 26 of the GDPR provides guidance on whether or not individuals are identifiable. It reads that

'to determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly.'[110]

---

[101] European Union Agency for Fundamental Rights and Council of Europe, *Handbook on European data protection law* (*supra* Chapter II. note 26), p. 89.

[102] WP136 (*supra* Chapter II. note 2), p. 13; European Union Agency for Fundamental Rights and Council of Europe, *Handbook on European data protection law* (*supra* Chapter II. note 26), p. 90.

[103] C. Bergauer, 'Begriff und Kategorien' (*supra* Chapter II. note 19), p. 53; D. Jahnel and C. Bergauer, *Teil-Kommentar zur DS-GVO* (*supra* Chapter II. note 1), p. 28; W. Ziebarth, 'Artikel 4 Begriffsbestimmungen' (*supra* Chapter II. note 21), para. 14; C. Bergauer, 'Art 4 Z 1 personenbezogene Daten' (*supra* Chapter II. note 1), para. 15.

[104] WP136 (*supra* Chapter II. note 2), p. 13.

[105] Ibid; D. Jahnel and C. Bergauer, *Teil-Kommentar zur DS-GVO* (*supra* Chapter II. note 1), pp. 26 and 29; W. Ziebarth, 'Artikel 4 Begriffsbestimmungen' (*supra* Chapter II. note 21), para. 17; C. Bergauer, 'Art 4 Z 1 personenbezogene Daten' (*supra* Chapter II. note 1), para. 19.

[106] See Article 4 (1) GDPR.

[107] WP136 (*supra* Chapter II. note 2), p. 14.

[108] European Union Agency for Fundamental Rights and Council of Europe, *Handbook on European data protection law* (*supra* Chapter II. note 26), p. 89; W. Ziebarth, 'Artikel 4 Begriffsbestimmungen' (*supra* Chapter II. note 21), para. 18.

[109] Case C-101/101 *Lindqvist,* para. 27.

[110] See Recital 26 GDPR.

Since both data controllers and other persons are mentioned here, significantly more constellations fall under the concept of personal data compared to if only data controllers were considered.[111]

The WP136 specifies that a simple hypothetical probability of identifying an individual is not sufficient to regard the individual as 'identifiable'.[112] The criteria of 'all means reasonably likely to be used' should take into consideration aspects such as the cost of identification, the likelihood of operational instability and technological errors, the state of the art in technology and the purpose.[113] To illustrate the last factor, the WP136 mentions video surveillance. Since the purpose of video surveillance is to identify persons, who are seen in video images, the entire video footage as such must be assumed to be processing the data of identifiable persons.[114] In cases where identification is not the purpose of data processing, technical and organisational measures that prevent data from being decrypted can ensure that individuals are not identifiable.[115]

a) Pseudonymised and anonymised data

In this context, the phenomenon of pseudonymisation has a significant role. The GDPR defines pseudonymisation as

'the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;'[116]

The purpose of pseudonymisation is to be able to gather data linked to a person without having to know his or her identity.[117] Pseudonymisation is a suitable technical and organisational measure for implementing data protection principles such as data minimisation.[118] Key-coded data is an example of pseudonymisation, where information relating to an individual is marked with a code and

---

[111] N. Purtova, 'The law of everything. Broad concept of personal data and future of EU data protection law' (*supra* Chapter II. note 15), p. 46; M. Finck and F. Pallas, 'They who must not be identified – distinguishing personal from non-personal data under the GDPR' (*supra* Chapter II. note 21), p. 16.

[112] WP136 (*supra* Chapter II. note 2), p. 15.

[113] Ibid; D. Jahnel and C. Bergauer, *Teil-Kommentar zur DS-GVO* (*supra* Chapter II. note 1), p. 31; P.M. Schwartz and D.J. Solove welcome this 'dynamic' interpretation, see Schwartz and Solove, 'Reconciling Personal Information in the United States and European Union' (*supra* Chapter II. note 97), p. 892.

[114] WP136 (*supra* Chapter II. note 2), p. 16.

[115] Ibid, p. 17.

[116] See Article 4 (5) GDPR.

[117] WP136 (*supra* Chapter II. note 2), p. 18.

[118] See Article 25 (1) GDPR.

the key that provides the link between the code and the individual's identifiers is stored separately.[119] Here, too, additional information can lead to the fact that personal data is being processed.[120] Recital 26 of the GDPR states that

'personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person.'[121]

In fact, pseudonymisation means that data can be traced back to a person so that his or her identity is uncovered, although this only happens under certain scenarios.[122]

In contrast, anonymous data is not covered by the concept of personal data. Recital 26 of the GDPR describes anonymous data as

'information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or longer identifiable.'[123]

Anonymous data therefore includes information that originally allowed the identification of a natural person, but for various reasons no longer enables to identify a person.[124] Identification must permanently be averted.[125] Therefore, there may also be no copy of the original data set.[126] Here, too, the WP136 emphasises that the question of whether or not data is anonymous has to be assessed according to the specific circumstances and that a case-by-case approach is necessary.[127]

Based on the above, it is clear that the element 'identified or identifiable' is also understood very broadly. Pseudonymised data are considered personal data, and rightly so. This building block illustrates that it is not possible to say in general terms whether a person is identified or identifiable. On the basis of the intercon-

---

[119] WP136 (*supra* Chapter II. note 2), p. 18; C. Bergauer, 'Begriff und Kategorien' (*supra* Chapter II. note 19), p. 54.

[120] M. Finck and F. Pallas, 'They who must not be identified – distinguishing personal from non-personal data under the GDPR' (*supra* Chapter II. note 21), p. 21.

[121] See Recital 26 GDPR.

[122] WP136 (*supra* Chapter II. note 2), p. 18; A. Klabunde, 'Art. 4 Begriffsbestimmungen' (*supra* Chapter II. note 4), para. 29.

[123] See Recital 26 GDPR.

[124] A. Klabunde, 'Art. 4 Begriffsbestimmungen' (*supra* Chapter II. note 4), para. 20; C. Bergauer, 'Begriff und Kategorien' (*supra* Chapter II. note 19), p. 48.

[125] European Union Agency for Fundamental Rights and Council of Europe, *Handbook on European data protection law* (*supra* Chapter II. note 26), p. 93; M. Finck and F. Pallas, 'They who must not be identified – distinguishing personal from non-personal data under the GDPR' (*supra* Chapter II. note 21), p. 13; W. Ziebarth, 'Artikel 4 Begriffsbestimmungen' (*supra* Chapter II. note 21), para. 29.

[126] A. Klabunde, 'Art. 4 Begriffsbestimmungen' (*supra* Chapter II. note 4), para. 20.

[127] WP136 (*supra* Chapter II. note 2), p. 21; also European Union Agency for Fundamental Rights and Council of Europe, *Handbook on European data protection law* (*supra* Chapter II. note 26), p. 93.

nected world, it can be argued that a person is virtually always at least identifiable by the means reasonably likely to be used.[128] This is highlighted by the example of the WP136, in which a store owner displays surveillance images of thieves in his store, but with their faces blanked out. According to the WP136, despite the blankening of faces, there is still a possibility that the thieves will be identified by their friends based on their figure, clothing and external appearance and are thus identifiable.[129] ISP/IP addresses[130], fingerprints[131], data collected by a private detective[132] and web cookies[133] also make it possible to identify a person.[134] Furthermore, the communication of names and physical addresses of Internet users, whose IP address and connection were known, are personal data.[135] In summary, it can be argued that in many cases a pseudonymisation rather than an anonymisation is present.

b) Breyer case

The judgment in the *Breyer* case[136] is the CJEU's most important contribution to the interpretation of the element 'identified or identifiable' to date. Mr. Breyer visited websites of German federal institutions, which stored the IP addresses of visitors' computers for security reasons, among other things.[137] According to the CJEU, 'IP addresses are series of digits assigned to networked computers to facilitate their communication over the internet.'[138] A distinction can be made between static and dynamic IP addresses, with the focus in the *Breyer* case being on dynamic IP addresses. Dynamic IP addresses change with each new internet connection and thus do not allow conclusions to be drawn from the computer to the physical network connection on the basis of publicly available data.[139]

---

[128] Schwartz and Solove are critical of the fact that identified and identifiable persons are dogmatically classified in the same way, since there are different degrees of intensity to identify information, and therefore demand that a clear distinction be made between identified and identifiable information. See P. M. Schwartz and D. J. Solove, 'The PII Problem: Privacy and a New Concept of Personally Identifiable Information' (*supra* Chapter II. note 97), p. 1876.

[129] WP136 (*supra* Chapter II. note 2), p. 21.

[130] See Case C-70/10 *Scarlet*, EU:C:2011:771, para. 51; Case C-293/12 *Digital Rights Ireland*, EU:C:2014:238, para. 26.

[131] See Case C-291/12 *Schwarz*, EU:C:2013:670, para. 27.

[132] See Case C-473/12 *IPI*, EU:C:2013:715, para. 26.

[133] See Case C-673/17 *Planet49*, EU:C:2019:801, para. 45.

[134] Bergauer refers to these examples as 'online identifiers', C. Bergauer, 'Begriff und Kategorien' (*supra* Chapter II. note 19), p. 54.

[135] See Case C-275/06 *Promusicae*, EU:C:2008:54, paras. 30 and 45; Case C-557/07 *LSG*, EU:C:2009:107, paras. 39–41; Case C-461/10 *Bonnier*, EU:C:2012:219, paras. 51–52.

[136] Case C-582/14 *Breyer*, EU:C:2016:779.

[137] Ibid, paras. 13 and 14.

[138] Ibid, para. 15.

[139] Ibid, para. 16.

Mr. Breyer requested the national courts to prohibit the storage of his IP address. The BGH dealt with the matter and gave its opinion on the 'objective' and 'relative' criterion. The 'objective' criterion allows information to be considered personal data, if it is possible for the data controller (i.e. website operator) or solely for a third party (i.e. the Internet provider) to identify a person.[140] According to a 'relative' criterion, data could be considered personal for the Internet provider, whereas it is not personal data for the website operator, since this operator does not have the required information to identify him without unreasonable effort.[141] The BGH consequently asked the CJEU for a preliminary ruling on whether

'an IP address […] constitutes personal data for the service provider [website operator] if a third party (an access provider) has the additional knowledge required in order to identify the data subject?'[142]

The CJEU stated that the IP addresses in the proceedings at hand are dynamic IP addresses.[143] Based on dynamic IP addresses, a website operator cannot identify the user who accessed the website.[144] However, the Internet provider has additional information that, together with the IP address, would allow the user to be identified.[145] Based on these premises, the CJEU held that dynamic IP addresses did not constitute information relating to an 'identified' natural person because the identity of the person is not directly apparent.[146]

The CJEU then addresses the question of whether IP addresses stored by a website provider can be classified as information about an 'identifiable' natural person.[147] As stated above, an identifiable natural person can be identified either directly or indirectly. The CJEU emphasised that it is not the information alone that must enable identification. It referred to Recital 26 of the GDPR, which states that

'to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person'.[148]

The CJEU interpreted this wording as not requiring a single person to have all the information necessary to identify an individual.[149] Therefore, IP addresses could

[140] Ibid, para. 25.
[141] Ibid.
[142] Ibid, para. 30.
[143] Ibid, para. 36.
[144] Ibid, para. 37.
[145] Ibid.
[146] Ibid, para. 38.
[147] Ibid, para. 39.
[148] Ibid, paras. 41 and 42.
[149] Ibid, para. 43.

also constitute personal data for the website provider if the Internet provider has the information necessary for identification.[150]

The CJEU affirmed this because the possibility of linking a dynamic IP address to the additional information held by the Internet provider was a means likely reasonably to be used to identify a person.[151] This would not be the case if identifying the individual would be prohibited or impractical, for example, because it would require an unreasonable effort in terms of time, cost and manpower.[152] However, the website provider in Germany had legal options, especially in the event of cyberattacks, to contact the authorities in order to obtain information from the Internet provider and initiate prosecution.[153]

The CJEU answered the BGH's question that a dynamic IP address constitutes personal data, where the website provider has the legal means which enable it to identify the data subject with additional data which the internet service provider has about that person.[154]

It can be noted that again the CJEU supported a broad interpretation of the term 'personal data'.[155] Moreover, the Court followed the objective criterion of identifiability.[156] This is supported by the fact that, in contrast to the relative

---

[150] Ibid, para. 44.

[151] Ibid, para. 48.

[152] Ibid, para. 46.

[153] Ibid, para. 47.

[154] Ibid, dictum.

[155] See also, F. Zuiderveen Borgesius, 'The Breyer Case of the Court of Justice of the European Union: IP Addresses and the Personal Data Definition', 3 *European Data Protection Law Review* (2017), pp. 130–137; V. Stück, 'Dynamische IP-Adressen sind personenbezogene Daten', 10 *CCZ – Corporate Compliance* (2017), p. 230.

[156] N. Purtova, 'The law of everything. Broad concept of personal data and future of EU data protection law' (*supra* Chapter II. note 15), p. 64; F. Zuiderveen Borgesius, 'The Breyer Case of the Court of Justice of the European Union: IP Addresses and the Personal Data Definition' (*supra* Chapter II. note 155), pp. 130–137; Different interpretation: A. S. Reid, 'The European Court of Justice case of Breyer', 2 *Journal of Information Rights, Policy and Practice* (2017), p. 5; G. Ziegenhorn, 'Speicherung von IP-Adressen beim Besuch einer Website', 36 *NVwZ – Neue Zeitschrift für Verwaltungsrecht* (2017), p. 217; Keppeler notes that the Advocate General's opinion makes a clear case for a significant step toward the objective criterion, L. M. Keppeler, '"Objektive Theorie" des Personenbezugs und "berechtigtes Interesse" als Untergang der Rechtssicherheit?', 32 *CR – Computer und Recht* (2016), p. 362; Ziebarth points out that the CJEU, by formulating the knowledge of a third party in a broad way, is approaching the objective criterion, W. Ziebarth, 'Artikel 4 Begriffsbestimmungen' (*supra* Chapter II. note 21), para. 37; Hansen and Struwe argue that the objective criterion is complemented by a relative criterion, H. Hansen and D. Struwe, 'Speicherung von IP-Adressen zur Abwehr von Cyberattacken zulässig', 8 *GRUR-Prax – Praxis im Immaterialgüter- und Wettbewerbsrecht* (2016), p. 503; Kühling and Klar refer to a balanced approach by the CJEU rather in the direction of the relative criterion, J. Kühling and M. Klar, 'EuGH: Speicherung von IP-Adressen beim Besuch einer Internetseite', 7 *ZD – Zeitschrift für Datenschutz* (2017), p. 28; According to Mantz and Spittka, the CJEU takes a mediating view, R. Mantz and J. Spittka, 'EuGH: Speicherung von IP-Adressen beim Besuch einer Website', 69 *NJW – Neue Juristische Wochenschrift* (2016), p. 3582; Moos and Rothkegel state that the

criterion, the knowledge of third parties is taken into account.[157] Here, too, the CJEU addresses the circumstances of the particular case in its reasoning. The relationship of the two parties to each other is essential to answering the question of whether or not the information constitutes personal data.[158] The judgment is consistent with the wording of Recital 26 of the GDPR, which refers to 'means reasonably likely to be used'.[159] The threshold of means likely reasonably to be used is legality.[160] Reasonable, legal means are only those that do not violate the law or require a disproportionate effort in time, cost and man-power.[161] It remains unclear whether the mere existence of legal means and the purely theorical possibility of being able to make use of it is sufficient to affirm identifiability.[162] If there are no legal means to identify an individual, there may be *de facto* illegal means.[163] Unfortunately, the judgment does not make precise statements as to when such illegal means are to be considered 'likely reasonably to be used'.[164] *Purtova* reasonably argues, that this threshold does not suggest a general restrictive approach, but rather stems from the fact that the BGH asked a narrow

---

CJEU's ruling rejects the objective criterion, but it places certain restriction on the relative criterion, F. Moos and T. Rothkegel, 'EuGH: Speicherung von IP-Adressen beim Besuch einer Internetseite', 19 *MMR – Zeitschrift für IT-Recht und Recht der Digitalisierung* (2016), p. 845; Eckhardt mentions that the CJEU does not completely ignore the knowledge of third parties, J. Eckhardt, 'Anmerkung zu EuGH, Urteil vom 19. Oktober 2016 – C-582/14', 60 *ZUM – Zeitschrift für Urheber- und Medienrecht* (2016), p. 1029 and J. Eckhardt, 'Anwendungsbereich des Datenschutzrechts – Geklärt durch den EuGH?', 32 *CR – Computer und Recht* (2016), p. 787; Richter omits a classification, H. Richter, 'EuGH: Datenschutzrecht: Speicherung von IP-Adressen beim Besuch einer Website', 27 *EuZW – Europäische Zeitschrift für Wirtschaftsrecht* (2016), p. 912.

[157] W. Ziebarth, 'Artikel 4 Begriffsbestimmungen' (*supra* Chapter II. note 21), para. 38.

[158] M. Mourby et al., 'Are "pseudonymised" data always personal data? Implications of the GDPR for administrative data research in the UK', 34 *Computer Law & Security Report* (2018), p. 233.

[159] G. Ziegenhorn, 'Speicherung von IP-Adressen beim Besuch einer Website' (*supra* Chapter II. note 156), p. 217.

[160] F. Zuiderveen Borgesius, 'The Breyer Case of the Court of Justice of the European Union: IP Addresses and the Personal Data Definition' (*supra* Chapter II. note 155), pp. 130–137.

[161] Case C-582/14 *Breyer* (*supra* Chapter II. note 136), para. 46; Opinion of Advocate General Sánchez-Bordona in Case C-582/14 *Breyer,* EU:C:2016:339, para. 68.

[162] F. Moos and T. Rothkegel, 'EuGH: Speicherung von IP-Adressen beim Besuch einer Internetseite' (*supra* Chapter II. note 156), p. 846; H. Richter, 'EuGH: Datenschutzrecht: Speicherung von IP-Adressen beim Besuch einer Website' (*supra* Chapter II. note 156), p. 913.

[163] G. Ziegenhorn, 'Speicherung von IP-Adressen beim Besuch einer Website' *supra* Chapter II. note 156), p. 217.

[164] Ibid.

question.[165] Indeed, the BGH did not ask whether dynamic IP addresses always constitute personal data and whether they are also personal data if any third party can identify the person.[166] The consequence of this judgment is that it requires case-by-case decisions as to whether IP addresses are personal data.[167]

5. 'Natural person'

Article 4 (1) of the GDPR refers to natural persons, which is the last element of the definition of personal data.[168] Recital 14 of the GDPR also states that

'the protection afforded by this Regulation should apply to natural persons, whatever their nationality or place of residence, in relation to the processing of their data'.[169]

Every human being is considered a 'natural person' and is a bearer of rights and obligations ('legal subject').[170] As is generally known, legal capacity begins at birth and ends at death in principle. The WP136 concludes that personal data is therefore in theory any information relating to identified or identifiable living human beings.[171] This concept opens up three problem areas, which will be discussed briefly: data on deceased persons, unborn children and legal persons.

In principle, data relating to deceased persons are not covered by the concept of personal data, but they may have an indirect personal link.[172] For example, the

---

[165] N. Purtova, 'The law of everything. Broad concept of personal data and future of EU data protection law' (*supra* Chapter II. note 15), p. 65; See also, R. Mantz and J. Spittka, 'EuGH: Speicherung von IP-Adressen beim Besuch einer Website' (*supra* Chapter II. note 156), p. 3582.

[166] Opinion of Advocate General Sánchez-Bordona in Case C-582/14 *Breyer* (*supra* Chapter II. note 161), para. 50; F. Zuiderveen Borgesius, 'The Breyer Case of the Court of Justice of the European Union: IP Addresses and the Personal Data Definition' (*supra* Chapter II. note 155), pp. 130–137.

[167] P. De Hert, 'Data protection's future without democratic bright line rules. Co-existing with Technologies in Europe after Breyer', 3 *European Data Protection Law Review* (2017), p. 27; See also El Khoury, whose article highlights this as early as the title, A. El Khoury, 'Dynamic IP Addresses Can be Personal Data, Sometimes. A story of Binary Relations and Schrödinger's cat', 8 *European Journal of Risk Regulation* (2017), p. 196.

[168] See Article 4 (1) GDPR.

[169] See Recital 14 GDPR.

[170] See Section 16 of the ABGB: 'Jeder Mensch hat angeborene, schon durch die Vernunft einleuchtende Rechte, und ist daher als eine Person zu betrachten.'; Article 6 of the Universal Declaration of Human Rights: 'Everyone has the right to recognition everywhere as a person before the law'.

[171] WP136 (*supra* Chapter II. note 2), p. 22.

[172] See Recital 27 GDPR; WP136 (*supra* Chapter II. note 2), p. 22; Feiler and Forgó express a different view, L. Feiler and N. Forgó, *EU-DSGVO* (Verlag Österreich, 2016), p. 71; Ziebarth argues that only data processing that occurred during the lifetime of the data subject can be taken into account, W. Ziebarth, 'Artikel 4 Begriffsbestimmungen' (*supra* Chapter II. note 21), para. 11.

information that a deceased person suffered from a hereditary disease, may indicate that the living descendants also have this hereditary disease and thus refer to living individuals.[173] In addition, some Member States grant rights to persons after death as part of post-mortem privacy.[174]

The degree to which the data of unborn children fall under the concept of personal data depends on the legal system of each Member State.[175] For instance, unborn children in Austria have legal capacity as soon as they are conceived and can be heirs, for example, under the condition that they are born alive.[176] According to the WP136, these national provisions are to be consulted when determining whether information of unborn children should be considered personal data.[177] In my opinion, this view should be followed, since it would not make sense systematically to distinguish between the data of deceased and unborn persons.[178]

Recital 14 of the GDPR states that the Regulation does not cover the data processing of legal persons.[179] This concerns in particular undertakings, name, contact details and the form of the legal person.[180] This is also in line with the rest of the Regulation, which only includes natural persons in its scope of protection.[181] However, information about legal persons may also relate to natural persons if at least one of the characteristics 'content', 'purpose' or 'result' is fulfilled.[182] This may be the case, for example, with one-person companies or

---

[173] WP136 (*supra* Chapter II. note 2), p. 22; A. Klabunde, 'Art. 4 Begriffsbestimmungen' (*supra* Chapter II. note 4), para. 13.

[174] WP136 (*supra* Chapter II. note 2), p. 22.

[175] Ibid.

[176] See Section 22 ABGB: 'Selbst ungeborne Kinder haben von dem Zeitpunkte ihrer Empfängnis an, einen Anspruch auf den Schutz der Gesetze. Insoweit es um ihre und nicht um die Rechte eines Dritten zu tun ist, werden sie als Geborne angesehen; ein totgebornes Kind aber wird in Rücksicht auf die ihm für den Lebensfall vorbehaltenen Rechte so betrachtet, als wäre es nie empfangen worden'.

[177] WP136 (*supra* Chapter II. note 2), p. 22.

[178] See also W. Ziebarth, 'Artikel 4 Begriffsbestimmungen' (*supra* Chapter II. note 21), para. 12; but Feiler and Forgó state that the term (probably) does not include nascituri, L. Feiler and N. Forgó, *EU-DSGVO* (*supra* Chapter II. Note 172), p. 71.

[179] See Recital 14 GDPR.

[180] Ibid.

[181] See, for example, the title of the Regulation: '[…] on the protection of *natural persons* […]'; in contrast, C. Bergauer states that Article 8 of the Charter refers to 'everyone', which is why the Charter's wording would in principle include legal persons, C. Bergauer, 'Begriff und Kategorien' (*supra* Chapter II. note 19), p. 52.

[182] WP136 (*supra* Chapter II. note 2), p. 23; A. Klabunde, 'Art. 4 Begriffsbestimmungen' (*supra* Chapter II. note 4), para. 10; W. Ziebarth, 'Artikel 4 Begriffsbestimmungen' (*supra* Chapter II. note 21), para. 13; see also, F. Costa-Cabral and O. Lynskey, 'Family ties: The intersection between data protection and competition in EU law' (*supra* Chapter II. note 4), p. 16.

with e-mail addresses such as 'forename.surname@company.eu'.[183] The CJEU ruled accordingly in the *Volker und Markus Schecke und Eifert* case.[184] It held that

'legal persons can claim the protection of Articles 7 and 8 of the Charter in relation to such identification only in so far as the official title of the legal person identifies one or more natural persons.'[185]

6. Conclusion: Broad definition of 'personal data' in the GDPR

The aim of this chapter was to take a closer look at the concept of personal data, which usually depends on the specific case on hand. This concept is often taken for granted. The analysis of the WP136 and relevant CJEU case law, which was undertaken in this chapter, helps to understand which case constellations are included in the concept of personal data and which are not.

It is clear that the EU legislator intended a broad definition of personal data. This is also the understanding of the WP29 and the CJEU. In this context, it is worth citing *Purtova*, who mentions that according to this understanding, almost any data is personal data and the option of abandoning the concept of personal data altogether should be considered and instead, the focus could shift to addressing 'information-induced harms', treating all data as personal and requiring impact assessments for all processing.[186] The reason for this understanding seems to be that the protection of fundamental rights of natural persons is at the core of this protection, which should therefore be as extensive as possible. Furthermore, the broad definition takes into account ongoing technical developments, including an almost omnipresent data processing. Moreover, it is noteworthy that the data concerned are never examined in isolation. Both the WP29 and the CJEU take a contextual view. While this approach does not allow for a general statement as to when personal data are involved, it does prevent a generally excessive or restrictive definition. The four conditions 'any information', 'relating to', 'an identified or identifiable', 'natural person' must all be met for information to be personal data.

The first building block, 'any information', requires a broad interpretation of the definition. It does not matter whether the information is subjective or objective. Content and format are also irrelevant. This was also held by the CJEU in the *Nowak* case.

---

[183] European Commission, *Do the data protection rules apply to data about a company?*, https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/application-regulation/do-data-protection-rules-apply-data-about-company_en (accessed 31 January 2024).

[184] Case C-92/09 *Volker und Markus Schecke und Eifert*, EU:C:2010:662.

[185] Ibid, para. 53; see also Case C-419/14 *WebMindLicenses*, EU:C:2015:832, para. 79.

[186] N. Purtova, 'The law of everything. Broad concept of personal data and future of EU data protection law' (*supra* Chapter II. note 15), p. 80.

The second building block, 'relating to', makes it clear that information can be personal data that does not appear to be such at first glance. Especially the alternative elements 'content', 'purpose' and 'result' enable an extensive scope. These elements are also used by the CJEU, even if the exact wording is different. In the *Nowak* case, the CJEU revised the narrower line of the *YS* judgment in favour of a broader interpretation.

The third building block, 'identified or identifiable' deals in particular with the 'means reasonably likely to be used' by a person to identify an individual directly or indirectly. The CJEU stated here that in certain circumstances it is sufficient if a third party has the necessary means to be able to identify a person. According to the *Breyer* judgment, the limit of reasonableness of the means is legality. Here, too, it comes down to a case-by-case assessment. While pseudonymous data are covered by the concept of identifiability, anonymous data are not.

The fourth element, 'natural person', in principle includes living human beings. But as stated above, deceased persons, unborn children and legal persons may also be included.

As the term 'personal data' has now been defined, the following chapter will address the extent to which personal data can be measured in value and be an economic asset.

III. The value of personal data

The previous chapter narrowed down what is meant by personal data. This chapter will examine the value of personal data. The term 'personal data as an economic asset', as used in the title of this work, suggests that data has a monetary value. The widely known claim that 'data is the new oil'[1] comes to mind in this context.

'The Economist' went even further in 2017 by publishing an article entitled 'The world's most valuable resource is no longer oil, but data'.[2] If one examines the world's most valuable companies it quickly becomes apparent that many of them are active in the data economy and the article's claim seems valid. In 2020, the top five most valuable brands were Apple, Google, Microsoft, Amazon and Facebook.[3] These five companies had a combined value of around $ 800 billion US dollars.[4]

The EU also believes that data is an invaluable resource for economic growth, innovation and social development.[5] In its data strategy, the European Commission describes data as the 'lifeblood of economic development'.[6] The data strategy aims to create a single market for data that ensures Europe's competitiveness and data sovereignty.[7] Investments, legislative measures and access are intended to ensure that more data is available for use in business and society, with individuals empowered to be in control of their data.[8]

What is the value of personal data? Why are data referred to as 'lifeblood' of the economy? This chapter attempts to answer these questions. In this context, it is useful to follow the structure of an OECD paper that uses different methods to

---

[1] The origin of this quote likely goes back to the mathematician Clive Humby in 2006.

[2] The Economist*, The world's most valuable resource is no longer oil, but data*, 6 May 2017, https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data (accessed 31 January 2024).

[3] M. Swant*, 'The world's most valuable brands 2020', Forbes* (2020), https://www.forbes.com/the-worlds-most-valuable-brands/#41073ad5119c (accessed 31 January 2024).

[4] Ibid.

[5] European Commission*, A European strategy for data*, 9 March 2021, https://digital-strategy.ec.europa.eu/en/policies/strategy-data (accessed 31 January 2024).

[6] Communication from the Commission to the European Parliament, the Council, the European economic and social committee and the committee of the regions – A European strategy for data, COM(2020) 66 final, p. 2.

[7] Ibid, p. 4.

[8] Ibid, p. 10.

assess the value of personal data.[9] Section 1 sets out the unique economic characteristics surrounding personal data. Section 2 examines how companies use, share and value personal data in the data-driven economy. Section 3 then delves into the market value of personal data. Section 4 reflects on how prices in illegal markets and the cost of a data breach can be used as proxies for the valuation of personal data. Section 5 analyses the value of personal data using surveys and experiments, while Section 6 provides an overview of the valuation of personal data based on individual willingness to pay to protect personal data. Finally, Section 7 outlines the criteria for the selection of a valuation method.

1. The Economics of Personal Data

Personal data stands apart from conventional assets due to its unique economic characteristics that warrant careful consideration in determining its value. The following characterisation follows the structure of 'The Value of Data summary report 2020'.[10] Firstly, personal data is non-rivalrous, enabling multiple users to access and utilise its simultaneously without depletion.[11] Contrary to traditional ownership or exchange, the concept of ownership does not apply to personal data, as will be shown below. Moreover, the excludability of data varies. Public data are accessible to anyone, while other data types allow for exclusion.[12] As personal data can possess infinite usability, significant societal benefits can be derived from scenarios where multiple researchers utilise the same data concurrently.[13] *Jones* and *Tonetti* indicate that limitations imposed on the non-rivalrous use of data can result in substantial welfare costs.[14]

Personal data introduces externalities, both positive and negative, with the combination of datasets often enhancing their value (positive externalities) and harms arising from data collection or usage (negative externalities).[15] Balancing these externalities is crucial for finding the equilibrium between exploiting personal data's potential and protecting privacy.[16] Under certain conditions, these externalities may disrupt data markets, resulting in both suboptimally low prices

---

[9] OECD, *Exploring the Economics of Personal Data*, 2 April 2013, p. 30, https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en (accessed 31 January 2024).

[10] D. Coyle et al., 'The value of data summary report', *The Bennett Institute for Public Policy* (2020), p. 4.

[11] Ibid, p. 4; C. I. Jones and C. Tonetti, 'Nonrivalry and the Economics of Data', 110 *American Economic Review* (2020), p. 2819.

[12] D. Coyle et al., 'The value of data summary report' (*supra* Chapter III. note 10), p. 4.

[13] C. I. Jones and C. Tonetti, 'Nonrivalry and the Economics of Data' (*supra* Chapter III. note 11), p. 2856.

[14] Ibid, p. 2857.

[15] D. Coyle et al., 'The value of data summary report' (*supra* Chapter III. note 10), p. 4.

[16] Ibid, p. 4.

for data and excessive privacy losses, driven by the perception that others are already selling their personal data at reduced rates.[17] For example, when an individual shares their personal data on online platforms, they inadvertently disclose information about others.[18] In this context, externalities contribute to lowering the value of personal data, as once a person's information is exposed by others, the person becomes less incentivised to safeguard their personal data[19] The resultant decrease in personal data value fosters a trend of excessive data sharing.[20]

Furthermore, personal data may exhibit increasing or decreasing returns.[21] There are many key factors that characterise data-based value creation, e.g. data source, data analysis, customer etc.[22] Therefore, while collecting more personal data can yield additional insights, there are instances where accumulating more personal data adds minimal value.[23] This accumulation often occurs as companies anticipate the potential future significance of personal data, leading to personal data hoarding practices.[24]

Additionally, personal data holds substantial option value, i.e. the right but not the obligation to use personal data as an asset, due to its unpredictable future relevance.[25] Especially the duration of its benefits and the appropriate level of cost alignment remain uncertain.[26] Factors like new data, evolving technologies, algorithms and legislation can reshape the importance of existing personal data.[27] Yet, companies often retain personal data not just for its current value but also for its untapped potential.[28] In such instances, companies may opt to delay personal data processing as they await additional information, such as updates on policy changes, technological advancements, shifts in consumer preferences, and other relevant factors, to assess the value of the personal data.[29]

---

[17] C. I. Jones and C. Tonetti, 'Nonrivalry and the Economics of Data' (*supra* Chapter VIII. note 4), p. 2823.

[18] D. Acemoglu et al., 'Too Much Data: Prices and Inefficiencies in Data Markets', 14 *American Economic Journal: Microeconomics* (2022), p. 218.

[19] Ibid.

[20] Ibid, p. 243.

[21] D. Coyle et al., 'The value of data summary report' (*supra* Chapter III. note 10), p. 4.

[22] See C. Lim et al., 'From data to value: A nine-factor framework for data-based value creation in information-intensive services', 39 *International Journal of Information Management* (2018), pp. 121–135.

[23] D. Coyle et al., 'The value of data summary report' (*supra* Chapter III. note 10), p. 4.

[24] Ibid.

[25] Ibid.

[26] H. Cheong et al., 'A Data Valuation Model to Estimate the Investment Value of Platform Companies: Based on Discounted Cash Flow', 16 *Journal of Risk and Financial Management* (2023), p. 2.

[27] D. Coyle et al., 'The value of data summary report' (*supra* Chapter III. note 10), p. 4.

[28] Ibid.

[29] D. Coyle and A. Manley, 'What is the Value of Data? A review of empirical methods', *The Bennett Institute for Public Policy* (2022), p. 18.

The dynamics of personal data collection involve a high upfront cost, including investments in hardware, digitisation, or quality improvement, with subsequent lower ongoing costs for collecting additional personal data, especially with automated processes.[30] These initial high costs can serve as barriers for some firms, incentivising a focus on financial returns.[31] Moreover, the utilisation of personal data requires additional investments in complementary elements such as software, computing resources and skilled personnel.[32] These investments act as barriers that companies need to overcome to derive tangible value from their personal data assets.[33]

In essence, understanding and valuing data necessitate navigating through these intricate economic characteristics that define its role and significance in contemporary contexts.

2. How companies use, share and value personal data

Increasing digitisation is a well-known phenomenon. Virtual assistants, smartphones and social media are just three of countless examples that are shaping our everyday lives and have become indispensable. Information and data are collected with every digital interaction. Thus, every person leaves a digital footprint. The author of this work checked his own digital footprint on Facebook. It is possible to access and download the information stored by Facebook.[34] The file downloaded as a result had a size of 250 megabytes. It contained a considerable amount of information: personal information (including face recognition, voice recording and transcription, friend/peer-group, notifications, preferences, viewed and visited profiles/pages), ads (ads interests, advertisers who uploaded a contact list with the author's information, advertisers the author has interacted with), comments, like/reactions, events (event invitations, event responses), location (last location, primary location, time zone, voting location), messages, posts, search history, etc.

In this context, *Becerril* describes how people have become digital 'ones' and 'zeros' of online companies, alluding to the binary system that computers utilise to store information.[35] For many users, these online services give the impression of being free of charge, as they usually do not require payment. However, in return, users disclose personal data about themselves and 'pay' with it.[36]

---

[30] D. Coyle et al., 'The value of data summary report' (*supra* Chapter III. note 10), p. 4.

[31] Ibid.

[32] Ibid.

[33] Ibid.

[34] Facebook Help Centre, https://www.facebook.com/help/contact/2032834846972583 (accessed 31 January 2024).

[35] A. Becerril, 'The value of our personal data in the Big Data and the Internet of all Things Era', 7 *Advances in Distributed Computing and Artificial Intelligence Journal* (2018), p. 72.

[36] G. Malgieri and B. Custers, 'Pricing privacy – the right to know the value of your

a) Companies' use of personal data

Internet users are estimated to have totaled 5.3 billion in 2023, accounting for nearly 65 % of the world's population.[37] These users create countless amounts of data on the Internet. It is estimated that 500 hours of video material is uploaded every minute on YouTube alone.[38] This figure is from 2022, and since the amount of data has been steadily increasing in the years before, it is reasonable to assume that the amount of video material uploaded to YouTube per minute will be even higher in 2024.[39] The four online giants Google, Microsoft, Amazon and Facebook are believed to store nearly 1,200 petabytes.[40] This equals 1,2 trillion megabytes.[41] This number of stored data is already impressive when considering that the author's Facebook file contains 250 megabytes and in itself a considerable amount of information. If one additionally considers that this data is only stored by four companies and many other institutions are processing data, this number takes on another dimension that almost exceeds human comprehension. These companies have been described as 'data vultures' by *Véliz*.[42]

The above-mentioned online companies have in common that they collect and analyse this information. As a result, personal profiles can be created. This process is called 'profiling'.

The GDPR provides a legal definition of profiling:

'profiling means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;'[43]

---

personal data', 34 *Computer Law & Security Review* (2018), p. 292; B. Ehrenberg, 'How much is your personal data worth?', *The Guardian* (2014), https://www.theguardian.com/news/datablog/2014/apr/22/how-much-is-personal-data-worth (accessed 31 January 2024).

[37] A. Petrosyan, 'Worldwide digital population 2023', *Statista* (2023), https://www.statista.com/statistics/617136/digital-population-worldwide/ (accessed 31 January 2024).

[38] L. Ceci, 'Hours of video uploaded to Youtube every minute as of February 2022', *Statista* (2023), https://www.statista.com/statistics/259477/hours-of-video-uploaded-to-youtube-every-minute/ (accessed 31 January 2024).

[39] An interesting overview of how much data was generated per minute in 2021 can be found at Domo, *Data never sleeps 9.0*, https://www.domo.com/learn/infographic/data-never-sleeps-9 (accessed 31 January 2024).

[40] G. Mitchell, 'How much data is on the internet?', *Science Focus* (2021), https://www.sciencefocus.com/future-technology/how-much-data-is-on-the-internet/ (accessed 31 January 2024).

[41] Computer Hope, *How much is 1 byte, kilobyte, megabyte, gigabyte, etc.?*, https://www.computerhope.com/issues/chspace.htm (accessed 31 January 2024).

[42] C. Véliz, *Privacy Is Power* (Penguin Random House, 2020), pp. 7–30.

[43] See Article 4 (4) GDPR.

The personal aspects named here are only exemplary and not conclusive.[44] Data processing to create profiles and to control interaction with individuals has gained great importance and is the basis of the business models of some major internet companies.[45] It is therefore not surprising that the GDPR also explicitly addresses profiling by internet companies. Thus, profiling also occurs when a profile is created to track internet activities in order to identify or predict a person's habits, behaviours or preferences.[46] By combining online identifiers such as IP addresses and cookies with other relevant information, profiles of natural persons can also be created.[47] The merging of other information relating to the data subject, such as information from 'smart' things (e.g. smartphone, smartwatch, smart speaker etc.), is an example of profiling, too.[48] Through these types of data processing and profiling, the data can be used to the economic advantage of companies.[49]

These profiles are where essential value of personal data lies for companies, as will be illustrated on the following pages using the example of Facebook. Facebook changed the name of its conglomerate to 'Meta', but due to the familiarity of the term 'Facebook' and because the terms are used synonymously in common parlance, the term 'Facebook' will be used to describe the conglomerate in this work. Facebook is used as an example because it is not only one of the most valuable companies in the world, but also due to its tremendous impact and importance in everyday life through Instagram and WhatsApp, in addition to its namesake social network. Indeed, 96 % of adolescents in Austria use WhatsApp.[50]

Facebook uses what is known as ad targeting. This involves displaying ads that are relevant to specific target pages or groups. Companies can use this method for a fee and thus place targeted, group-oriented ads on Facebook. The slogan 'Reach the people who want to hear from you' on the Facebook ad targeting help page speaks for itself.[51] One can choose between multiple advertising options here: 'core audiences', 'custom audiences' and 'lookalike audiences'.[52]

---

[44] S. Ernst, 'IV. Profiling (Nr. 4)' in B. Paal and D. Pauly (eds.), *DS-GVO BDSG* (3rd edition, CH-Beck, 2021), para. 37.

[45] A. Klabunde, 'Art. 4 Begriffsbestimmungen' (*supra* Chapter II. note 4), para. 28.

[46] See Recital 24 GDPR.

[47] See Recital 30 GDPR.

[48] S. Ernst, 'IV. Profiling (Nr. 4)' (*supra* Chapter III. note 44), para. 39.

[49] A. Klabunde, 'Art. 4 Begriffsbestimmungen' (*supra* Chapter II. note 4), para. 28.

[50] Saferinternet, *Jugend-Internet-Monitor 2023*, https://www.saferinternet.at/services/jugend-internet-monitor/ (accessed 31 January 2024).

[51] See Facebook, *Ad targeting*, https://www.facebook.com/business/ads/ad-targeting (accessed 31 January 2024).

[52] Ibid.

Using criteria such as location, demographics, interest, behaviour and connections, it is possible to precisely define the target audience with 'core audiences' and thus determine who sees the advertising and who does not.[53] With the second advertising option 'custom audiences', companies can reach people who are either already customers or have shown interest in the company.[54] This method of targeted advertising is often the topic of privacy debates.[55] In this case, not only does Facebook use the information it has profiled itself, but companies can also upload customer e-mail lists, which Facebook then compares with their own profiles. Furthermore, a person can be targeted based on visits on an advertiser's website, app or store. This means that information is shared across multiple homepages and devices. The third option allows companies to reach people who are similar to existing customers.[56] Here, people are targeted who have the same characteristics, behaviours and interests, thereby expanding the target group to include a similar set of people.

Through profiling and based on the analysis of online behaviour, personalised advertising strategies can be developed for companies.[57] Knowledge and information about existing and future customers is generated, which is considered the key to commercial success.[58] This is to create tractable and predictable customers.[59] This phenomenon, also known as behavioural targeting, was the subject of a study conducted by *Beales.*[60] The study examined how much money twelve advertising networks[61] spent on advertising, how many people were converted from interested parties to customers as a result and how much revenue was generated. A distinction was made between advertising that was applied without specific criteria and behavioural targeting that uses the online behaviour of users and is applied to specific sites.

The study has three main findings. First, study participants were willing to spend almost 2.6 times more on behavioural advertising than on non-personalised advertising.[62] Second, the percentage of ad views that resulted in purchases

---

[53] Ibid.

[54] Ibid.

[55] See for example, C. Blasi Casagran and M. Vermeulen on political campaigns utilising advertising tools offered by online platforms: C. Blasi Casagran and M. Vermeulen, 'Reflections on the murky legal practices of political micro-targeting from a GDPR perspective', 11 *International Data Privacy Law* (2021), pp. 348–359.

[56] See Facebook, *Ad targeting* (*supra* Chapter III, note 51).

[57] A. Becerril, 'The value of our personal data in the Big Data and the Internet of all Things Era' (*supra* Chapter III. note 35), p. 74.

[58] See J. E. Cohen, 'The Inverse Relationship between Secrecy and Privacy', 77 *Social Research* (2010), p. 884.

[59] J. E. Cohen, 'What Privacy Is For' (*supra* Chapter I. note 2), p. 1917.

[60] See H. Beales, 'The Value of Behavioral Targeting', *Network Advertising Initiative* (2010), pp. 1–24.

[61] Ibid, p. 19, advertising networks are intermediaries, pairing advertisers with online publishers.

[62] Ibid, p. 8.

was twice as high for behavioural advertising than for non-personalised advertising.[63] Third, nearly 40 % of the revenue of the ad networks surveyed was generated by behavioural advertising.[64] Since personal advertising is driven by personal information generated by a user's online behaviour, it is reasonable to argue that personal data is considered a valuable asset in the online advertising world.

A more recent paper analyses how smart speakers use people's voice input. The authors found that Amazon tracks voice inputs into their smart speaker system 'Amazon Echo'.[65] Amazon used this personal data for targeted advertising on its platform and off its platform.[66] These smart speaker voice inputs lead to 30x higher advertising bids from advertisers.[67] Personal data therefore becomes a valuable asset through profiling and targeted advertising.

For the purpose of completeness, it should be mentioned that while behavioural advertising was indeed the leading business model for a long time, at least recently, user data-independent advertising has also seen increased use, especially in the form of contextual advertising.[68] Contextual advertising is a method of displaying online advertising in a content environment that is ideally suited to it.[69] The basic idea is to display adverts on pages that are mostly visited by people who are interested in such offers. For example, in the case of promoting Basketball game tickets, ads can strategically be placed within articles of a newspaper directly associated with the game, optimising engagement through precise contextual alignment.[70]

The growing prevalence of contextual advertising can be attributed to heightened concern for consumer privacy, (temporary) bans on behavioural advertising and major tech companies that are progressively limiting targeting capabilities, with Google notably restricting website access to third-party cookies for 1 % of user, as part of their aim to limit cross-site tracking on the web.[71] This shift

---

[63] Ibid, p. 12.

[64] Ibid, p. 14.

[65] U. Iqbal et al., *Your Echos are Heard: Tracking, Profiling, and Ad Targeting in the Amazon Smart Speaker Ecosystem*, 28 April 2022, p. 5, https://alexaechos.com/amazon_echo.pdf (accessed 31 January 2024).

[66] Ibid, p. 11.

[67] Ibid.

[68] See E. Häglund and J. Björklund, 'AI-Driven Contextual Advertising: A Technology Report and Implication Analysis', *arXiv:2205.00911* (2022).

[69] See K. Zhang and Z. Katona, 'Contextual Advertising', 6 *Journal of Business Ethics* (2012), pp. 980–994; I. Yaveroglu and N. Donthu, 'Advertising repetition and placement issues in on-line environments', 37 *Journal of Advertising* (2008), pp. 31–44.

[70] B. Shepard, 'The New Rise of Contextual Advertising', *Forbes* (2021), https://www.forbes.com/sites/forbesagencycouncil/2021/07/22/the-new-rise-of-contextual-advertising/?sh=3114abb65e5d (accessed 31 January 2024).

[71] G. Fouche, 'Facebook owner Meta faces EU ban on targeted advertising', *Reuters* (2023), https://www.reuters.com/technology/facebook-owner-faces-eu-ban-targeted-advertising-norway-says-2023-11-01/#:~:text=%22On%2027%20October%2C%20the%20EDPB,Economic%20Area%2C%22%20it%20said. (accessed 31 January 2024); Chrome, *The next step*

encourages a departure from personal data and behavioural tracking, positioning contextual advertising, which operates without relying on such data, as an appealing alternative.[72] Instead of relying on previously collected personal data, contextual advertising assumes that consumers' content requests reflect their current mindset and product preferences, allowing for tailored ad placements and an increase in revenue.[73]

Nevertheless, behavioural advertising increases the effectiveness of advertising.[74] In a recent study, behavioural advertising increased the Click-through-rate, i.e. the number of clicks that an ad receives divided by the number of times the ad is shown, by 66,8 %.[75] Thus, despite the above challenges, behavioural advertising can still be profitable, especially if it does not target narrow audiences.[76] Therefore, it contributes to the value of personal data.

b) Sharing personal data

Companies also share the data with third parties. This practice became known to the wider public through the *Cambridge Analytica scandal.* Facebook users were asked to participate in a personality survey and download an app that extracted some private information from their profiles and those of their friends – an activity Facebook allowed at the time and has since banned.[77] In the wake of this scandal, it was revealed in March 2018 that more than 50 million data records of

---

toward phasing out third-party cookies in Chrome, 14 December 2023, https://blog.google/products/chrome/privacy-sandbox-tracking-protection/ (accessed 31 January 2024); E. Häglund and J. Björklund, 'AI-Driven Contextual Advertising: A Technology Report and Implication Analysis' (*supra* Chapter III. note 68), p. 3.

[72] See E. Häglund and J. Björklund, 'AI-Driven Contextual Advertising: A Technology Report and Implication Analysis' (*supra* Chapter III. note 68), p. 3, who are referencing IPSOS, 'IAB State of Data 2021 Quantitative Analysis Assessing Perceived vs. Actual Preparedness for the Post Third-Party Cookie and Identifier Tracking and Ecosystem', *International Advertising Bureau* (2021), https://www.iab.com/wp-content/uploads/2021/03/IAB_Ipsos_State_Of_Data_2021-03.pdf (accessed 31 January 2024).

[73] See S. Ada et al., 'Context information can increase revenue in online display advertising auctions: Evidence from a policy change', 59 *Journal of Marketing Research* (2022), pp. 1040–1058; E. Häglund and J. Björklund, 'AI-Driven Contextual Advertising: A Technology Report and Implication Analysis' (*supra* Chapter III. note 68), p. 3.

[74] See J. Yan et al., 'How much Can Behavioral Targeting Help Online Advertising?', *Proceedings of the 18th International Conference on World Wide Web* (2009), pp. 261–270; A. Farahat and M.C. Bailey, 'How Effective is Targeted Advertising', *Proceedings of the 21st International Conference on World Wide Web* (2012), pp. 111–120.

[75] O. Rafieian and H. Yoganarasimhan, 'Targeting and Privacy in Mobile Advertising', 40 *Marketing Science* (2021), pp. 193–218.

[76] See I. Ahmadi et al., 'Overwhelming targeting options: Selecting audience segments for online advertising', *International Journal of Research in Marketing*, forthcoming.

[77] K. Granville, 'Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens', *The New York Times* (2018), https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html (accessed 31 January 2024).

Facebook users were used and processed without their knowledge and consent by *Cambridge Analytica*.[78] In April 2018, Facebook announced that 87 million data records had been harvested and that the number of affected users was therefore even higher than first assumed.[79] These data sets are also said to have been obtained by Donald Trump's campaign team in 2016.[80] The potential influence that obtaining personal information of potential voters could have had on the 2016 US elections should not be understated.[81]

Mark Zuckerberg is facing legal action as he is accused of being personally involved in Facebook's inadequate protection of users' privacy in the wake of the *Cambridge Analytica scandal*.[82] Initially, after this news was made public, *Mark Zuckerberg*, CEO of Facebook, was summoned before the US Congress and testified that Facebook 'does not sell data to anyone'.[83] While this may be true, it is misleading, as The New York Times reported that Facebook has reached agreements with 150 companies to share data.[84] Most of these companies are

---

[78] M. Rosenberg, N. Confessore and C. Cadwalladr, 'How Trump Consultants Exploited the Facebook Data of Millions', *The New York Times* (2018), https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html (accessed 31 January 2024); C. Cadwalladr and E. Graham-Harrison, 'Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach', *The Guardian* (2018), https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election (accessed 31 January 2024).

[79] Facebook, *An Update on Our Plans to Restrict Data Access on Facebook,* 4 April 2018, https://about.fb.com/news/2018/04/restricting-data-access/ (accessed 31 January 2024); C. Kang and S. Frenkel, 'Facebook Says Cambridge Analytica Harvested Data of Up to 87 Million Users', *The New York Times* (2018), https://www.nytimes.com/2018/04/04/technology/mark-zuckerberg-testify-congress.html (accessed 31 January 2024).

[80] M. Rosenberg, N. Confessore and C. Cadwalladr, 'How Trump Consultants Exploited the Facebook Data of Millions' (*supra* Chapter III. note 78); C. Cadwalladr and E. Graham-Harrison, 'Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach' (*supra* Chapter III. note 78).

[81] K. Collins and G. Dance, 'How Researchers Learned to Use Facebook "Likes" to Sway Your Thinking', *The New York Times* (2018), https://www.nytimes.com/2018/03/20/technology/facebook-cambridge-behavior-model.html (accessed 31 January 2024); A. Hern, 'Cambridge Analytica: how did it turn clicks into votes?', *The Guardian* (2018), https://www.theguardian.com/news/2018/may/06/cambridge-analytica-how-turn-clicks-into-votes-christopher-wylie (accessed 31 January 2024); however, it has already been established that Cambridge Analytica did not misuse the data sets to influence the Brexit referendum, see J. Waterson, 'Cambridge Analytica did not misuse data in EU referendum, says watchdog', *The Guardian* (2020), https://www.theguardian.com/uk-news/2020/oct/07/cambridge-analytica-did-not-misuse-data-in-eu-referendum-says-watchdog (accessed 31 January 2024).

[82] E. Birnbaum, 'D.C. attorney general sues Mark Zuckerberg over Cambridge Analytica', *Politico* (2022), https://www.politico.com/news/2022/05/23/attorney-general-sues-mark-zuckerberg-cambridge-analytica-00034368 (accessed 31 January 2024).

[83] The Washington Post, *Transcript of Mark Zuckerberg's Senate hearing*, 11 April 2018, https://www.washingtonpost.com/news/the-switch/wp/2018/04/10/transcript-of-mark-zuckerbergs-senate-hearing/ (accessed 31 January 2024).

[84] G. Dance, M. LaForgia and N. Confessore, 'As Facebook Raised a Privacy Wall, It

from the digital-tech industry, but car manufacturers and media organisations are also among them.[85] These companies received even more data than Cambridge Analytica, including, for example, users' email addresses and phone numbers.[86] Netflix and Spotify were provided with private messages of some of Facebook's users.[87] Even if Facebook users had deactivated the sharing of data with third parties, companies had access to it.[88] As another example, Google broadcasts information about people's online behaviour to 1,042 companies and AT&T broadcasts information to 1,647 companies.[89] This happens every day, billions of times.[90] This practice, which is also carried out by numerous other companies, has been described as the 'world's biggest data breach'.[91]

Data sharing also came into the public spotlight when WhatsApp updated its privacy policy in January 2021. WhatsApp has been part of Facebook since 2014, a sale a former WhatsApp executive regrets because of Facebook's reliance on online advertising.[92] During its policy update in early 2021, particular attention was drawn to data sharing with other Facebook companies.[93] WhatsApp stated that it shared WhatsApp data with other Facebook companies to ensure the security and integrity of its products.[94] Some users were concerned that their data would be shared with Facebook inevitably and without choice from this point on. However, this had already been the case since WhatsApp's 2016 privacy policy update.[95] This update stipulated that WhatsApp shares data with other Facebook

---

Carved an Opening for Tech Giants', *The New York Times* (2018), https://www.nytimes.com/2018/12/18/technology/facebook-privacy.html (accessed 31 January 2024).

[85] Ibid.

[86] N. Confessore, M. LaForgia and G. Dance, 'Facebook's Data Sharing and Privacy Rules: 5 Takeaways From Our Investigations', *The New York Times* (2018), https://www.nytimes.com/2018/12/18/us/politics/facebook-data-sharing-deals.html (accessed 31 January 2024

[87] G. Dance, M. LaForgia and N. Confessore, 'As Facebook Raised a Privacy Wall, It Carved an Opening for Tech Giants' (*supra* Chapter III. note 84).

[88] N. Confessore, M. LaForgia and G. Dance, 'Facebook's Data Sharing and Privacy Rules: 5 Takeaways From Our Investigations' (*supra* Chapter III. note 86).

[89] Irish Council for Civil Liberties, *Landmark Litigation.*, 15 June 2021, https://www.iccl.ie/rtb-june-2021/#scale (accessed 31 January 2024).

[90] Ibid.

[91] Ibid.

[92] D. Seetharaman, 'Former Facebook, WhatsApp Employees Lead New Push to Fix Social Media', *The Wall Street Journal* (2022), https://www.wsj.com/articles/social-media-startups-take-aim-at-facebook-and-elon-musk-11651656600 (accessed 31 January 2024).

[93] See WhatsApp, *WhatsApp Privacy Policy*, 4 January 2021, https://www.whatsapp.com/legal/updates/privacy-policy-eea#CiIOqowf5JJ18ztWP (accessed 31 January 2024).

[94] Ibid.

[95] WhatsApp, *WhatsApp Privacy Policy,* 25 August 2016, https://www.whatsapp.com/legal/privacy-policy/revisions/20160825 (accessed 31 January 2024); L. Newman, 'WhatsApp Has Shared Your Data with Facebook for Years, Actually', *Wired* (2021), https://www.wired.com/story/whatsapp-facebook-data-share-notification/ (accessed 31 January 2024); S. Ovide, 'The Truth About your Whatsapp Data', *The New York Times* (2021), https://www.nytimes.com/2021/01/13/technology/whatsapp-data.html (accessed 31 January 2024).

companies.[96] This specific issue illustrates two things. Firstly, the intensive exchange of data within the companies that belong to Facebook. Secondly, that the awareness of data sharing and data protection has gained in importance in recent years, especially since there was not as much media coverage for the 2016 update as for the update in 2021.

Another aspect of extensive data sharing is that users can log into numerous websites with their Facebook account.[97] This has the advantage that they do not have to create a new, specific account and can also use existing usernames and passwords. As a logical consequence, Facebook can access the data collected when visiting these websites.[98] The potential negative consequences were highlighted by a data breach in 2018. The accounts of about 50 million Facebook users were compromised in a hacker attack.[99] This enabled the hackers to gain access not only to the personal information of the Facebook profiles, but also supposedly to all the personal data of the websites on which the affected users had logged in with their Facebook profile.[100]

Until 2018, Facebook also collaborated with one of the largest data broker companies called Acxiom.[101] Data brokers obtain and process information about individuals and sell it to third parties. They obtain this information through public records, online search behaviour, electoral registers, loyalty cards and publicly available data.[102] These third parties use this information for targeted marketing and personalised advertising. It is estimated that the data broker in-

---

[96] It reads as follows: 'As part of the Facebook family of companies, WhatsApp receives information from, and shares information with, this family of companies.', WhatsApp, *WhatsApp Privacy Policy*, 25 August 2016.

[97] Google or Twitter accounts can also often be used for this purpose.

[98] R. Shapiro and S. Aneja, 'Who Owns Americans' Personal Information and What Is It Worth?', *Future Majority* (2019), p. 8, https://assets.futuremajority.org/uploads/report-for-future-majority-on-the-value-of-people-s-personal-data-shapiro-aneja-march-8-2019.pdf (accessed 31 January 2024).

[99] M. Isaac and S. Frenkel, 'Facebook Security Breach Exposes Accounts of 50 Million Users', *The New York Times* (2018), https://www.nytimes.com/2018/09/28/technology/facebook-hack-data-breach.html?action=click&module=RelatedCoverage&pgtype=Article&region=Footer (accessed 31 January 2024).

[100] F. Manjoo, 'Why You Shouldn't Use Facebook to Log In to Other Sites', *The New York Times* (2018), https://www.nytimes.com/2018/10/02/technology/personaltech/facebook-log-in-hack.html (accessed 31 January 2024).

[101] D. Berger, 'Facebook beendet Zusammenarbeit mit Datenhändlern', *Heise Online* (2018), https://www.heise.de/newsticker/meldung/Facebook-beendet-Zusammenarbeit-mit-Datenhaendlern-4008444.html (accessed 31 January 2024).

[102] WebFX, *What Are Data Brokers – And What is Your Data Worth?*, 16 March 2020, https://www.webfx.com/blog/internet/what-are-data-brokers-and-what-is-your-data-worth-infographic/ (accessed 31 January 2024); Information Commissioner's Office, *Investigation into data protection compliance in the direct marketing data broking sector*, October 2020, https://ico.org.uk/media/action-weve-taken/2618470/investigation-into-data-protection-compliance-in-the-direct-marketing-data-broking-sector.pdf (accessed 31 January 2024).

dustry is worth up to $ 200 million US dollars.[103] It is not surprising that, in a similar way to Facebook, the use of personal data for marketing purposes is boosting the business of the data broker industry. Furthermore, companies in the data broker industry are competing with each other to find the best methods for classifying and generating knowledge about individuals and potential customers, further boosting the industry.[104]

According to Acxiom's homepage, the company has data on 2.5 billion people in over 60 countries and can provide up to 11,000 data attributes per person.[105] These numbers are impressive when one considers that in 2022, approximately 5 billion people were using the internet.[106] Therefore Acxiom processes the data of more than half of internet users worldwide. Here, too, the trend is upwards, given that Acxiom had data on 500 million users in 2012.[107]

Another data broker company, Experian, was investigated by the ICO, the United Kingdom's independent body to uphold information rights. The ICO looked at Experian's use of personal data for advertising purposes.[108] The investigation found that Experian held information on nearly 50 million adults in the United Kingdom, with more than 500 attributes connected to each identified person.[109] The ICO noted that this information was traded and enhanced without the awareness of the data subjects.[110] Because the data subjects did not know about this comprehensive handling of data sets and would not expect it (the ICO refers to 'invisible' processing in this context)[111], Experian violated the transparency requirement of Article 5 (1) (a) GDPR.[112] Similarly, Amazon leaked smart speaker data to advertisers and trackers.[113] Furthermore the actual data collec-

---

[103] D. Lazarus, 'Column: Shadowy data brokers make the most of their invisibility cloak', *Los Angeles Times* (2019), https://www.latimes.com/business/story/2019-11-05/column-data-brokers (accessed 31 January 2024).

[104] J. E. Cohen, 'The Inverse Relationship between Secrecy and Privacy' (*supra* Chapter III. note 58), p. 884.

[105] See Acxiom's homepage: https://www.acxiom.com (accessed 31 January 2024).

[106] S. Kemp, 'Digital 2022: Global Overview Report', *Datareportal* (2022), https://datareportal.com/reports/digital-2022-global-overview-report (accessed 31 January 2024).

[107] N. Singer, 'Mapping, and Sharing, The Consumer Genome', *The New York Times* (2012), https://www.nytimes.com/2012/06/17/technology/acxiom-the-quiet-giant-of-consumer-database-marketing.html?_r=0%20 (accessed 31 January 2024).

[108] See DataGuidance, *UK: ICO takes enforcement action against Experian after data broking investigation*, 28 October 2020, https://www.dataguidance.com/news/uk-ico-takes-enforcement-action-against-experian-after (accessed 31 January 2024).

[109] Information Commissioner's Office, *Enforcement notice to Experian Limited*, 27 October 2020, p. 12, https://ico.org.uk/action-weve-taken/enforcement/experian-limited/ (accessed 31 January 2024).

[110] DataGuidance, *UK: ICO takes enforcement action against Experian after data broking investigation* (*supra* Chapter III. note 108.

[111] Ibid.

[112] Information Commissioner's Office, *Enforcement notice to Experian Limited*, 27 October 2020, p. 16.

[113] U. Iqbal et al., *Your Echos are Heard: Tracking, Profiling, and Ad Targeting in the Amazon Smart Speaker Ecosystem* (*supra* Chapter III. note 65), p. 6.

tion and sharing practices are often not explicitly stated in their privacy policies.[114]

These examples illustrate that personal data usually does not stay with a single company, but is shared with others. Companies have agreements with other companies, notably data brokers. In this process, personal data are enhanced and enriched, usually without the knowledge of the data subjects.

c) Value of personal data to companies

The examples of Facebook and data broker companies illustrate how companies use, share and trade personal data.[115] Advertisers can make use of these profiles and place advertisements tailored to the users. Sharing the data with other companies also adds value. This approach is the norm in today's digital world and contributes to why almost all of today's most valuable companies are in the online industry and commodify personal data.

Facebook generates revenue through the fee that advertisers pay. These fees are not insignificant. Advertising revenue is the most important and also the largest part of the total revenue of the company. In 2021, approximately 98 % of Facebook's revenue came from advertising.[116] In total, advertising revenue accounted for just under $ 84.2 billion US dollars in 2020.[117] Advertising revenue in 2021 increased to $ 114.9 billion US dollars or 37 % compared to 2020.[118] These figures have been rising steadily for years, considering that advertising revenue was just under $ 3.1 billion US dollars in 2011.[119] Facebook has thus increased its advertising revenue more than twenty-fivefold in these 10 years.

Another noteworthy figure is the average revenue per user. This provides an estimate of how much the individual user is worth to Facebook. If one divides the total revenue generated in 2020 by the number of all Facebook users worldwide, one obtains the average revenue per user. In 2020, Facebook's average revenue per user stood at $ 27.51 US dollars.[120] Here, too, there has been a significant

---

[114] Ibid, p. 14.

[115] See already with other examples regarding the commodification of personal data, P.M. Schwartz, 'Property, Privacy, and Personal Data' (*supra* Chapter I. note 14), pp. 2060–2076.

[116] Facebook, *Annual Report*, 28 January 2021, p. 72, https://investor.fb.com/financials/default.aspx (accessed 31 January 2024); Dixon provides a minimally lower figure of 97,9 %, see S. Dixon, 'Facebook: advertising revenue worldwide 2009–2022', *Statista* (2023), https://www.statista.com/statistics/271258/facebooks-advertising-revenue-worldwide/ (accessed 31 January 2024).

[117] Facebook, *Annual Report*, 28 January 2021, p. 66; S. Dixon, 'Facebook: advertising revenue worldwide 2009–2022', *Statista* (2023) (*supra* Chapter III. note 116).

[118] Facebook, *Annual Report*, 3 February 2022, p. 65, https://investor.fb.com/financials/default.aspx (accessed 31 January 2024).

[119] S. Dixon, 'Facebook: advertising revenue worldwide 2009–2022' (*supra* Chapter III. note 116).

[120] Facebook, *Annual Report*, 28 January 2021, p. 60.

increase in recent years, as Facebook's average revenue per user was $ 5 US dollars in 2011.[121]

However, these figures are misleading insofar as the costs are included in revenue figures. Costs incurred for collecting, processing, analysing and marketing users' personal data are included in revenue figures. If one adds up the cost of sales, expenses for marketing, sales and administrative matters, one gets the relevant costs for personal data.[122] These amounted to $ 41.7 billion US dollars in 2020.[123] If this amount is subtracted from the generated advertising revenue, one gets the profit generated by personal advertising and thus by profiling personal data. From this, one can conclude that personal information of Facebook users is worth $ 42.5 billion US dollars, since Facebook collected this sum through the advertiser's fees. This is equivalent to a profit of $ 15.7 US dollars per user. However, users do not have a share in the profits, which raises the question of whether they should receive a digital dividend, especially since they are the basis for the revenue.[124]

These figures reiterate that monetisation of personal data is a major revenue generator for online companies such as Facebook.[125] In this regard, profiling has significant economic importance, as correct predictions can increase revenues and reduce risks of investments, for example.[126]

However, measuring the value of personal data on the basis of a company's revenue has its drawbacks. Revenue and profit of a company can have a significant impact on the perceived value of personal data.[127] Many other factors (e.g. economic situation, product development etc.) have an impact on revenue and can therefore affect the revenue per personal data and the associated value.[128] Furthermore, the personal data of an individual has a lower value for companies than the data sets of thousands of persons.[129]

---

[121] S. Dixon, 'Facebook: advertising revenue worldwide 2009–2022' (*supra* Chapter III. note 116).

[122] R. Shapiro, 'What Your Data Is Really Worth to Facebook', *Washington Monthly* (2019), https://washingtonmonthly.com/magazine/july-august-2019/what-your-data-is-really-worth-to-facebook/ (accessed 31 January 2024).

[123] Facebook, *Annual Report*, 28 January 2021, 28 January 2021, p. 65.

[124] H. Bolsinger, 'Wo bleibt die digitale Dividende für Europas Konsumenten?', 40 *DuD – Datenschutz und Datensicherheit* (2016), p. 382.

[125] R. Shapiro and S. Aneja, 'Who Owns Americans' Personal Information and What Is It Worth?', *Future Majority* (2019), p. 6.

[126] S. Ernst, 'IV. Profiling (Nr. 4)' (*supra* Chapter III. note 44), para. 39.

[127] G. Malgieri and B. Custers, 'Pricing privacy – the right to know the value of your personal data' (*supra* Chapter III. note 36), p. 296.

[128] OECD, *Exploring the Economics of Personal Data* (*supra* Chapter III. note 9), p. 24.

[129] G. Malgieri and B. Custers, 'Pricing privacy – the right to know the value of your personal data' (*supra* Chapter III. note 36), p. 295; OECD, *Exploring the Economics of Personal Data* (*supra* Chapter III. note 9), p. 25.

In summary, it can be stated that companies use personal data to create profiles. These data sets and profiles are often shared with other companies and enhanced and enriched with their data sets. These comprehensive data sets provide companies with information and profiles about individuals to display targeted, personalised advertising. Advertising is the main source of revenue for many major internet companies. Thus, personal data is an economic asset for these companies.

3. Market value of personal data

The previous section has shown that personal data is a multi-billion-dollar asset for companies. Thus, personal data are an economic asset and have value, regardless of what the law says.[130] Consequently, the question arises whether a concrete monetary value can be attached to personal data. It needs to be clarified whether personal data as defined in Chapter II., such as name, age profession, gender etc., have an independent monetary value. How much money would one receive for making one's address available? What price can be charged on the market for personal data?

These questions also interested Dutch student *Shawn Buckles*, who therefore organised an auction in which he wanted to sell his personal data to the highest bidder.[131] The highest bidder would receive *Shawn Buckles'* personal profile, location track records, train track records, personal calendar, email conversations, online conversations, 'thoughts', consumer preferences and browsing history.[132] The website 'The Next Web' was awarded the personal data after a successful bid of € 350.[133] *Shawn Buckles* told The Guardian that the website would use his personal information in order to raise awareness of privacy issues.[134] He added that he had received more money than he had expected, but had also revealed his most personal information in return.[135]

Shawn Buckles underlined that certain online services are not necessarily free because users do not have to pay money for them, especially since their identity is the means of payment.[136] Even if this auction is not representative, it reflects an everyday phenomenon: people are willing to spend money for personal data. Consequently, personal data can have a monetary value.[137]

---

[130] See also A.-A. Wandtke, 'Ökonomischer Wert von persönlichen Daten', 20 *MMR – Zeitschrift für IT-Recht und Recht der Digitalisierung* (2017), p. 8.

[131] Shawn Buckles*, Data for Sale*, https://shawnbuckles.nl/dataforsale/ (accessed 31 January 2024).

[132] Ibid.

[133] Ibid.

[134] B. Ehrenberg, 'How much is your personal data worth?' (*supra* Chapter III. note 36).

[135] Ibid.

[136] Shawn Buckles*, Data for Sale* (*supra* Chapter III. note 131).

[137] Costa-Cabral and Lynskey come to the same conclusion, as companies forego mon-

However, it is not possible to determine exactly how much individual data points such as a name or an address are worth. According to research by the Financial Times, these kinds of general personal information do not have a high monetary value.[138] The Financial Times came to this conclusion by evaluating the prices the data broker industry charges for selling personal data to third parties. Here, information of a single person such as name, age, place of residence is worth a fraction of a cent.[139] Information about people who are about to experience a significant life event, such as graduation, has a higher value.[140] People often change their consumption behaviour[141] or invest more money at these events and hence it is appealing for advertisers to gain information about these people and reach them with targeted ads.

Sensitive data is sold at a much higher price in comparison. Data brokers are willing to spend 26 cents per person to obtain information about health conditions, previous or future surgeries and medication.[142] A distressing, negative example is a company that offered a list of 1000 rape victims for $ 79 US dollars.[143] This is thought-provoking, but unfortunately not surprising and not a one-off. A US Senate report revealed that data brokers hold thousands of records, including information on visits to gynecologists over the past 12 months.[144] Furthermore, the user data of a gay-dating app was sold through advertising networks.[145] Through this user data, romantic encounters could be inferred.[146] A Catholic news outlet claimed that through this commercially available data, it was tracking app usage by individuals, leading to the resignation of a priest.[147] Moreover, a

---

etary payment to obtain personal data, see F. Costa-Cabral and O. Lynskey, 'Family ties: The intersection between data protection and competition in EU law' (*supra* Chapter II. note 4), p. 12.

[138] E. Steel, 'Financial worth of data comes in at under a penny a piece', *The Financial Times* (2013), https://www.ft.com/content/3cb056c6-d343-11e2-b3ff-00144feab7de (accessed 31 January 2024).

[139] Ibid.

[140] Ibid.

[141] Ibid.

[142] Ibid.

[143] E. Dwoskin, 'Data Broker Removes Rape-Victims List After Journal Inquiry', *The Wall Street Journal* (2013), https://www.wsj.com/articles/BL-DGB-31536 (accessed 31 January 2024).

[144] Committee on Commerce, Science, and Transportation*, A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes*, 18 December 2013, https://www.commerce.senate.gov/services/files/bd5dad8b-a9e8-4fe9-a2a7-b17f4798ee5a (accessed 31 January 2024).

[145] B. Tau and G. Wells, 'Grindr User Data Was Sold Through Ad Networks', *The Wall Street Journal* (2022), https://www.wsj.com/articles/grindr-user-data-has-been-for-sale-for-years-11651492800 (accessed 31 January 2024).

[146] Ibid.

[147] Ibid; NBCnews*, Priest outed via Grindr App highlights rampant data tracking*, 22 July 2021, https://www.nbcnews.com/tech/security/priest-outed-grindr-app-highlights-rampant-data-tracking-rcna1493 (accessed 31 January 2024).

data broker sold location data of people who visited an abortion clinic.[148] It cost $ 160 US dollars to get a week's worth of data on where people came from and where they went after visiting the abortion clinic.[149] Fertility and cycle tracking apps often share personal data with data brokers and advertisers, too.[150] This information could be used to prosecute people for terminating a pregnancy.[151]

According to the GDPR, sensitive data includes intimate information about political opinions, religious or ideological beliefs, health data, data about sexual life or sexual orientation.[152] With this information, one knows the most private and often also the most formative characteristics or events in a person's life. It is therefore a logical conclusion that in the data industry, which seeks to obtain as much insight as possible about people, this sensitive information is traded for more money. For the people concerned, this intimate and private information is certainly worth more than a few cents. However, as the examples above illustrate, this is unfortunately common practice in the data broker industry.

Using these common data broker industry prices, the Financial Times has provided an interactive calculator where one can determine the value of one's own data.[153] For the calculation, information can be provided in five categories: demographics, family and health, property, activities, consumer. Under demographics it is described that data brokers probably already know a person's age, gender, ZIP code, ethnicity and education level due to accessing public records.[154] After answering some questions about oneself, one gets the result of how much one's data would be worth to a data broker. The author's data would have an approximate market value of $ 0.80 US dollars. In various other imagined scenarios, from millionaire pensioner to young father, the data value remained below $ 1 US dollar.

When calculating prices using this interactive calculator, three aspects stand out: Information about health, fitness and any diseases adds significantly to the value of the data. The fact that health and fitness data is particularly valuable has also been shown with Amazon echo, as advertisers are willing to bid up to 30x higher to serve ads to people with these interests.[155] As mentioned above, data

---

[148] J. Cox, 'Data Broker Is Selling Location Data of People Who Visit Abortion Clinics', *Vice* (2022), https://www.vice.com/en/article/m7vzjb/location-data-abortion-clinics-safegraph-planned-parenthood (accessed 31 January 2024).

[149] Ibid.

[150] N. Wetsman, 'Cycle-tracking apps stand behind their privacy policies as Roe teeters', *The Verge* (2022), https://www.theverge.com/2022/5/6/23060000/period-apps-privacy-abortion-roe-supreme-court (accessed 31 January 2024).

[151] Ibid.

[152] See Article 9 GDPR.

[153] E. Steel et al., 'How much is your personal data worth?, *The Financial Times* (2013), http://ig-legacy.ft.com/content/927ca86e-d29b-11e2-88ed-00144feab7de#axzz70TwxUoqY (accessed 31 January 2024).

[154] Ibid.

[155] U. Iqbal et al., *Your Echos are Heard: Tracking, Profiling, and Ad Targeting in the Amazon Smart Speaker Ecosystem* (*supra* Chapter III. note 65), p. 11.

brokers are willing to pay more for sensitive data. The second aspect is that data from wealthy people are worth more.[156] Thus, it increases the value of the data if one states that one owns a house or cultivates hobbies such as flying or boating. Thirdly, the data of people with families is more valuable than the data of single people. This is particularly true if one has recently become a parent.

The results of the calculator raise the question of how the data broker industry can be a multi-million-dollar sector when the information is generally worth less than one dollar per person. The answer is quantity. It is typically not the data of a single targeted person that is traded. Data brokers usually sell datasets that include 1000 people.[157] For example, using the value of $ 0.80 US dollars calculated above, a dataset with information similar to the author's would cost $ 800 US dollars. When one considers that the data broker company Acxiom holds data on 2.5 billion people, the value of data to the data broker industry becomes even more apparent.

It should be noted that the merging of many individual pieces of information into large datasets does not make the individual pieces of information more valuable per se. There are complex data value metrics to determine whether appending, expanding or augmenting of information can contribute to the added value of personal data.[158] Some authors even suggest a nine-factor framework for data-based value creation.[159] Key activities within the data value chain include data acquisition, data analysis, data curation, data storage and data usage.[160] Due to this complexity and multi-layered nature, studies also show that many companies have vast amounts of data but do not know how to use it to create value.[161]

A different approach to measuring the value of personal data was taken by a company called Datacoup. The company paid up to $ 8 US dollars per month to individuals who disclosed social networking information, payment transactions and other personal data in exchange.[162] Datacoup then sold the analysed data to

---

[156] See also, L. Burgess et al., 'The Value of Personal Data in Iot : Industry Perspectives on Consumer Conceptions of Value', *Living in the Internet of Things* (2019), p. 5.

[157] E. Steel et al., 'How much is your personal data worth?' (*supra* Chapter III. note 153).

[158] See for example, M. Noshad et al., 'A data value metric for quantifying information content and utility', 8:82 *Journal of Big Data (*2021), pp. 1–23.

[159] See C. Lim et al., 'From data to value: A nine-factor framework for data-based value creation in information-intensive services' (*supra* Chapter III. note 22), pp. 121–135.

[160] E. Curry, 'The Big Data Value Chain: Definitions, Concepts, and Theoretical Approaches' in J. Cavanillas et al. (eds.) *New Horizons for a Data-Driven Economy* (Springer, 2020), p. 32.

[161] See R. Schüritz and G. Satzger, 'Patterns of Data-Infused Business Model Innovation', *IEEE 18th Conference on Business Informatics* (2018), pp. 133–142; B. H. Wixom and J.W. Ross, 'How to monetize your data', 58 *MIT Sloan Management Review* (2017), pp. 10–13.

[162] T. Simonite, 'Datacoup Wants to Buy Your Credit Card and Facebook Data', *MIT Technology Review* (2014), https://www.technologyreview.com/2014/09/08/171469/datacoup-wants-to-buy-your-credit-card-and-facebook-data/ (accessed 31 January 2024).

third parties.[163] A similar example is the Ipsos Screenwise Panel.[164] Here, people can apply to take part in a study for Google on how consumers use the internet, apps and television. Using a WIFI router provided free of charge, the participant's online behaviour is analysed. The people who take part in the study are remunerated for their participation, depending on the extent of their involvement. Participants of the study can receive $ 20 US dollars if one is selected for the study.[165] Participants receive $ 100 US dollars if they install the WIFI router provided.[166] In addition, one can earn $ 16 US dollars per month for each additional household member who connects to the WIFI router.[167] If major tech companies also followed this approach, individuals could participate in the exploitation of their personal data and receive some sort of digital dividend.[168] So far however, this remains a pipe dream.

The advantages of using market prices to attempt to calculate the value of personal data are that the prices are easy to obtain and reflect a real market situation.[169] Yet, this method neglects the different contexts in which personal data are offered and acquired.[170] *Malgieri* and *Custers* also point out that personal data often changes and can therefore become outdated.[171] Moreover, as personal data cannot be exhausted like other resources, they can be used or sold several times.[172] Therefore, market prices do not reflect the value of personal data as such, but rather the value of individual copies.[173]

---

[163] Ibid.

[164] See Ipsos Screenwise Panel, https://screenwisepanel.com/home (accessed 31 January 2024).

[165] Ibid.

[166] Ibid.

[167] Ibid.

[168] See H. Bolsinger, 'Wo bleibt die digitale Dividende für Europas Konsumenten?' (*supra* Chapter III. note 124), p. 382.

[169] OECD, *Exploring the Economics of Personal Data* (*supra* Chapter III. note 9), p. 26.

[170] G. Malgieri and B. Custers, 'Pricing privacy – the right to know the value of your personal data' (*supra* Chapter III. note 36), p. 296.

[171] Ibid.

[172] Ibid; F. Costa-Cabral and O. Lynskey, 'The Internal and External Constraints of Data Protection on Competition Law in the EU' (*supra* Chapter II. note 4), p. 11; N. Duch-Brown et al., 'The economics of ownership, access and trade in digital era', *JRC Digital Economy Working Paper* (2017), p. 12; J. Drexl, 'Designing Competitive Markets for Industrial Data – Between Propertisation and Access', 8 *JIPITEC – Journal of Intellectual Property, Information Technology and E-Commerce Law* (2017), p. 281; S. Spiekermann et al., 'The challenges of personal data markets and privacy', 25 *Electronic Markets* (2015), p. 162.

[173] OECD, *Exploring the Economics of Personal Data* (*supra* Chapter III. note 9), p. 25.

4. Illegal markets and data breaches as proxy for value

Another marketplace, albeit not a legal one, for determining the value of personal data is the dark web. The company Privacy Affairs publishes an annual Dark Web Price Index.[174] This index is intended to illustrate how much data is worth on the dark web and why data is a valuable commodity. According to this index, hacked credit card details with CVV are sold on average between $10 and $ 30 US dollars depending on the country.[175] Compromised crypto accounts are priced much higher at up to $ 2,650 US dollars and are among the most valuable items on the list.[176] Hacked social media accounts are being sold ranging from Twitter accounts for $ 20 US dollars to Gmail accounts for $ 60 US dollars.[177] By far the most expensive are forged physical travel documents, with EU passports selling for an average of $ 3,000 US dollars on the dark web.[178] All in all, $1,010 US dollars could be enough to take another person's identity.[179]

Even if the dark web is not a legal marketplace for data trading, it is still a reality and should not be completely disregarded when assessing the value of personal data. Certainly, the prices are extremely high due to the illegality, but they nevertheless reflect the fact that people are willing to spend this money for personal data. In addition, the index shows in a year-on-year comparison that the dark web is not getting smaller, but on the contrary, more and more information is being offered and the prices are also rising.[180] The noteworthy decline in pricing over a span of three years suggests that an increasing number of individuals are becoming targets of cybercriminal activities.[181]

Often, personal information ends up on the dark web due to a data breach. The data breach itself also provides a way to determine the value of the personal data by assessing the cost and fine for the data breach. According to IBM's 2023 Cost of a Data Breach Report, a data breach cost the affected company an average of $ 4.45 million US dollars.[182] There are, of course, also data breaches that are above the cost average. For example, the ICO fined British Airways 20 million pounds for a data breach.[183] The data of more than 400,000 customers

---

[174] See Privacy Affairs, https://www.privacyaffairs.com/tools-and-research/ (accessed 31 January 2024).

[175] M. Zoltan, 'Dark Web Price Index 2023', *Privacy Affairs* (2023), https://www.privacyaffairs.com/dark-web-price-index-2023/ (accessed 31 January 2024).

[176] Ibid.

[177] Ibid.

[178] Ibid.

[179] E. Woollacott, 'What are You Worth on the Dark Web?', *Forbes* (2021), https://www.forbes.com/sites/emmawoollacott/2021/03/09/what-are-you-worth-on-the-dark-web/?sh=6c77af73cbca (accessed 31 January 2024).

[180] M. Zoltan, 'Dark Web Price Index 2023' (*supra* Chapter III. note 175).

[181] Ibid.

[182] IBM, *How much does a data breach cost?,* https://www.ibm.com/security/data-breach (accessed 31 January 2024).

[183] BBC, *British Airways fined 20 million pounds over data breach*, 16 October 2020 https://www.bbc.com/news/technology-54568784 (accessed 31 January 2024).

were exposed in the wake of a cyber-attack.[184] The compromised data included names, addresses, payment card numbers, CVV numbers, usernames and passwords of employees and administrator accounts.[185] This data breach would cost British Airways 50 pounds per affected customer.

Another example is the 2017 Equifax data breach that exposed the personal data of 147 million people.[186] The company pledged up to $ 245 million US dollars to help people affected by the data breach.[187] Individuals could receive compensation for time spent recovering from identity theft or fraud of up to $ 25 US dollars per hour for up to 20 hours.[188] Facebook received the highest penalty to date following a data breach. Facebook was fined $ 5 billion US dollars in the aftermath of the *Cambridge Analytica scandal*.[189] This data breach would cost Facebook roughly $ 57 US dollars per affected user.

These figures certainly do not reflect the concrete monetary value of personal data per se, especially since numerous other circumstances are considered in the assessment of fines. For example, the ICO stated that the cyber-attack could affect individuals' lives and lead to anxiety and stress and that these conditions were taken into account in the fine calculation.[190] However, these considerations reflect a value that has not been taken into account so far, the (emotional) value of the data to the individuals concerned.

These two value calculations, illegal market prices and data breach fines, also have advantages and disadvantages. Data prices in illegal markets reflect a real market value.[191] However, the personal data is typically overvalued because criminals also factor the risk of detection and prosecution into the price.[192] The cost of a data breach also has the advantage of providing a market price.[193] The disadvantages of this method include that there is not necessarily a correlation between the cost of a data breach and the value of personal data.[194] As mentioned above, there are many factors that contribute to the cost of a data breach.

---

[184] Ibid.

[185] Ibid.

[186] Federal Trade Commission, *Equifax Data Breach Settlement*, February 2022, https://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement (accessed 31 January 2024).

[187] Ibid.

[188] Ibid.

[189] Federal Trade Commission, *FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook*, 24 July 2019, https://www.ftc.gov/news-events/news/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions-facebook (accessed 31 January 2024).

[190] BBC, *British Airways fined 20 million pounds over data breach* (*supra* Chapter III. note 183).

[191] OECD, *Exploring the Economics of Personal Data* (*supra* Chapter III. note 9), p. 28.

[192] Ibid, p. 29.

[193] Ibid, p. 20.

[194] F. Malgieri and B. Custers, 'Pricing privacy – the right to know the value of your personal data' (*supra* Chapter III. note 36), p. 296.

5. Empirical studies on the value of personal data

One approach to calculating the value of personal data to data subjects is to conduct surveys and experiments on how much people need to be paid to disclose their data.

There are numerous experiments and surveys in the literature on the question of how individuals value their personal data. Even if this question will result in a context-dependent and unprecise answer, the OECD writes in a report from 2013 that two general conclusions can be drawn from the research.[195] First, individuals appear to differ with regard to their own valuation of personal data (i.e. sum of money adequate for them to share personal data) and their own valuation of privacy (i.e. adequate sum of money they are willing to spend to safeguard their personal data from exposure).[196] Second, these individual valuations are context-dependent and hence cannot be assessed with exact accuracy and precision.[197]

One exemplary study is a conjoint analysis exercise in which *Hann et al.* presented 268 participants of an experiment with trade-off scenarios in which an organisation may either provide privacy protection or certain rewards when registering with a website.[198] The study aimed to identify the driving motivational factors, including privacy or monetary compensation, that lead individuals to sign up to a website.[199] They found that privacy safeguards are correlated with positive attitudes towards a website and that financial benefits and other advantages may considerably boost people's willingness to visit a website.[200] According to the study, benefits have a substantial impact on people's preferences over websites, regardless of privacy policies.[201] Furthermore, the value of website privacy protection among US subjects is worth approximately $ 30 US dollars to $ 45 US dollars.[202] Another finding of this study is that the participants can be divided into three groups. The majority of the participants were concerned about internet information privacy.[203] In comparison, a smaller percentage were prepared to reveal personal information in exchange for money and an even smaller

---

[195] OECD, *Exploring the Economics of Personal Data* (*supra* Chapter III. note 9), p. 30.

[196] Ibid.

[197] Ibid; see also, F. Costa-Cabral and O. Lynskey, 'The Internal and External Constraints of Data Protection Law in the EU' (*supra* Chapter II. note 4), p. 11; D. Nguyen and M. Paczos, 'Measuring the economic value of data and cross-border data flows – A business perspective', 297 *OECD Digital Economy Papers* (2020), p. 37; A. Wagner et al., 'Putting a Price Tag on Personal Information – A Literature Review', *Proceedings of the 51st Hawaii International Conference on System Sciences* (2018), p. 3766.

[198] See I. Hann et al., 'Overcoming Online Information Privacy Concerns: An Information-Processing Theory Approach', 24 *Journal of Management Information Systems* (2007), pp. 13–42.

[199] Ibid, p. 19.

[200] Ibid, p. 27.

[201] Ibid, p. 28.

[202] Ibid, p. 29.

[203] Ibid, p. 33.

percentage were ready to offer personal information in exchange for convenience.[204]

This study illustrates that the valuation of personal data and privacy can vary. Financial incentives play a significant role and illustrate that people are generally willing to receive money in exchange for their data. *Acquisti et al.* concluded that more people would provide their data in exchange for money than would spend money on privacy protections.[205] In other words, more people would accept money and have their internet activity monitored than would spend money to have that internet activity anonymised. This is similar to the phenomenon of people demanding more money for an asset than they themselves would be willing to spend on it.[206]

In another study on measuring the value of personal data, *Huberman et al.* held a fictitious auction with 127 people.[207] People could bid for information on age and weight, with the lowest bid winning. The average auction value was $ 57.56 US dollars for age and $ 74.06 US dollars for weight.[208] This price difference may indicate that weight is perceived by individuals as more intimate information than age and is therefore valued more highly.[209] The desirability of the characteristic plays a significant factor in the price evaluation. Participants in the study who weighed too much according to the Body Mass Index charged proportionately more for providing this information, possibly out of concern for stigmatisation.[210] Consequently, *Huberman et al.* conclude that the more undesirable the trait, the higher the price for disclosure.[211]

Regarding location data, participants in another experiment stated that they would request € 43 to provide this information.[212] Significantly less was demanded in another experiment with € 8 for home location data and € 5.4 for work location.[213] In a different study, 60 people were given smartphones for a period of

---

[204] Ibid.

[205] A. Acquisti et al., 'What is Privacy Worth?', 42 *The Journal of Legal Studies* (2013), p. 267; the gap between willingness-to-accept and willingness-to-protect was also examined in J. Grossklags and A. Acquisti, 'When 25 Cents is too much: An Experiment on Willingness-To-Sell and Willingness-To-Protect Personal Information', *Proceedings of the Workshop on the Economics of Information Security* (2007).

[206] S. Spiekermann and J. Korunovska, 'Towards a value theory for personal data', 32 *Journal of Information Technology* (2017), p. 71.

[207] B. Huberman, E. Adar and L. Fine, 'Valuating Privacy', 3 *IEEE Security and Privacy Magazine* (2005), pp. 22–25.

[208] Ibid, p. 24.

[209] Ibid.

[210] Ibid, p. 23.

[211] Ibid, p. 22.

[212] D. Cvrcek et al., 'A study on the value of location privacy', *Proceedings of the 2006 ACM Workshop on Privacy in the Electronic Society* (2006), p. 10.

[213] O. Barak et al., 'The price is right?: economic value of location sharing', *Proceedings of the 2013 ACM conference on Pervasive and ubiquitous computing adjunct publication* (2013), p. 897.

6 weeks that both recorded location, communication, application and media data and gave the possibility to auction off this data.[214] As with *Huberman et al.*, the lowest bid in this study won. On average, participants demanded between € 1 and € 2 per day for tracking their location data.[215] Of the four categories of information recorded, location data was ranked the most valuable.[216] In addition, participants trusted themselves the most with the handling of their data and information from atypical days received higher bids than information from typical days.[217] This is consistent with the point made above that data from special events is worth more than data from everyday occurrences.

Carrascal et al. conducted a study over a period of two weeks in which 168 participants were able to auction their data.[218] Here, too, the lowest bid received the award. Study participants valued their offline data (age, gender, address etc.) at around € 25.[219] Internet browsing history was auctioned at a significantly lower price of € 7.[220] The majority of individuals demanded more for the disclosure of social media activity and online financial services than for search history and online shopping.[221] In addition, the study found that people preferred money or additional services over free services and customised ads.[222] In this study too, participants trusted themselves the most with the handling of their personal data.[223]

In a further study, 218 participants were again able to auction off their data.[224] The personal data were divided into four categories: Identifiers (e.g. full name, phone number, email address, home address), Quasi-Identifiers (e.g. date of birth, zip code), Demographics (e.g. age, gender, ethnicity, marital status, education, occupation) and Private (e.g. income, credit scores).[225] The study participants bid an average of $ 30 US dollars for weight data, $ 75 US dollars for

---

[214] J. Staiano et al., 'Money Walks: A Human-Centric Study on the Economics of Personal Mobile Data', *Proceedings of the 2014 ACM Conference on Ubiquitous Computing* (2014), p. 8.

[215] Ibid, p. 8.

[216] Ibid, p. 10.

[217] Ibid.

[218] J. Carrascal et al., 'Your browsing behavior for a Big Mac: Economics of personal information online', *Proceedings of the 22nd International Conference on World Wide Web* (2011), pp. 189–200.

[219] Ibid, p. 194.

[220] Ibid.

[221] Ibid, p. 196.

[222] Ibid, p. 195; a similar result was found by *Morey et al.,* T. Morey et al., 'Customer Data: Designing for Transparency and Trust', 93 *Harvard business review* (2015), p. 101.

[223] J. Carrascal et al., 'Your browsing behavior for a Big Mac: Economics of personal information online' (*supra* Chapter III. note 218), p. 197.

[224] X. Li et al, 'Valuing Personal Data with Privacy Consideration', 52 *Decision Sciences* (2021), pp. 393–426.

[225] Ibid, p. 399.

medical data and $ 100 US dollars for tax data.[226] Even though the price valuations varied greatly in this experiment, it is evident that private, sensitive information is considered the most valuable, especially since many people did not provide complete data in this fourth category.[227] It should also be emphasised that people who did not provide certain data rated them significantly higher than people who did.[228] It can therefore be argued that people who are more conscious of privacy and data protection value their data more highly.[229]

It clearly results from the studies presented in this section that the category of data is important for the valuation.[230] Sensitive data are deemed to be particularly valuable.[231] Special events and unusual traits are also highly valued. In addition, people who have privacy concerns tend to price their data accordingly. Trust is another important factor that makes people more likely to share their personal data.[232] In addition, people are more inclined to share their data if they have the right to be forgotten.[233]

Besides these essential value indicators, *Spiekermann* and *Korunovska* consider two other indicators. In a survey experiment, 1269 Facebook users were asked how they would value their personal data. The first indicator is awareness of the asset. Once the respondents became aware that their personal data could and would be traded, their valuation of the data increased significantly.[234] The second indicator is psychological ownership. Data was valued more highly when it was seen as one's own property.[235] In particular, identifying with the data, sharing it

[226] Ibid, p. 408

[227] Ibid.

[228] Ibid, p. 419.

[229] S. Spiekermann and J. Korunovska, 'Towards a value theory for personal data' (*supra* Chapter III. note 206), p. 73; I. Hann et al., 'Overcoming Online Information Privacy Concerns: An Information-Processing Theory Approach' (*supra* Chapter III. note 198), p. 30; B. Huberman, E. Adar and L. Fine, 'Valuating Privacy' (*supra* Chapter III. note 207), p. 24; D. Cvrcek et al., 'A study on the value of location privacy' (*supra* Chapter III. note 212), p. 6; A. Wagner et al., 'Putting a Price Tag on Personal Information – A Literature Review' (*supra* Chapter III. note 197), p. 3766.

[230] See also, B. Roeber et al., 'Personal data: how context shapes consumer's data sharing with organizations from various sectors', 25 *Electronic Markets* (2015), p. 101.

[231] A. Wagner et al., 'Putting a Price Tag on Personal Information – A Literature Review' (*supra* Chapter III. note 197), p. 3766.

[232] T. Morey et al., 'Customer Data: Designing for Transparency and Trust' (*supra* Chapter III. note 222), p. 102; B. Roeber et al., 'Personal data: how context shapes consumer's data sharing with organizations from various sectors' (*supra* Chapter III. note 230), p. 103; S. Spiekermann et al., 'The challenges of personal data markets and privacy' (*supra* Chapter III. note 172), p. 165.

[233] B. Roeber et al., 'Personal data: how context shapes consumer's data sharing with organizations from various sectors' (*supra* Chapter III. note 230), p. 105.

[234] S. Spiekermann and J. Korunovska, 'Towards a value theory for personal data' (*supra* Chapter III. note 206), p. 72.

[235] Ibid, p. 74.

with friends and seeing Facebook as home, so to speak, were decisive for higher prices.[236]

However, as already mentioned above, these results of the valuation of personal data and privacy are significantly dependent on their context. The level of valuation depends not only on the category of data, but also on the country from which the person comes from.[237] For example, the same data categories are valued differently in China, India, the USA, Germany and the United Kingdom, with Germans viewing their personal data as most valuable and people from China and India ascribing the least value.[238] *Morey et al.* consider the cultural conditions to be decisive for these differences in valuation.[239] They argue that China and India are more collectivistic and hierarchical than Germany, the USA and the United Kingdom, whose societies are individualistic and thus also assign a high value to personal, individual data.[240] While there is some merit to this argument, in my opinion the affinity with privacy issues is more decisive. Individuals that are less privacy conscious for a variety of reasons (e.g. political system, national legislation) attach less importance to personal data than individuals that are more concerned about the protection of personal data and their privacy.[241]

Demographic attributes also need to be considered in context. Women usually are more privacy conscious and demand more for their personal data than men.[242] Older people are more cautious in handling their personal data than younger

---

[236] Ibid.

[237] See J. Carrascal et al., who argue that the differences between results may stem from cultural differences, J. Carrascal et al., 'Your browsing behavior for a Big Mac: Economics of personal information online' (*supra* Chapter III. note 218), p. 197; D. Cvrcek et al., 'A study on the value of location privacy' (*supra* Chapter III. note 212), p. 5.

[238] T. Morey et al., 'Customer Data: Designing for Transparency and Trust' (*supra* Chapter III. note 222), p. 100.

[239] Ibid.

[240] Ibid.

[241] See D. Cvrcek et al., 'A study on the value of location privacy' (*supra* Chapter III. note 212), pp. 5–6, who came to a similar conclusion; S. Preibusch, D. Kübler and A. R. Beresford, 'Price versus privacy: an experiment into the competitive advantage of collecting less personal information', 13 *Electronic Commerce Research* (2013), p. 452.

[242] X. Li et al, 'Valuing Personal Data with Privacy Consideration' (*supra* Chapter III. note 224), p. 412; M. Rowan and J. Dehlinger, 'Observed gender differences in privacy concerns and behaviors of mobile device end users', 37 *Procedia Computer Science* (2014), p. 346; M. G. Hoy and G. Milne, 'Gender Differences in Privacy-Related Measures for Young Adult Facebook Users', 10 *Journal of Interactive Advertising* (2010), p. 41; B. Huberman, E. Adar and L. Fine, 'Valuating Privacy' (*supra* Chapter III. note 207), p. 24; however, Y.J. Park found that men have better technical data protection measures than women, see Y.J. Park, 'Do men and women differ in privacy? Gendered privacy and (in)equality in the Internet', 50 *Computers in Human Behavior* (2015); *Carrascal et al.* found that men charged more for their email address than women, see J. Carrascal et al., 'Your browsing behavior for a Big Mac: Economics of personal information online' (*supra* Chapter III. note 218), p. 195.

people.[243] Depending on which participants a study group comprises, the outcome can be influenced.[244]

A particularly striking example of the importance of context is a 2004 survey of office workers at a London railway station as part of the Infosecurity Europe 2004.[245] In this survey, 71 % of people were willing to give up their email password in exchange for a bar of chocolate.[246] The value of email addresses here falls short of that measured by other studies. But this was a social engineering exercise and meant to raise awareness about privacy, which was repeated in the following years.[247] This value is therefore not to be given much attention, but it illustrates the importance of context when calculating the value of personal data.

Studies and experiments encourage people to state the value of their personal data themselves. These studies provide the value from the perspective of the data subject and thus from an essential angle. In addition, these studies are comparable and replicable, as the settings of the experiments allow them to be repeated with different groups and in different countries and contexts, and there are thus numerous comparative studies.[248] The auction model is an effective tool because of the exchange of money and personal data and the resulting ease of measurement in a currency.[249]

A significant disadvantage of relying on survey results as a standard for valuing personal data is the failure to provide a market validation.[250] As a matter of fact, these surveys indicate the hypothetical and speculative value of personal

---

[243] X. Li et al, 'Valuing Personal Data with Privacy Consideration' (*supra* Chapter III. note 224), p. 412; A. Goldfarb and C. Tucker, 'Shifts in Privacy Concerns', 102 *American Economic Review* (2012), p. 350; B. Huberman, E. Adar and L. Fine, 'Valuating Privacy' (*supra* Chapter III. note 207), p. 24; I. Hann et al., 'Overcoming Online Information Privacy Concerns: An Information-Processing Theory Approach' (*supra* Chapter III. note 198), p. 34; M. Walrave at al., 'Connecting and protecting? Comparing predictors of self-disclosure and privacy setting use between adolescents and adults', 6 *Cyberpsychology: Journal of Psychosocial Research on Cyberspace* (2012), https://cyberpsychology.eu/article/view/4259/3297 (accessed 31 January 2024); contrary to this, Carrascal et al. found that older people bid less for their photos online, ee J. Carrascal et al., 'Your browsing behavior for a Big Mac: Economics of personal information online' (*supra* Chapter III. note 218), p. 195.

[244] A. Wagner et al., 'Putting a Price Tag on Personal Information – A Literature Review' (*supra* Chapter III. note 197), p. 3766.

[245] See Help Net Security, *Office Workers Give Away Passwords for a Chocolate Bar*, 20 April 2004, https://www.helpnetsecurity.com/2004/04/20/office-workers-give-away-passwords-for-a-chocolate-bar/ (accessed 31 January 2024).

[246] Ibid.

[247] J. Schofield, 'Woman 4 times more likely than men to give passwords for chocolate', *The Guardian* (2008), https://www.theguardian.com/technology/blog/2008/apr/16/woman4timesmorelikelythan (accessed 31 January 2024).

[248] See OECD, *Exploring the Economics of Personal Data* (*supra* Chapter III. note 9), pp. 30–31.

[249] See X. Li et al, 'Valuing Personal Data with Privacy Consideration' (*supra* Chapter III. note 224), p. 397.

[250] OECD, *Exploring the Economics of Personal Data* (*supra* Chapter III. note 9), p. 32.

data as stated by data subjects, without representing an actual market value.[251] *Li et al.* criticise studies in which personal data is not actually exchanged for money, as there is typically a strong discrepancy between fictitious and real values.[252]

Another downside is that these studies, as already described in detail, lead to a wide variety of results due to the context.[253] People value their personal data differently depending on their country and age but also depending on their trust in the other party and the third parties with whom the data is shared.[254]

6. Valuation based on willingness to pay to protect personal data

An additional approach to measuring the value of personal data is to examine how much money people spend or are willing to spend on protecting their data. Some companies offer the protection of privacy in return for money. These offers can be used to analyse the value of personal data.

In a study from New Zealand, 47 % of respondents said they would be willing to pay money to protect their privacy.[255] On average, people were willing to pay $ 28.25 US dollars for the protection of their privacy.[256] A similar figure was obtained by *Hann et al.*, in the study described above, in which participants were willing to spend between $ 30 US dollars and $ 45 US dollars for privacy protection.[257]

In another experiment with 47 participants, questions were asked about personal information (test performance, weight, favourite holiday destination and number of sexual partners).[258] They were then asked how much they would be willing to pay to avoid having their answers read out in front of the other participants.[259] On average, people were willing to pay $ 0.8 US dollars to protect their

---

[251] Ibid; V. Benndorf and H.-T. Normann, 'The Willingness to Sell Personal Data', 120 *The Scandinavian Journal of Economics* (2018), p. 1276.

[252] X. Li et al, 'Valuing Personal Data with Privacy Consideration' (*supra* Chapter III. note 224), p. 397; see also, A. Wagner et al., 'Putting a Price Tag on Personal Information – A Literature Review' (*supra* Chapter III. note 197), p. 3766.

[253] OECD, *Exploring the Economics of Personal Data* (*supra* Chapter III. note 9), p. 32.

[254] This is highlighted in particular by T. Morey et al., 'Customer Data: Designing for Transparency and Trust' (*supra* Chapter III. note 222), pp. 96–107.

[255] E. Rose, 'Data Users versus Data Subjects: Are Consumers Willing to Pay for Property Rights to Personal Information?', *Proceedings of the 38th Annual Hawaii International Conference on System Sciences* (2005), p. 6.

[256] Ibid, p. 7.

[257] See I. Hann et al., 'Overcoming Online Information Privacy Concerns: An Information-Processing Theory Approach' (*supra* Chapter III. note 198), p. 29.

[258] J. Grossklags and A. Acquisti, 'When 25 Cents is too much: An Experiment on Willingness-To-Sell and Willingness-To-Protect Personal Information' (*supra* Chapter III. note 205), p. 11.

[259] Ibid, p. 10.

test results and $ 0.8 US dollars to protect their weight data.[260] Moreover, they would have spent $ 0.0 US dollars for their favourite holiday destination and $ 12.1 US dollars for the number of sexual partners in order to prevent them from being read out in front of the other participants.[261] The example of weight data illustrates the difference between willingness to accept and willingness to protect. In the *Huberman et al.* experiment mentioned above, participants asked for an average of $ 74,06 US dollars to sell their weight data. In this study, they were only willing to spend less than one dollar to protect the weight data from third parties.

160 internet users were asked by *Schreiner et al.* about their willingness to pay for privacy.[262] Here, a 'freemium model' was analysed, which allows users to use the free version of an online service or to get additional privacy options against payment of a monthly rate.[263] As a result, it was found that Facebook users would be willing to pay € 1.67 and Google users between € 1 and € 1.5 per month for a more privacy-friendly service.[264] The larger the Facebook network, the higher the willingness to pay.[265] In another study conducted by *Schreiner et al.,* the average was € 0.63.[266] With this 'freemium model', users are especially willing to pay for privacy if the paid service is considered useful and trustworthy.[267] *Krasnova et al.* concluded that users would be willing to pay between € 1.2 and € 1.4 for a privacy-enhanced online social network.[268] People are generally willing to choose the more privacy-friendly option when all other factors are equal.[269]

---

[260] Ibid, p. 13.

[261] Ibid, p. 13.

[262] See M. Schreiner et al., 'On The Willingness To Pay For Privacy As A Freemium Model: First Empirical Evidence', *Proceedings of the 21st European Conference on Information Systems* (2013).

[263] Ibid, p. 2.

[264] Ibid, p. 6.

[265] C. Bauer, J. Korunovska, S. Spiekermann, 'On the Value of Information – What Facebook Users are Willing to Pay', *Proceedings of the 20th European Conference on Information Systems* (2012), p. 10.

[266] M. Schreiner and T. Hess, 'Why Are Consumers Willing to Pay for Privacy? An Application of the Privacy-freemium Model to Media Companies', *Proceedings of the 23rd European Conference on Information Systems* (2015), p. 9.

[267] Ibid, p. 12.

[268] H. Krasnova et al., 'Investigating the Value of Privacy in Online Social Networks: Conjoint Analysis', *Proceedings of the 30th International Conference on Information Systems* (2009), p. 15.

[269] ENISA – European Network and Information Security Agency, *Study on monetizing privacy – An economic model for pricing personal information*, 28 February 2021, p. 35; S. Preibusch, 'The Value of Web Search Privacy', 13 *IEEE Security & Privacy* (2015), p. 29; the contrary result was found by S. S. Preibusch, D. Kübler and A. R. Beresford, 'Price versus privacy: an experiment into the competitive advantage of collecting less personal information' (*supra* Chapter III. note 241), p. 444.

In *Acquisti's* experiment on willingness to pay for privacy, 349 participants were given one of two sets of gift cards.[270] The first one was a $ 12 US dollars gift card that was not anonymised and shared personal information.[271] The second one was a $ 10 US dollars gift card that was anonymised and did not share personal information.[272] When given the choice to switch to another card, less than 10 % of participants changed from the $ 12 US dollars gift card to the $ 10 US dollars gift card to protect their personal information.[273] Thus, $ 2 US dollars was too expensive to protect their privacy.[274]

The prices to pay for privacy differ in these studies. Different prices could come from different definitions of privacy.[275] The willingness to pay to protect privacy in the latter studies is low. However, this does not mean that individuals do not value their personal data.[276] In reality, individuals are indeed willing to spend money for the protection of their privacy. This conclusion can be reached by looking at the numerous privacy insurance offers on the market. The following paragraphs provide examples of such offers.

The willingness to pay for privacy can be observed in insurance policies that include identity theft protection.[277] Data breach insurance is becoming increasingly popular and can be used as a means to measure the value of personal data, as insurance companies themselves determine the value of personal data for their insurance premiums.[278] Remarkably, *Experian*, the company that trades personal data without the knowledge of the data subjects, offers identity theft protection with its 'IdentityWorks' insurance plan.[279] This insurance plan offers Dark Web monitoring, which checks whether information has been stolen and is being sold on the Dark Web.[280] In addition, one will be notified if a sex offender moves into the neighbourhood.[281] Moreover, one will be warned in case someone tries to access one's social security number or credit card in an unauthorised way.[282] The

---

[270] See A. Acquisti et al., 'What is Privacy Worth?' (*supra* Chapter III. note 205), pp. 249–274.

[271] Ibid, p. 260.

[272] Ibid.

[273] Ibid, p. 267

[274] Ibid.

[275] A. Wagner et al., 'Putting a Price Tag on Personal Information – A Literature Review' (*supra* Chapter III. note 197), p. 3764.

[276] See J. Grossklags and A. Acquisti, 'When 25 Cents is too much: An Experiment on Willingness-To-Sell and Willingness-To-Protect Personal Information' (*supra* Chapter III. note 205), p. 15.

[277] OECD, *Exploring the Economics of Personal Data* (*supra* Chapter III. note 9), p. 32.

[278] D. Nguyen and M. Paczos, 'Measuring the economic value of data and cross-border data flows – A business perspective' (*supra* Chapter III. note 197), p. 32.

[279] See Experian Identity Theft Protection, https://www.experian.com/consumer-products/identity-theft-and-credit-protection.html (accessed 31 January 2024).

[280] Ibid.

[281] Ibid.

[282] Ibid.

basic insurance plan costs $ 24.99 US dollars per month.[283] A similar service is offered by Norton's Lifelock, which also costs just under $ 100 US dollars per year.[284]

People are also willing to buy the app 'Jumbo Privacy' to protect their privacy. Jumbo offers a kind of central privacy assistant for smartphones, where the privacy settings of Facebook, Google, Youtube etc. can be adjusted.[285] In order to be able to edit the privacy settings of additional apps such as Instagram or LinkedIn, the fee-based version of Jumbo must be downloaded.[286] For this version, one can pay between $ 0 and $ 14.99 US dollars depending on 'what you think is fair'.[287] By summer 2020, 15 % of users had already switched to the subscription-based version.[288] Jumbo's CEO explained this by claiming that people trust a subscription-based service more because they know that Jumbo does not need to monetise user data to make money.[289] Jumbo is trying to gain customers who, in the wake of data protection scandals, are becoming aware that 'if you're not paying for a product, you are the product'.[290]

In the market of paying for privacy, there are also anti-tracking software solutions. The company Avast offers anti-tracking software designed to block trackers that collect and share data by encrypting online identity and activity.[291] This is to avoid targeted advertising and price manipulation.[292] This anti-tracking software costs $ 54.99 US dollars per year.[293] However, Avast made headlines at the beginning of 2020 when it was revealed that a subsidiary had sold user data to companies including Google, Microsoft and Pepsi.[294] This implies that data from

---

[283] Ibid.

[284] See NortonLifeLock, https://www.nortonlifelock.com/us/en/ (accessed 31 January 2024).

[285] D. Ingram, 'Privacy is a right, but it may not be free. How does $3 a month sound?', *NBCNews* (2020), https://www.nbcnews.com/tech/security/privacy-right-it-may-not-be-free-how-does-3-n1184291 (accessed 31 January 2024).

[286] C. Summerson, 'Jumbo Privacy is the Only App You Need to Protect Your Online Info', *ReviewGeek* (2021), https://www.reviewgeek.com/65253/jumbo-privacy-is-the-only-app-you-need-to-protect-your-online-info/ (accessed 31 January 2024).

[287] See Jumbo*, Jumbo 2: A step closer to our vision*, 24 June 2020, https://blog.jumboprivacy.com/jumbo-2.0-a-step-closer-to-our-vision.html (accessed 31 January 2024).

[288] I. A. Hamilton, 'Mark Zuckerberg's former mentor has invested in privacy app Jumbo, which helps you mass delete old social media posts', *Business Insider* (2020), https://www.businessinsider.com/privacy-app-jumbo-raises-8-million-series-a-2020-6 (accessed 31 January 2024).

[289] Ibid.

[290] Ibid.

[291] See Avast Antitrack, https://www.avast.com/en-us/antitrack#mac (accessed 31 January 2024).

[292] Ibid.

[293] Ibid.

[294] J. Cox, 'Leaked Documents Expose the Secretive Market for Your Web Browsing Data', *Vice* (2020), https://www.vice.com/en/article/qjdkq7/avast-antivirus-sells-user-browsing-data-investigation (accessed 31 January 2024).

people who were Avast customers and probably even paid for anti-tracking software was shared. In the wake of this becoming public, the subsidiary's activities were discontinued.[295]

The benefit of using payment in return for data protection as a means of determining the value of personal data is that the value of a privacy breach is examined from an individual perspective.[296] People are willing to pay the above described prices to protect their privacy. This market verification is another advantage. Privacy protection offers are not studies or fictitious figures, but every day, real economic assets based on personal data. Supply of it and demand for it confirm as much.

However, there are also disadvantages to consider when using the individual's willingness to pay for privacy protection as a measure of the value of personal data. If individuals provide a monetary value for which they would be willing to have their personal data protected, this value may be too low to receive an offer from a company that protects personal data.[297] In this case, market verification would not be given and the value would be purely hypothetical.[298]

Another disadvantage of willingness to pay to protect the privacy is that it is the value of a potential damage and not the value of the personal data itself.[299] Individuals choose from a wide range of privacy protection services to prevent data breaches. The prevention of these breaches and the possible consequences are essential in measuring the value. The feeling of security accounts for a significant part of the monetary value. The amount of money people accept to share their personal data and the amount of money people invest to protect their privacy can vary substantially, as described above.[300] This is another reason why figures for privacy protection should be treated with caution when calculating the value of personal data.[301]

Moreover, the pay for privacy model as such has drawbacks. *Cohen* argues that privacy is distributed more unfairly when requiring money.[302] This could be a burden on lower-income households if privacy could be chosen like a neighbour-

---

[295] Avast, *Avast to Commence Wind Down of Subsidiary Jumpshot,* 30 January 2020, https://press.avast.com/en-gb/avast-to-commence-wind-down-of-subsidiary-jumpshot (accessed 31 January 2024).

[296] OECD, *Exploring the Economics of Personal Data* (*supra* Chapter III. note 9), p. 32.

[297] Ibid.

[298] Ibid.

[299] Ibid.

[300] See also, I. Hann et al., 'Overcoming Online Information Privacy Concerns: An Information-Processing Theory Approach' (*supra* Chapter III. note 198), p. 33; A. Acquisti et al., 'What is Privacy Worth?' (*supra* Chapter III. note 205), p. 267.

[301] OECD, *Exploring the Economics of Personal Data* (*supra* Chapter III. note 9), p. 32.

[302] J. E. Cohen, 'Examined Lives: Informational Privacy and the Subject as Object', 52 *Stanford Law Review* (2020), p. 1398; see also, L. Burgess et al., 'The Value of Personal Data in Iot: Industey Perspectives on Consumer Conceptions of Value' (*supra* Chapter III. note 156), p. 4.

hood or luxury goods.[303] The poor would then be excluded from access to privacy and would have no choice but to waive their fundamental right to privacy. *Schwartz* argues that pay for privacy models would undermine the fundamental right to privacy and thus prevent people from asserting their rights.[304] He further states that paying for privacy would lead to two classes of 'haves' and 'have nots' divided by income.[305] *Elvy* echoes this sentiment, noting that the pay for privacy model creates the opportunity for 'predatory' and 'discriminatory' behaviour.[306]

Finally, the question arises as to whether the companies that use pay for privacy models actually protect privacy. This is certainly questionable, considering the examples of Experian and Avast, both of which were confronted with data protection scandals. In this regard, a study found that consumers expect more privacy and data security from paid app versions than from free app version.[307] However, half of the paid apps in the study shared the same data with third parties as their free app version.[308]

7. Criteria for selection of valuation method

Coyle and *Manley* have narrowed down the criteria for the selection of a valuation method down to four questions: (i) what is being valued; (ii) who is valuing the data; (iii) when is the valuation taking place; (iv) what is the purpose of the valuation.[309] Due to their comprehensible and concise manner, the core statements of their research results are reproduced below.

The authors depict the various facets of the concept of 'data' within the data value chain, ranging from raw data generation to the utilisation of data insights for potential end-user value.[310] They highlight that different valuation methodologies often bundle data value with analytics and the translation of insights into decisions, making data more valuable in dynamic firms.[311] However, some

---

[303] J. E. Cohen, 'Examined Lives: Informational Privacy and the Subject as Object' (*supra* Chapter III. note 302), p. 1398; see also, J. E. Cohen, 'Affording Fundamental Rights: A Provocation Inspired by Mireille Hildebrandt, 4 *Critical Analysis of Law* (2017), p. 86.

[304] A. Schwartz, 'The Payoff From California's "Data Dividend" Must be Stronger Privacy Laws', *Electronic Frontier Foundation* (2019), https://www.eff.org/de/deeplinks/2019/02/payoff-californias-data-dividend-must-be-stronger-privacy-laws (accessed 31 January 2024).

[305] Ibid.

[306] S.-A. Elvy, 'Paying for Privacy and the Personal Data Economy', 117 *Columbia Law Review* (2017), p. 1426.

[307] K. A. Bamberger et al., 'Can You Pay for Privacy? Consumer Expectations and the Behavior of Free and Paid Apps', 35 *Berkeley Technology Law Journal* (2020), p. 354.

[308] Ibid, p. 354.

[309] D. Coyle and A. Manley, 'What is the Value of Data? A review of empirical methods' (*supra* Chapter III. note 29), pp. 1–30.

[310] Ibid, p. 19.

[311] Ibid, p. 20.

approaches, may result in value estimates independent of data content and context, potentially leading to incomplete assessments.[312] Additionally, they note that generating valuable insights may not always necessitate the entire dataset, prompting inquiries into the minimum data required for effective decision-making, especially when considering associated costs.[313]

Coyle and *Manley* argue that the perspective of the entity or individual assessing the data influences the suitable methods.[314] Public sector focus on data cost contrasts with the private sector's emphasis on usage impact, while users prioritise insights.[315] Data hubs, as intermediaries, are concerned with market prices.[316] The authors underscore the public sector's broader societal perspective on data value and highlight challenges, including undervaluation and the unique role of data as a strategic asset for firms.[317]

The discussion on the timing of data valuation is elucidated by *Coyle* and *Manley*, emphasising the distinction between *ex-ante* and *ex-post* methods.[318] *Ex-ante* valuations, limited by the uncertainty of prospective insights, often neglect the significant option value of data.[319] *Ex-post* valuations, providing more certainty, prompt considerations on depreciation rates and timelines for diverse data types, with real-time data depreciating rapidly in certain contexts compared to slower or negligible depreciation in other data types.[320]

Finally, *Coyle* and *Manley* underscore that the purpose of data valuation influences the choice of methodologies.[321] While cost-based methods are preferred for cautious estimates, market-based approaches may overlook certain aspects of data's value in different decisions.[322] Additionally, the divergence between private and public sector purposes, along with debates on data intermediaries and value allocation, adds complexity to the valuation landscape.[323]

---

[312] Ibid.
[313] Ibid, p. 21.
[314] Ibid.
[315] Ibid.
[316] Ibid.
[317] Ibid, p. 22.
[318] Ibid.
[319] Ibid.
[320] Ibid, p. 23.
[321] Ibid.
[322] Ibid.
[323] Ibid.

8. Conclusion: Context-dependent monetary value of personal data

The aim of this chapter was to illustrate that data has a monetary value. Personal data has become increasingly important in the economy, as exemplified by the world's most valuable companies. These companies operate in the data economy and derive value from it. Consequently, personal data has economic value. Personal information such as name, address and health data are already traded on the global market as an economic asset.

The example of Facebook highlights how these companies use personal data. Profiling is a means of creating overall images of a personality for specific purposes. Profiling involves the merging of data, as well as its subsequent analysis and purpose-related evaluation. This results in detailed information about the identity of a person. In this way, an attempt is made to analyse what a person likes and dislikes, and thus to predict the person's behaviour. These profiles are particularly interesting for advertising companies. They can use these profiles to place personalised advertisements and reach the desired target group. The numbers and various studies are proof that this approach is highly lucrative.

Data sharing is emblematic of the monetisation of personal data. Facebook shares data with subsidiaries within its own group, but also with external companies, as has recently become clear to the wider public. However, not only Facebook, but also data brokers use and trade personal data as an economic asset. These data brokers specialise in collecting large amounts of information (data sets) about individuals and selling it on to third parties.

Based on the prices for which data brokers sell personal data, the market value can be calculated. Individual pieces of information such as name, age and address are only worth a few cents. The true value of personal data lies in its quantity. Data sets with information on thousands of people make personal data trading profitable. There are some companies that have set out to let the data subjects themselves participate in this trade and earn money from it.

During this data sharing and processing, a data breach may occur. Data breaches may be penalised, on the basis of which the price per affected customer can be calculated. These fines can quickly cost significant sums of money. A data breach often results in personal data ending up on the dark web. The prices charged on the dark web for selling data can also be used to determine the value. However, the value of both the data breach and the prices on the dark web are influenced by numerous other factors.

There are numerous surveys and experiments on how much money people demand to reveal their personal data. There are also many theoretical and practical approaches to the willingness to pay for privacy. The latter concept is criticised by data protection advocates. Survey and experiments are nevertheless relevant, as they indicate the value from the individual perspective of the data subject. They prove that individuals are more willing to sell their personal data

than to protect their data for money. There is a clear difference between the willingness to accept, i.e. the minimum monetary amount that a person is willing to accept to sell their personal data, and the willingness to pay, i.e. the maximum price a person is willing to pay to protect their personal data.

The various methods that were presented in this chapter are attempts to estimate the value of personal data. A concrete value cannot be determined for personal data. A name is not always worth 0.50 cents. The monetary value depends on many factors, including the method of valuation, the context and the people studied. In addition, each method has advantages and disadvantages. Nevertheless, conclusions can be drawn. First, the value varies depending on the data category, with sensitive data always being the most valuable, regardless of method. Second, unusual characteristics or daily routines as well as unique events are particularly valuable. Third, the value increases when data subjects become aware that their data is being traded and the see themselves as owners.

As demonstrated through these various methods and analyses, personal data holds inherent monetary value, a value that is, however, variable. Contingent on factors such as context, data category and the specific evaluation methods applied, this nuanced perspective underscores that personal data does not possess a fixed, universal value. The most valuable companies use, share and value personal data, which is why it is called the 'lifeblood' of the economy. What rights individuals have or could have to this 'lifeblood' of the economy, to personal data as an economic asset, will be addressed in the next chapter.

IV. Rights to personal data as an economic asset

The Cambridge dictionary defines asset as 'a useful or valuable quality, skill, or person' or 'something having value, such as a possession or property, that is owned by a person, business, or organisation'.[1] Therefore, an asset has to be something valuable that belongs to a person or a company in some way. In this work, personal data is the asset under consideration.

Chapter II. has focused on defining personal data. Chapter III. has demonstrated that personal data has an economic value. Considering the definition of asset, it remains to be clarified to what extent there can be ownership over personal data. The question of ownership and allocation of personal data has to be addressed given the economic exploitation of data outlined in the previous chapter.[2] Can data be a property and are there consequently data owners? To answer these questions, the chapter is divided into the following sections: Section 1 looks at ownership rights to data. Section 2 analyses specific ownership-like rights to data. Section 3 examines the rights under the GDPR and how these rights grant data subjects, similar to ownership, control and disposition over their personal data.

1. Ownership of data

In the legal system, property is assigned to a person and protected by means of ownership.[3] Ownership is one of the strongest forms of allocating rights.[4] The discussion about ownership of data follows economic interests in assigning rights to data and thus their value exclusively.[5] For personal data, it is therefore discussed whether *de lege lata* there is an allocation and protection by property-like rights and, if not, which property-like rights to data would be conceivable from a

---

[1] See the definition for asset in the Cambridge Dictionary, https://dictionary.cambridge.org/dictionary/english/asset (accessed 31 January 2024).

[2] See also V. Janeček, 'Ownership of personal data in the Internet of Things', 34 *Computer Law & Security Review* (2018), p. 1040.

[3] A. Schmid, K.-J. Schmidt and H. Zech, 'Rechte an Daten zum Stand der Diskussion', 22 *sic! – Zeitschrift für Immaterialgüter-, Informations- und Wettbewerbsrecht* (2018), p. 629.

[4] H. Zech, 'Daten als Wirtschaftsgut – Überlegungen zu einem Recht des Datenerzeugers', 31 *CR – Computer und Recht* (2015), p. 140.

[5] A. Boerding et al., 'Data Ownership – A Property Rights Approach from a European Perspective', 11 *Journal of Civil Law Studies* (2018), p. 357.

normative perspective.[6] *Purtova* takes this idea even further and argues that it is not a question of if, but how property rights should be allocated regarding personal data.[7] The interests of the data subject and the data controller must be taken into account.[8]

The question arises whether data ownership is protected by EU law. Data ownership is not protected by either primary or secondary EU law. For example, the Data Act[9] does not envisage ownership rights to data, which is to be welcomed.[10] Recital 5 of the Data Act states that it 'should not be interpreted as recognizing or conferring any new right on data holders […]'. The CJEU clarified that Article 17 of the Charter ('Right to property')

'applies to rights with an asset value creating an established legal position under the legal system, enabling the holder to exercise those rights autonomously and for his benefits'.[11]

Consequently, there needs to be a possibility of exercising rights and not merely a bare protection of possession, as a result of which data possession is not protected by EU law either.[12] The absence of protection of data ownership under EU law does not leave a gap in legal protection as personal data are indeed protected by the Charter.[13] However, this protection is not a typical protection of possession, as it is rather aimed at ensuring that another person does not gain possession of personal data, does not exploit its possession or gives it up by deleting the data.[14]

a) Ownership of data de lege lata *in national legal systems*

This section explores findings from German-speaking national legal systems and, in particular, the debate in the German-speaking academic discussion regarding ownership of data. This debate then provides a backdrop for the discussion in the EU law context in Chapter IV. 3.

---

[6] A. Schmid, K.-J. Schmidt and H. Zech, 'Rechte an Daten zum Stand der Diskussion' (*supra* Chapter IV. note 3), p. 629.

[7] N. Purtova, 'The illusion of personal data as no one's property' (*supra* Chapter I. note 14), p. 109.

[8] M. Grützmacher, 'Dateneigentum – ein Flickenteppich', 32 *CR – Computer und* Recht (2016), p. 495.

[9] Regulation (EU) 2023/2854 of the European Parliament and of the Council 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.

[10] See also M. Hennemann and B. Steinrötter, 'Data Act – Fundament des neuen EU-Datenwirtschaftsrechts?', 75 *NJW – Neue Juristische Wochenschrift* (2022), p. 1486.

[11] See Case C-283/11 *Sky Österreich*, EU:C:2013:28, para. 34.

[12] F. Michl, 'Datenbesitz – ein grundrechtliches Schutzgut?', 72 *NJW – Neue Juristische Wochenschrift* (2019), p. 2732.

[13] See Article 8 of the Charter; F. Michl, 'Datenbesitz – ein grundrechtliches Schutzgut?' (*supra* Chapter IV. note 12), p. 2732.

[14] Ibid, p. 2733.

With regard to personal data under private law, it should first be noted that the provisions of the BGB[15] do not provide for a property right over personal data.[16] This applies both to individual data and to the entire data set, for example in the form of a database.[17] Personal data are not physical objects and are therefore not covered by the property law provisions of the BGB.[18]

Likewise, in Switzerland, within the meaning of property law, individuals can only be owners of tangible goods.[19] However, since personal data are non-tangible goods, there can be no ownership of data in the framework of property law.[20]

The problem of allocating personal data under property law, as shown in Germany or Switzerland, does not arise in Austria, because Austrian property law does not presuppose a tangible object.[21] Although the prevailing view in the academic literature recognises personal data as non-tangible objects, it is also generally recognised that an ownership of personal data does not exist.[22]

De lege lata, personal data cannot therefore be allocated to an owner and personal data cannot be protected by ownership.[23] The allocation of personal

---

[15] Bürgerliches Gesetzbuch in der Fassung der Bekanntmachung vom 2. Januar 2002 (BGBl. I S. 42, 2909; 2003 I S. 738), das zuletzt durch Artikel 1 des Gesetzes vom 10. August 2021 (BGBl. I S. 3515) geändert worden ist.

[16] J. Froese and S. Straub, 'Wem gehören die Daten? – Rechtliche Aspekte der digitalen Souveränität in der Wirtschaft' in E. Hartmann (ed.), *Digitalisierung souverän gestalten – Innovative Impulse im Maschinenbau* (Springer Verlag, 2021), p. 88; A. Duisberg, 'Datenhoheit und Recht des Datenbankherstellers – Recht am Einzeldatum vs. Rechte an Datensammlungen' in O. Raabe and M. Wagner (eds.), *Daten als Wirtschaftsgut – Europäische Datenökonomie oder Rechte an Daten?* (Smart Data, 2017), p. 16; C. Peschel and S. Rockstroh, 'Big Data in der Industrie – Chancen und Risiken neuer datenbasierter Dienste', 17 *MMR – Zeitschrift für IT-Recht und Recht der Digitalisierung* (2014), p. 572.

[17] Ibid.

[18] See Section 90 BGB; T. Heymann, 'Rechte an Daten – Warum Daten keiner eigentumsrechtlichen Logik folgen', 32 *CR – Computer und Recht* (2016), p. 650; T. Heymann, 'Der Schutz von Daten bei der Cloud Verarbeitung', 31 *CR – Computer und Recht* (2015), p. 809; M. Markendorf, 'Recht an Daten in der deutschen Rechtsordnung', 9 *ZD – Zeitschrift für Datenschutz* (2018), p. 410; F. Michl, 'Datenbesitz – ein grundrechtliches Schutzgut?' (*supra* Chapter IV. note 12), p. 2730; W. Reiners, 'Datenschutz in der Personal Data Economy – Eine Chance für Europa', 5 *ZD – Zeitschrift für Datenschutz* (2015), p. 54; F. Schuster and S. Hunzinger, 'Vor- und nachvertragliche Pflichten beim IT-Vertrag – Teil II: Nachvertragliche Pflichten', 31 *CR – Computer und Recht* (2015), p. 279; A. Sattler, 'Personenbezogene Daten als Leistungsgegenstand', 72 *JZ – Juristen Zeitung* (2017), p. 1037.

[19] A. Schmid, K.-J. Schmidt and H. Zech, 'Rechte an Daten zum Stand der Diskussion' (*supra* Chapter IV. note 3), p. 630.

[20] Ibid.

[21] N. Forgó, 'Daten als Gegenstand von sachenrechtlichen, datenschutz- und urheberrechtlichen Regelungen' in N. Forgó and B. Zöchling-Jud (eds.), *Das Vertragsrecht des ABGB auf dem Prüfstand: Überlegungen im digitalen Zeitalter* (Manz Verlag, 2018), p. 356.

[22] Ibid.

[23] L. Specht, 'Ausschließlichkeitsrechte an Daten – Notwendigkeit, Schutzumfang, Alternativen', 32 *CR – Computer und Recht* (2016), p. 289; A. Schmid, K.-J. Schmidt and H. Zech,

data is therefore in principle purely factual: anyone who is technically able to access and process data can do so.[24] Although it is possible to give data as contractual performance or consideration, this does not constitute a criterion for the allocation of goods.[25] The fact that personal data as such cannot be an object of ownership has also been reiterated by courts.[26]

De lege lata one can own data carriers on which the data are stored. For example, the unauthorised modification or deletion of personal data can be an infringement of ownership of the data carrier.[27] Ownership of the storage medium could thus be a starting point for assigning rights to data.[28] This approach could have an incredible impact, especially in the light of the *UsedSoft* judgment.[29] In this case, the CJEU ruled that the download of software is comparable to the transfer of a physical storage medium.[30] The principles of selling tangible objects could therefore also apply to non-tangible objects.

However, the right to the data and the right to the data carrier must not be confused. *Heun* and *Assion* poignantly ask what happens if the data 'belong' to one person and the data carrier to the other, whose right prevails?[31] A look at cloud services shows that it is not rights to the storage medium that are important.[32] With these business models, the user stores his data on third-party servers

---

'Rechte an Daten zum Stand der Diskussion' (*supra* Chapter IV. note 3), p. 630; M. Dorner, 'Big Data und Dateneigentum', 30 *CR – Computer und Recht* (2014), p. 626; H. Zech, 'Daten als Wirtschaftsgut – Überlegungen zu einem Recht des Datenerzeugers' (*supra* Chapter IV. note 4), p. 144; B. Custers and G. Malgieri, 'Priceless data: why the EU fundamental right to data protection is at odds with trade in personal data' (*supra* Chapter I. note 11), p. 3.

[24] J. Froese and S. Straub, 'Wem gehören die Daten? – Rechtliche Aspekte der digitalen Souveränität in der Wirtschaft' (*supra* Chapter IV. note 16), p. 88.

[25] L. Specht, 'Ausschließlichkeitsrechte an Daten – Notwendigkeit, Schutzumfang, Alternativen' (*supra* Chapter IV. note 23), p. 289.

[26] See, for example, OLG Dresden, 05.09.2012, 4 W 961/12; OLG Naumburg, 27.08.2014, 6 U 3/14.

[27] M. Bartsch, 'Computerviren und Produkthaftung', 16 *CR – Computer und Recht* (2000), p. 723; H. Zech, 'Daten als Wirtschaftsgut – Überlegungen zu einem Recht des Datenerzeugers' (*supra* Chapter IV. note 4), p. 142.

[28] A. Boerding et al., 'Data Ownership – A Property Rights Approach from a European Perspective' (*supra* Chapter IV. note 5), p. 356.

[29] See Case C-128/11 *UsedSoft*, EU:C:2012:407.

[30] Ibid, para. 61.

[31] S.-E. Heun and S. Assion, 'Internet(recht) der Dinge – Zum Aufeinandertreffen von Sachen- und Informationsrecht', 31 *CR – Computer und Recht* (2015), p. 814; see also M. Bartsch, 'Software als Rechtsgut', 26 *CR – Computer und Recht* (2010), p. 554.

[32] T. Hoeren, 'Datenbesitz statt Dateneigentum', 22 *MMR – Zeitschrift für IT-Recht und Recht der Digitalisierung* (2019), p. 7; F. Schuster and S. Hunzinger, 'Vor- und nachvertragliche Pflichten beim IT-Vertrag – Teil II: Nachvertragliche Pflichten' (*supra* Chapter IV. note 18), p. 279; G. Wagner, 'BGB § 823' in F.J. Säcker et al. (eds.), *Münchener Kommentar zum Bürgerlichen Gesetzbuch* (8th edition, C.H. Beck, 2020), para. 332; K. Zdanowiecki, 'Recht an den Daten' in P. Bräutigam and T. Klindt (eds.), *Digitalisierte Wirtschaft / Industrie 4.0* (2015), p. 21.

but does not want to give up his own right to control the data in favour of the cloud provider.[33] The terms and conditions of cloud providers often state that providers retain the rights to the service and customers retain the rights to the content.[34] Thus, the rights are allocated separately. *Hoeren* refers to the fact that the owner of a rented flat is also not entitled to ownership of the tenant's objects brought into the flat.[35] The ownership right to the carrier medium must therefore be separated from the rights to the data contained on it.[36] The storage medium of the data is irrelevant for the allocation of rights.[37] Data ownership is intended to clarify the question of the allocation of data that is precisely not embodied in a data carrier.[38]

For years, German courts ruled in an undifferentiated manner that data carriers and the data contained on them are collectively one thing.[39] Thus, the unauthorised deletion of data was also considered a violation of property.[40] A violation of property is therefore not only given in the case of destruction of and damage to the substance of the object, but in the case of any effect on the object that prevents the owner from using it according to his wishes.[41] This would mean that the owner of the data carrier would also have comprehensive rights to the stored data itself. Austrian courts also focused on the data carrier when assessing the ownership of data.[42] Accordingly, it is established case law in Austria that the

---

[33] T. Hoeren, 'Dateneigentum – Versuch einer Anwendung von § 303a StGB im Zivilrecht', 16 *MMR – Zeitschrift für IT-Recht und Recht der Digitalisierung* (2013), p. 487; A. Kalle, 'Herausgabe von Daten in der Insolvenz', 13 *BRJ – Bonner Rechtsjournal* (2020), p. 40; T. Hoeren, 'Datenbesitz statt Dateneigentum' (*supra* Chapter IV. note 32), p. 7.

[34] S. Bradshaw, C. Millard and I. Walden, 'Contracts for clouds: comparison and analysis of the Terms and Conditions of cloud computing services', 19 *International Journal of Law and Information Technology* (2011), p. 208.

[35] T. Hoeren, 'Dateneigentum – Versuch einer Anwendung von § 303a StGB im Zivilrecht' (*supra* Chapter IV. note 33), p. 487.

[36] L. Specht, 'Ausschließlichkeitsrechte an Daten – Notwendigkeit, Schutzumfang, Alternativen' (*supra* Chapter IV. note 23), p. 291; G. Wagner, 'BGB § 823' (*supra* Chapter IV. note 32), para. 333.

[37] M. Markendorf, 'Recht an Daten in der deutschen Rechtsordnung' (*supra* Chapter IV. note 18), p. 411; H. Redeker, 'Information als eigenständiges Rechtsgut', 27 *CR – Computer und Recht* (2011), p. 634; K. Zdanowiecki, 'Recht an den Daten' (*supra* Chapter IV. note 32), p. 21.

[38] G. Wagner, 'BGB § 823' (*supra* Chapter IV. note 32), para. 335; see also S. van Erp, 'Ownership of data: the numerus clausus of legal objects', 6 *Brigham-Kanner Property Rights Conference Journal* (2017), p. 251.

[39] See BGH, 06.06.1984, VIII ZR 83/83; BGH, 02.05.1985, I ZB 8/84; BGH, 07.03.1990, VIII ZR 56/89; BGH, 14.07.1993, VIII ZR 147/92; BGH, 04.03.1997, X ZR 141/95.

[40] See OLG Karlsruhe, 07.11.1995, 3 U 15/95.

[41] See B. Müller-Christmann, 'Haftung für Zerstörung von Computerdaten', 49 *NJW – Neue Juristische Wochenschrift* (1996), p. 200.

[42] N. Forgó, 'Daten als Gegenstand von sachenrechtlichen, datenschutz- und urheberrechtlichen Regelungen' (*supra* Chapter IV. note 21), p. 354.

permanent transfer of standard software embodied on data carriers in return for a one-off payment is to be qualified as a purchase.[43]

The more recent ruling on the *Kohl diaries* ('*Kohl-Tagebücher*') by the BGH demonstrated that the right to the data and the right to the data carrier can fall apart.[44] This judgment concerned tape recordings. The BGH ruled that the owner of the audio tapes and the person entitled to the spoken content may be different.[45] Accordingly, the person who spoke the recorded content cannot necessarily demand the handover of the data carrier.[46] In view of the technical developments in recent years, one can agree with this judgment that data and data carrier are to be separated. In addition, the CJEU ruled that an e-book cannot be compared to a printed book, as the former deteriorates through use.[47] This reasoning can also be applied to data and the respective storage medium. The data does not deteriorate, but the physical storage medium does. The allocation of data on the basis of ownership of the carrier medium must therefore be rejected.[48]

The purpose of this chapter is to illustrate that there is no ownership and thus no owners of personal data exist under property law in German-speaking national legal systems. *De lege lata*, an attempt was made to construct an allocation of rights to the basis of the storage medium. However, cloud services highlight that this approach is no longer up to date.

b) The desirability of ownership over data from a normative perspective

Given that ownership of data does not exist, neither under current primary or secondary EU law nor under German-speaking legal frameworks, the question arises as to whether such a right should be introduced. Modern definitions of property are significant in this regard because they do not discuss property in isolation, but contextually in the social environment.[49] The principle of all-encompassing ownership is limited by multiple, socially oriented restrictions.[50] Examples of such restrictions on property rights are expropriation or immission control. In addition, a good can have several owners, meaning that interests of

---

[43] See OGH, 13.11.1997, RS0108702, AT:OGH0002:1997:RS0108702.

[44] See BGH, 10.07.2015, V ZR 206/14.

[45] Ibid, para. 20.

[46] Ibid.

[47] See Case C-263/18 *Nederlands Uitgeversverbond und Groep Algemene* Uitgevers, EU:C:2019:1111, para. 58.

[48] L. Specht, 'Ausschließlichkeitsrechte an Daten – Notwendigkeit, Schutzumfang, Alternativen' (*supra* Chapter IV. note 23), p. 292; see also M. Grützmacher, 'Dateneigentum – ein Fleckenteppich' (*supra* Chapter IV. note 8), p. 487, who argues that ownership of tangible objects is not a suitable criterion for assigning rights to data.

[49] I. Stepanov, 'Introducing a property right over data in the EU: the data producer's right – an evaluation', 34 *International Review of Law, Computers & Technology* (2020), p. 69.

[50] J. Ensthaler, 'Industrie 4.0 und die Berechtigung an Daten', 69 *NJW – Neue Juristische Wochenschrift* (2016), p. 3475.

co-owners must be considered. Private law theory therefore no longer refers to undivided ownership, but to a bundle of rights.[51] The following paragraphs present arguments for and against the introduction of ownership of data. In addition, different approaches are presented as to who could be the owner of data.

The definition and form of property differs from one legal system to another. What is recognised as property in one country is not considered property in another. What the legal systems have in common is that property is an *erga omnes* right and must therefore be respected by every person.[52] Data ownership would thus grant the owner an exclusive right of access to data and exclude third parties from it.[53] In addition, the owner would have the right to exploit the data and the profit that comes with it.[54] Moreover, claims for damages might be possible in case of unauthorised use or infringement of the data by third parties.[55] As a result, data ownership would grant both positive and negative rights.[56]

The question of the introduction of an *erga omnes* right to data was also addressed by the European Commission.[57] The relevant Commission Staff Working Document only deals with non-personal and anonymised data, as it states that the fundamental right to data protection and other data protection legislation give extensive rights to individuals concerning personal data.[58] The European Commission suggests several possible ways forward, including a data producer's *erga omnes* right to non-personal and anonymous data.[59]

Proponents of an *erga omnes* right to data point out that software and tangible assets have clear parallels and similarities and should consequently be put on an equal footing as traditional objects of property protection.[60] In particular, as personal data have a substantial economic significance, it is argued that they should be classified as objects in the sense of property law.[61] In this context, reference is made to the principle of equality, i.e. what is equal should be treated equally and what is unequal should be treated unequally.[62] *Markendorf* argues that there needs to be an independent right to data, otherwise a certain degree of

---

[51] Ibid, p. 3476.

[52] I. Stepanov, 'Introducing a property right over data in the EU: the data producer's right – an evaluation' (*supra* Chapter IV. note 49), p. 70.

[53] A. Boerding et al., 'Data Ownership – A Property Rights Approach from a European Perspective' (*supra* Chapter IV. note 5), p. 356.

[54] Ibid, p. 362.

[55] Ibid, p. 363.

[56] Ibid, p. 369.

[57] Commission Staff Working Document on the free flow of data and emerging issues of the European data economy, (SWD 2017) 2 final, p. 33.

[58] Ibid, p. 33.

[59] Ibid.

[60] M. Bartsch, 'Software als Rechtsgut' (*supra* Chapter IV. note 31), p. 553; see also C. Rees, 'Who owns our data?', 30 *Computer Law & Security Review* (2014), p. 76.

[61] A. Kalle, 'Herausgabe von Daten in der Insolvenz' (*supra* Chapter IV. note 33), p. 43.

[62] M. Bartsch, 'Software als Rechtsgut' (*supra* Chapter IV. note 31), p. 558.

legal uncertainty would remain.[63] With an ownership right to personal data, access to the data could be certain and secured.[64] Data ownership could protect against unauthorised access by third parties and reduce costs.[65] Such an exclusive right could create an incentive to engage in the data economy and thus strengthen innovation.[66] Furthermore, the non-rivalrous nature of data can be cited as a reason for creating a right to data.[67] An exclusive right could create markets that facilitate trading in data.[68] However, *Heymann* states that the lack of rivalry of data does not trigger a need for protection, since it is precisely the fact that countless third parties can access data that can be the advantage of data.[69]

As far as the establishment of an *erga omnes* right is concerned, the European Commission states that the right should be allocated to those who have made investments in the creation of the data.[70] Likewise, *Ensthaler* welcomes the adoption of provisions of property law, where the processor of an object is entitled to a claim on the object.[71] It is not necessarily the new technical idea or an intellectual personal creation that is rewarded, but the effort required to collect the data.[72] Companies have an interest in ensuring that data is allocated to the legal subject who invests in the production, irrespective of any personal reference.[73]

Supporters of an *erga omnes* right to data argue that in the case of multiple parties, fractional rights should apply, according to which the participants may use the data.[74] This would be a similar approach to the co-ownership recognised in private law.[75] Further use would be dependent on the consent of the co-entitled

---

[63] M. Markendorf, 'Recht an Daten in der deutschen Rechtsordnung' (*supra* Chapter IV. note 18), p. 411.

[64] A. Kalle, 'Herausgabe von Daten in der Insolvenz' (*supra* Chapter IV. note 33), p. 43.

[65] G. Wagner, 'BGB § 823' (*supra* Chapter IV. note 32), para. 335.

[66] H. Zech, 'Daten als Wirtschaftsgut – Überlegungen zu einem Recht des Datenerzeugers' (*supra* Chapter IV. note 4), p. 144.

[67] T. Heymann, 'Rechte an Daten – Warum Daten keiner eigentumsrechtlichen Logik folgen' (*supra* Chapter IV. note 18), p. 652.

[68] H. Zech, 'Daten als Wirtschaftsgut – Überlegungen zu einem Recht des Datenerzeugers' (*supra* Chapter IV. note 4), p. 145.

[69] T. Heymann, 'Rechte an Daten – Warum Daten keiner eigentumsrechtlichen Logik folgen' (*supra* Chapter IV. note 18), p. 653; see also S. van Erp, 'Ownership of data: the numerus clausus of legal objects' (*supra* Chapter IV. note 38), p. 250.

[70] Commission Staff Working Document (SWD 2017) 2 final (*supra* Chapter IV. note 57), p. 35.

[71] J. Ensthaler, 'Industrie 4.0 und die Berechtigung an Daten' (*supra* Chapter IV. note 50), p. 3476.

[72] Ibid.

[73] L. Specht, 'Ausschließlichkeitsrechte an Daten – Notwendigkeit, Schutzumfang, Alternativen' (*supra* Chapter IV. note 23), p. 291; A. Boerding et al., 'Data Ownership – A Property Rights Approach from a European Perspective' (*supra* Chapter IV. note 5), p. 358.

[74] J. Ensthaler, 'Industrie 4.0 und die Berechtigung an Daten' (*supra* Chapter IV. note 50), p. 3478.

[75] L. Specht, 'Ausschließlichkeitsrechte an Daten – Notwendigkeit, Schutzumfang, Alternativen' (*supra* Chapter IV. note 23), p. 295.

parties.[76] It is not a novelty that certain rights can be limited by third parties. For example, this applies to the protection of photographs in which the copyright of the photographer, the personality right of the person photographed and the property right of the owner of the carrier medium can co-exist.[77]

However, an allocation problem could arise in the case of multiple stakeholders.[78] For example, maintenance data of a car could belong to its owner and the garage.[79] Data ownership could hinder the flow of data, as data owners would have to deal with a group of other persons who can also claim rights of possession.[80] Granting property rights over data would thus lead to legal uncertainty and less use of data due to the multitude of people involved in data.[81] *Heymann* also emphasises that the different actors and constellations of interests do not allow for a standardised determination of the person with rights to data.[82] The question of who is ultimately entitled to a property right to data would therefore remain unanswered.[83]

Legal scholars have different approaches to answering the question of who might potentially own personal data. In the case of personal data, it would be reasonable to grant such a right to the data subject. Data sovereignty and digital private autonomy strengthen the position of the data subject as the person entitled to exercise control over his or her personal data.[84] This approach would be systematically in line with EU data protection law. Under EU data protection law, the right over personal data is principally allocated to the right of disposition of the data subject.[85] The data subject decides on the use of personal data.[86]

---

[76] J. Ensthaler, 'Industrie 4.0 und die Berechtigung an Daten' (*supra* Chapter IV. note 50), p. 3478.

[77] L. Specht, 'Ausschließlichkeitsrechte an Daten – Notwendigkeit, Schutzumfang, Alternativen' (*supra* Chapter IV. note 23), p. 294.

[78] A. Wiebe, 'Von Datenrechten zu Datenzugang – Ein rechtlicher Rahmen für die europäische Datenwirtschaft', 33 *CR – Computer und Recht* (2017), p. 90.

[79] A. Roßnagel, 'Fahrzeugdaten – wer darf über sie entscheiden?', 14 *SVR – Straßenverkehrsrecht* (2014), p. 283.

[80] S.-E. Heun and S. Assion, 'Internet(recht) der Dinge – Zum Aufeinandertreffen von Sachen- und Informationsrecht' (*supra* Chapter IV. note 31), p. 814.

[81] I. Stepanov, 'Introducing a property right over data in the EU: the data producer's right – an evaluation' (*supra* Chapter IV. note 49), p. 79.

[82] T. Heymann, 'Rechte an Daten – Warum Daten keiner eigentumsrechtlichen Logik folgen' (*supra* Chapter IV. note 18), p. 655.

[83] T. Heymann, 'Der Schutz von Daten bei der Cloud Verarbeitung' (*supra* Chapter IV. note 18), p. 810.

[84] B. Weber, 'Datenschutz 4.0 – Daten als Wirtschaftsgut in digitalisierten Märkten' in D. Wolff and R. Göbel (eds.), *Digitalisierung: Segen oder Fluch* (Springer Verlag, 2018), p. 114.

[85] S.-E. Heun and S. Assion, 'Internet(recht) der Dinge – Zum Aufeinandertreffen von Sachen- und Informationsrecht' (*supra* Chapter IV. note 31), p. 813.

[86] J. Ensthaler, 'Industrie 4.0 und die Berechtigung an Daten' (*supra* Chapter IV. note 50), p. 3473; B. Buchner, 'Wissen ist Macht?', 32 *DuD – Datenschutz und Datensicherheit* (2008), p. 728.

However, there are personal data that data subjects cannot dispose of in an ownership-like manner, such as a criminal record or an electronic health record.[87]

The creator of the data could also be the entitled party to data, which would follow the logic of the rights to software.[88] This concept is one of the earliest attempts at allocating exclusive rights to data.[89] The creator is usually also the person storing and accessing the data.[90] If these are different persons, the creator of the data should be protected against others restricting the usability of the data, the creation of which may have required a considerable economic effort.[91] Once the data is created, it is not necessarily apparent who created it and who is entitled to possession of the data, which contradicts fundamental property law principles.[92] Thus, data creation and possession cannot assume the '*Publizitätsfunktion*' referred to in the German-speaking legal sphere, according to which the legal situation *in rem* must be recognisable to everyone at all times.[93] However, the possession of an object is often not externally evident, with the result that the lack of recognisability of possession does not necessarily speak against data possession.[94] *Markendorf* also refutes the argument of the impossible transparency of a creator's right to data by claiming that the blockchain would be a technical solution for a clear allocation.[95] Proof of the actual ownership of the data could be entered in the blockchain and would be visible and verifiable for everyone.[96] However, it is questionable whether a data creator/producer right would actually be effective.[97]

---

[87] W. Reiners, 'Datenschutz in der Personal Data Economy – Eine Chance für Europa' (*supra* Chapter IV. note 18), p. 51.

[88] T. Hoeren, 'Dateneigentum – Versuch einer Anwendung von § 303a StGB im Zivilrecht' (*supra* Chapter IV. note 33), p. 487; M. Markendorf, 'Recht an Daten in der deutschen Rechtsordnung' (*supra* Chapter IV. note 18), p. 410.

[89] A. Boerding et al., 'Data Ownership – A Property Rights Approach from a European Perspective' (*supra* Chapter IV. note 5), p. 356.

[90] M. Markendorf, 'Recht an Daten in der deutschen Rechtsordnung' (*supra* Chapter IV. note 18), p. 411; G. Wagner, 'BGB § 823' (*supra* Chapter IV. note 32), para. 336.

[91] T. Hoeren, 'Datenbesitz statt Dateneigentum' (*supra* Chapter IV. note 32), p. 7; M. Markendorf, 'Recht an Daten in der deutschen Rechtsordnung' (*supra* Chapter IV. note 18), p. 411; A. Kalle, 'Herausgabe von Daten in der Insolvenz' (*supra* Chapter IV. note 33), p. 43.

[92] T. Hoeren, 'Datenbesitz statt Dateneigentum' (*supra* Chapter IV. note 32), p. 7.

[93] F. Michl, 'Datenbesitz – ein grundrechtliches Schutzgut?' (*supra* Chapter IV. note 12), p. 2731.

[94] T. Hoeren, 'Datenbesitz statt Dateneigentum' (*supra* Chapter IV. note 32), p. 7.

[95] M. Markendorf, 'Recht an Daten in der deutschen Rechtsordnung' (*supra* Chapter IV. note 18), p. 411; see also regarding blockchain as a measure to avoid loss of personal data: N. Fabiano, 'The value of personal data is the Data Protection and Privacy preliminary condition: synthetic human profiles on the web and ethics', *3rd International Conference on Applications of Intelligent Systems* (2020), p. 5.

[96] M. Markendorf, 'Recht an Daten in der deutschen Rechtsordnung' (*supra* Chapter IV. note 18), p. 412.

[97] I. Stepanov, 'Introducing a property right over data in the EU: the data producer's right – an evaluation' (*supra* Chapter IV. note 49), p. 80.

Social media companies analyse and process personal data. As shown in the previous chapter, this is the main reason why personal data generates value. Thus, one approach could be that data controllers should have a certain data sovereignty due to their work and enrichment of the data. Given the importance of data to business owners, an argument could therefore be made in favour of allocating personal data as an asset.[98]

In the case of an allocation of data under property law, data protection concerns must be taken into account.[99] Data sovereignty requires that a highly personal, inalienable core content remains with the data subject.[100] This core content includes objections to the use of the data such as the right to be forgotten, the right to information and the right to deletion.[101] Thus, if one decides to allocate the right over personal data to the data controller and not to the data subject, data protection law limits such an exclusive right by requiring that the data controller obtains the consent of the data subject or fulfills the lawfulness of processing.[102] This issue raises the question of the worth of an exclusive right to personal data if this right can be withdrawn at any time and by unilateral declaration of the data subject.[103]

Furthermore, *Heymann* considers the ownership of data to be in conflict with the core idea of data protection law.[104] He argues that the function of data protection law is to strike a reasonable balance between the manifold interests of the public in the free exchange of data, on the one hand, and the protection of the privacy of the individual, on the other.[105] This is precisely what distinguishes ownership from data, *Heymann* explains, because data are not related to anyone and are thus ownerless.[106] This argument can be opposed by the fact that personal data relates to a person and consequently this person could be granted certain ownership-like rights for protection. Unlike classic property, data has countless social functions and uses, *Heymann* continues.[107] The fact that property also has

---

[98] L. Specht, 'Ausschließlichkeitsrechte an Daten – Notwendigkeit, Schutzumfang, Alternativen' (*supra* Chapter IV. note 23), p. 296.

[99] Ibid, p. 289.

[100] B. Weber, 'Datenschutz 4.0 – Daten als Wirtschaftsgut in digitalisierten Märkten' (*supra* Chapter IV. note 84), p. 114.

[101] Ibid, p. 114.

[102] L. Specht, 'Ausschließlichkeitsrechte an Daten – Notwendigkeit, Schutzumfang, Alternativen' (*supra* Chapter IV. note 23), p. 294.

[103] A. Duisberg, 'Datenhoheit und Recht des Datenbankherstellers – Recht am Einzeldatum vs. Rechte an Datensammlungen' (*supra* Chapter IV. note 16), p. 19; B. Custers and G. Malgieri, 'Priceless data: why the EU fundamental right to data protection is at odds with trade in personal data' (*supra* Chapter I. note 11), p. 4.

[104] T. Heymann, 'Rechte an Daten – Warum Daten keiner eigentumsrechtlichen Logik folgen' (*supra* Chapter IV. note 18), p. 656.

[105] Ibid.

[106] Ibid.

[107] Ibid.

numerous social functions and uses and the reason why these functions make data incompatible with property are not discussed.

Some scholars go even further and state that a general protection of information is unthinkable in a democratic society, because it would result in the exclusive allocation of information to a person, which is incompatible with a social system based on discourse.[108] With regard to the right of possession, there is potential to ensure that access to data is universal.[109] Therefore, there is no need for an *erga omnes* right, but rather for an order as to who is allowed to dispose of the personal data, in which relationship and how.[110] Ultimately, the arguments presented, along with the concerns about the impracticality of data ownership affirm that data ownership does not need to be created *de lege ferenda*.[111] As mentioned above, the Data Act also does not envisage ownership rights to data, which is to be welcomed.[112] Therefore, a more nuanced approach, rather than an *erga omnes* right, is better suited to address the complexities of allocating rights to personal data.

2. Specific ownership-like rights to data

The previous paragraphs have shown that there is no ownership of data, neither *de lege lata* nor *de lege ferenda*. The question thus arises whether other rights to data can put individuals in an ownership-like position. This aspect of ownership-like rights to data is the subject of the following paragraphs.

a) Right to data according to the Database Directive

In EU law, the Database Directive[113] specifically protects database rights. Article 1 (2) of the Directive states that '"database" shall mean a collection of […] data

---

[108] T. Heymann, 'Der Schutz von Daten bei der Cloud Verarbeitung' (*supra* Chapter IV. note 18), p. 810; however Schwartz argues that a personal data as public good 'does not preclude the propertisation of personal data', P.M. Schwartz, 'Property, Privacy, and Personal Data' (*supra* Chapter I. note 14), p. 2090.

[109] T. Hoeren, 'Datenbesitz statt Dateneigentum' (*supra* Chapter IV. note 32), p. 8.

[110] A. Roßnagel, 'Fahrzeugdaten – wer darf über sie entscheiden?' (*supra* Chapter IV. note 79), p. 283; see also V. Janeček, 'Ownership of personal data in the Internet of Things' (*supra* Chapter IV. note 2), p. 1051.

[111] M. Dorner, 'Big Data und Dateneigentum' (*supra* Chapter IV. note 23), p. 626; A. De Franceschi and M. Lehmann, 'Data as Tradeable Commodity and New Measures for their Protection', 1 *The Italian Law Journal* (2015), p. 55; A. Gärtner and K. Brimsted, 'Let's Talk about Data Ownership', 39 *European Intellectual Property Review* (2017), p. 464.

[112] See also M. Hennemann and B. Steinrötter, 'Data Act – Fundament des neuen EU-Datenwirtschaftsrechts?' (*supra* Chapter IV. note 10), p. 1486.

[113] Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases (Database Directive), [1996] OJ L 77/20.

[…] arranged in a systematic or methodical way […]'.[114] As a condition of protection, Article 7 (1) of the Database Directive requires a qualitatively or quantitatively substantial investment in the obtaining, verification or presentation of the contents of a database.[115] The objective of the Directive is to provide investment protection for the producer of the database.[116] It could be argued that a ownership-like right to data is established by this Directive.

The Database Directive protects the investment in the data collected, analysed or provided, but not the investment in the data produced.[117] The CJEU clarified the difference in its *The British Horseracing Board* and *Fixtures Marketing* judgments.[118] The CJEU held that the Database Directive is intended to promote the protection of already existing information and not information that is subsequently created.[119] Similarly, in the *Football Dataco* case the CJEU limited the legal protection to the investment of already existing data collections and thus did not consider an investment in the generation of new data as justifying protection.[120] Therefore, the Database Directive protects an existing data collection and investments made in this context.[121]

The Database Directive also provides copyright, but clearly states that it is not the content of the databases that is protected.[122] Hence, copyright protection does not exist for data itself, but only for originally created databases.[123] The CJEU also specified that it is not the data itself, but the database that is the object of protection under the Directive.[124] Consequently, creators of databases will rarely be able to invoke copyright, as the requirements of originality of the database as such certainly limit that.[125]

---

[114] See Article 1 (1) Database Directive.

[115] See Article 7 (1) Database Directive.

[116] See Recital 48 Database Directive; P. De Filippi and L. Maurel, 'The paradoxes of open data and how to get rid of it? Analysing the interplay between open data and sui-generis rights on databases', 23 *International Journal of Law and Information Technology* (2015), p. 5.

[117] I. Stepanov, 'Introducing a property right over data in the EU: the data producer's right – an evaluation' (*supra* Chapter IV. note 49), p. 71.

[118] See Cases C-203/02 *The British Horseracing Board*, EU:C:2004:695, para. 31 and C-444/02 *Fixtures Marketing*, EU:C:2004:697, para. 40.

[119] Ibid.

[120] See Case C-604/10 *Football Dataco*, EU:C:2012:115, para. 34.

[121] J. Ensthaler, 'Industrie 4.0 und die Berechtigung an Daten' (*supra* Chapter IV. note 50), p. 3475.

[122] See Recitals 15 and 46 Database Directive.

[123] I. Stepanov, 'Introducing a property right over data in the EU: the data producer's right – an evaluation' (*supra* Chapter IV. note 49), p. 71; P. De Filippi and L. Maurel, 'The paradoxes of open data and how to get rid of it? Analysing the interplay between open data and sui-generis rights on databases' (*supra* Chapter IV. note 116), p. 4; M. Dorner, 'Big Data und Dateneigentum' (*supra* Chapter IV. note 23), p. 622.

[124] See Case C-203/02 *The British Horseracing Board* (*supra* Chapter IV. note 118), para. 72; Case C-604/10 *Football Dataco* (*supra* Chapter IV. note 120), para. 30.

[125] P. De Filippi and L. Maurel, 'The paradoxes of open data and how to get rid of it?

The reason for rejecting the argument that the Database Directive grants ownership-like rights to personal data is that a decision on data sovereignty on the basis of the criteria named in database law would be rather artificial.[126] Database law does not answer the question of the right to data, as that is not part of its normative purpose.[127] Furthermore, the concept of the Directive is quite complicated and case-specific, resulting in legal uncertainty.[128] Moreover, database investment protection does not grant a right to the individual database contents and can therefore not be used to establish an exclusive right to the data itself.[129] Rather, it illustrates the legislator's intention that data itself should remain free from exclusive legal allocation.[130] Consequently, no property right to data can be derived from the Directive.[131]

b) Right to data by means of trade secrets

The European Commission's Staff Working Document on the free flow of data and emerging issues of the European data economy further discusses whether a defensive right similar to know-how protection rules should be introduced. This right would entail a protection of *de facto* possession rather than ownership protection.[132] A set of purely defensive rights would protect the *de facto* holders of the data who set technical and organisational measures to protect the data from unauthorised access by third parties.[133]

Analysing the interplay between open data and sui-generis rights on databases' (*supra* Chapter IV. note 116), p. 5.

[126] J. Ensthaler, 'Industrie 4.0 und die Berechtigung an Daten' (*supra* Chapter IV. note 50), p. 3475.

[127] Ibid.

[128] P. De Filippi and L. Maurel, 'The paradoxes of open data and how to get rid of it? Analysing the interplay between open data and sui-generis rights on databases' (*supra* Chapter IV. note 116), p. 6.

[129] L. Specht, 'Ausschließlichkeitsrechte an Daten – Notwendigkeit, Schutzumfang, Alternativen' (*supra* Chapter IV. note 23), p. 294; N. Forgó, 'Daten als Gegenstand von sachenrechtlichen, datenschutz- und urheberrechtlichen Regelungen' (*supra* Chapter IV. note 21), p. 360; J. Froese and S. Straub, 'Wem gehören die Daten? – Rechtliche Aspekte der digitalen Souveränität in der Wirtschaft' (*supra* Chapter IV. note 16), p. 89; K. Zdanowiecki, 'Recht an den Daten' (*supra* Chapter IV. note 32), p. 22; H. Zech, 'Daten als Wirtschaftsgut – Überlegungen zu einem Recht des Datenerzeugers' (*supra* Chapter IV. note 4), p. 143.

[130] M. Dorner, 'Big Data und Dateneigentum' (*supra* Chapter IV. note 23), p. 622.

[131] I. Stepanov, 'Introducing a property right over data in the EU: the data producer's right – an evaluation' (*supra* Chapter IV. note 49), p. 71.

[132] Commission Staff Working Document (SWD 2017) 2 final (*supra* Chapter IV. note 57), p. 34.

[133] Ibid, p. 35; A. Wiebe, 'Von Datenrechten zu Datenzugang – Ein rechtlicher Rahmen für die europäische Datenwirtschaft' (*supra* Chapter IV. note 78), p. 89; H. Zech, 'Daten als Wirtschaftsgut – Überlegungen zu einem Recht des Datenerzeugers' (*supra* Chapter IV. note 4), p. 141.

The subject-matter of an exclusive right to data and an exclusive right to know-how is to a large extent identical, since know-how is also data that fulfils additional requirements for protection, namely that it is kept secret and is related to a business.[134] In this respect, know-how protection is a part of the possible exclusive right to data.[135] If this connection could be established, the discussion about an exclusive right to data and the future protection of know-how could possibly lead to a common result.[136]

Especially in the context of machine-generated data, the protection of trade and business secrets is becoming increasingly important.[137] These data are often used for product optimisation.[138] Personal data could be considered a trade or business secret if they are related to a business and the other requirements for protection are met.[139] The data will usually be related to the business in the Internet of Things.[140] Some personal data are not known to the public and there is an interest in keeping them secret because of their potential value to competitors.[141] Examples include customer lists, which would be a classic application of an exclusive right to data.[142] Nevertheless, private individuals could also be entitled to an exclusive right to data, which is why the protection of know-how could be presented as part of such an exclusive right.[143]

However, as the name suggests, the protection of trade or business secrets requires that a secret exists, which may not always be the case with personal data.[144] Consequently, not all data would be covered by trade secret protection and thus it would not be a comprehensive exclusive right.[145] Moreover, a constellation with several persons and companies could lead to problems as to whom

---

[134] L. Specht, 'Ausschließlichkeitsrechte an Daten – Notwendigkeit, Schutzumfang, Alternativen' (*supra* Chapter IV. note 23), p. 290; M. Dorner, 'Big Data und Dateneigentum' (*supra* Chapter IV. note 23), p. 622.

[135] L. Specht, 'Ausschließlichkeitsrechte an Daten – Notwendigkeit, Schutzumfang, Alternativen' (*supra* Chapter IV. note 23), p. 290.

[136] Ibid.

[137] J. Froese and S. Straub, 'Wem gehören die Daten? – Rechtliche Aspekte der digitalen Souveränität in der Wirtschaft' (*supra* Chapter IV. note 16), p. 89.

[138] M. Grützmacher, 'Dateneigentum – ein Flickenteppich' (*supra* Chapter IV. note 8), p. 488.

[139] L. Specht, 'Ausschließlichkeitsrechte an Daten – Notwendigkeit, Schutzumfang, Alternativen' (*supra* Chapter IV. note 23), p. 291.

[140] M. Grützmacher, 'Dateneigentum – ein Flickenteppich' (*supra* Chapter IV. note 8), p. 488.

[141] M. Dorner, 'Big Data und Dateneigentum' (*supra* Chapter IV. note 23), p. 623.

[142] L. Specht, 'Ausschließlichkeitsrechte an Daten – Notwendigkeit, Schutzumfang, Alternativen' (*supra* Chapter IV. note 23), p. 291.

[143] Ibid.

[144] N. Forgó, 'Daten als Gegenstand von sachenrechtlichen, datenschutz- und urheberrechtlichen Regelungen' (*supra* Chapter IV. note 21), p. 360.

[145] H. Zech, 'Data as a Tradeable Commodity' in A. De Franceschi (ed.), *European Contract Law and the Digital Single Market* (Intersentia, 2016), p. 63.

the secret is assigned to and hence who is the protected person.[146] Furthermore, the data can also be accessed without the consent of the trade secrets holder, given certain requirements are met, which contradicts an *erga omnes* approach.[147] In addition, the protection of trade secrets safeguards against certain infringements, but does not allocate personal data, which is inherent in ownership.[148] The model may also be contradicted by the fact that a complete disposal of the elements of personality as well as transfers of rights are excluded.[149] All in all, the majority of reasons therefore oppose the approach that trade secrets generally give rise to an ownership-like position regarding personal data.

c) Copyright law and patents as exclusive rights to data

Another approach would be to grant an exclusive right to data via copyright law. Copyright grants the creator of a work an exclusive, *erga omnes* right to it for a certain period of time.[150] The aim is to allow the creator to retain rights to the work in a long value chain (e.g. author – publisher – bookseller).[151] Personal data resembles intellectual property through its non-rivalry and non-excludability.[152] This similarity could be an argument for copyright as a place for an exclusive right to data.

Works within the meaning of, for example, the Austrian Copyright law need to be an original intellectual creation.[153] Personal data can therefore be protected by copyright if they are an original intellectual creation.[154] An example could be a novel manuscript stored on a computer.[155]

---

[146] Ibid, p. 64; M. Dorner, 'Big Data und Dateneigentum' (*supra* Chapter IV. note 23), p. 623; M. Grützmacher, 'Dateneigentum – ein Flickenteppich' (*supra* Chapter IV. note 8), p. 489.

[147] I. Stepanov, 'Introducing a property right over data in the EU: the data producer's right – an evaluation' (*supra* Chapter IV. note 49), p. 72.

[148] K. Zdanowiecki 'Recht an den Daten' (*supra* Chapter IV. note 32), p. 22; H. Zech, 'Daten als Wirtschaftsgut – Überlegungen zu einem Recht des Datenerzeugers' (*supra* Chapter IV. note 4), p. 140.

[149] L. Specht, 'Ausschließlichkeitsrechte an Daten – Notwendigkeit, Schutzumfang, Alternativen' (*supra* Chapter IV. note 23), p. 291.

[150] A. Schmid, K.-J. Schmidt and H. Zech, 'Rechte an Daten zum Stand der Diskussion' (*supra* Chapter IV. note 3), p. 630.

[151] A. Duisberg, 'Datenhoheit und Recht des Datenbankherstellers – Recht am Einzeldatum vs. Rechte an Datensammlungen' (*supra* Chapter IV. note 16), p. 18.

[152] I. Stepanov, 'Introducing a property right over data in the EU: the data producer's right – an evaluation' (*supra* Chapter IV. note 49), p. 77; G. Wagner, 'BGB § 823' (*supra* Chapter IV. note 32), para. 335.

[153] See Section 1 Urheberrechtsgesetz.

[154] A. Schmid, K.-J. Schmidt and H. Zech, 'Rechte an Daten zum Stand der Diskussion' (*supra* Chapter IV. note 3), p. 630.

[155] A. Kalle, 'Herausgabe von Daten in der Insolvenz' (*supra* Chapter IV. note 33), p. 40.

One difference between works protected by intellectual property and personal data is that these works require creative input and financial as well as time investment, while data is often a by-product.[156] Moreover, personal data will rarely be an original, individual creation.[157] Collecting email addresses, for example, is not an original intellectual creation.[158] Likewise, personal data usually do not constitute an invention, which is why patent protection is also not applicable.[159] Moreover, one reason for protecting intellectual property is that it can still be commercially released to the public, while data usually has an internal and not an external purpose.[160] Furthermore, traditional value chains have changed in the age of digitisation and the purpose of copyright is not necessarily applicable to the personal data economy.[161] The underlying principle of copyright is to protect the work of an author and not mere ideas and information.[162] The larger a dataset is, the more likely it is that intellectual property rights exist in only a fraction of it.[163]

Thus, there are many arguments against granting an exclusive right to personal data via copyright law. Ultimately, there is no need for copyright law to allocate personal data as an asset, because other approaches grant rights to data and secure the functioning of a potential data market for the time being.[164]

d) Contractual agreements

In contract law, exclusive rights to data could be granted. Due to their private autonomy, persons are free to agree rights to data individually.[165] For this pur-

---

[156] I. Stepanov, 'Introducing a property right over data in the EU: the data producer's right – an evaluation' (*supra* Chapter IV. note 49), p. 78; A. Schmid, K.-J. Schmidt and H. Zech, 'Rechte an Daten zum Stand der Diskussion' (*supra* Chapter IV. note 3), p. 630; M. Grützmacher, 'Dateneigentum – ein Flickenteppich' (*supra* Chapter IV. note 8), p. 488; H. Zech, 'Daten als Wirtschaftsgut – Überlegungen zu einem Recht des Datenerzeugers' (*supra* Chapter IV. note 4), p. 141.

[157] C. Peschel and S. Rockstroh, 'Big Data in der Industrie – Chancen und Risiken neuer datenbasierter Dienste' (*supra* Chapter IV. note 16), p. 572; F. Schuster and S. Hunzinger, 'Vor- und nachvertragliche Pflichten beim IT-Vertrag – Teil II: Nachvertragliche Pflichten' (*supra* Chapter IV. note 18), p. 279.

[158] A. Kalle, 'Herausgabe von Daten in der Insolvenz' (*supra* Chapter IV. note 33), p. 40.

[159] N. Forgó, 'Daten als Gegenstand von sachenrechtlichen, datenschutz- und urheberrechtlichen Regelungen' (*supra* Chapter IV. note 21), p. 360.

[160] I. Stepanov, 'Introducing a property right over data in the EU: the data producer's right – an evaluation' (*supra* Chapter IV. note 49), p. 78.

[161] A. Duisberg, 'Datenhoheit und Recht des Datenbankherstellers – Recht am Einzeldatum vs. Rechte an Datensammlungen' (*supra* Chapter IV. note 16), p. 18.

[162] I. Stepanov, 'Introducing a property right over data in the EU: the data producer's right – an evaluation' (*supra* Chapter IV. note 49), p. 71.

[163] A. Kalle, 'Herausgabe von Daten in der Insolvenz' (*supra* Chapter IV. note 33), p. 40.

[164] I. Stepanov, 'Introducing a property right over data in the EU: the data producer's right – an evaluation' (*supra* Chapter IV. note 49), p. 71.

[165] A. Kalle, 'Herausgabe von Daten in der Insolvenz' (*supra* Chapter IV. note 33), p. 40.

pose, technical and organisational measures must be implemented between the contracting parties to ensure that the rights to data retain their exclusivity.[166] Transparent rules could be established within the framework of contractual agreements, which would benefit fairness in the processing of personal data.[167] In addition, it should be determined who should have which rights of use and processing of the personal data.[168] Above all, it should be specified how the data is handled after termination of the contract. This raises the question of how the return of the data can be managed.[169]

Cloud computing is an everyday phenomenon where users store their data in a virtual space and pay the provider money for the service. It is an example of contractual agreements regarding the allocation of data. As mentioned above, the contract clauses usually stipulate that the cloud provider does not acquire any rights to the data, but that they remain with the user.[170] However, some terms and conditions stipulate that customer data may be used by the cloud provider for different purposes, such as advertising.[171] Yet, there is mostly no reference to property or property-like rights.[172]

Also widespread are companies that outsource personal data to external IT service providers for processing. The allocation of rights is arguably different in outsourcing than in cloud computing, as an external IT service provider edits and processes the data provided.[173] Nevertheless, contracts for the allocation of data are concluded in outsourcing.

There are several limits to private arrangements. First, there is a de facto power imbalance between the parties.[174] *Hornung/Goeble,* however, argue that consumer law could address this disparity.[175] *Heun/Assion* note that some con-

---

[166] H. Zech, 'Data as a Tradeable Commodity' (*supra* Chapter IV. note 145), p. 60.

[167] Ibid, p. 61.

[168] M. Dorner, 'Big Data und Dateneigentum' (*supra* Chapter IV. note 23), p. 628; K. Zdanowiecki, 'Recht an den Daten' (*supra* Chapter IV. note 32), p. 26.

[169] T. Hoeren and S. Pinelli, 'Daten im Rechtsverkehr – Überlegungen für ein allgemeines Datenvertragsrecht', 75 *JZ – Juristen Zeitung* (2020), p. 880.

[170] S. Bradshaw, C. Millard and I. Walden, 'Contracts for clouds: comparison and analysis of the Terms and Conditions of cloud computing services' (*supra* Chapter IV. note 34), p. 208; A. Boerding et al., 'Data Ownership – A Property Rights Approach from a European Perspective' (*supra* Chapter IV. note 5), p. 367; A. Kalle, 'Herausgabe von Daten in der Insolvenz' (*supra* Chapter IV. note 33), p. 41.

[171] S. Bradshaw, C. Millard and I. Walden, 'Contracts for clouds: comparison and analysis of the Terms and Conditions of cloud computing services'(*supra* Chapter IV. note 34), p. 208.

[172] Ibid, p. 209.

[173] M. Dorner, 'Big Data und Dateneigentum' (*supra* Chapter IV. note 23), p. 618; A. Kalle, 'Herausgabe von Daten in der Insolvenz' (*supra* Chapter IV. note 33), p. 41.

[174] T. Heymann, 'Der Schutz von Daten bei der Cloud Verarbeitung' (*supra* Chapter IV. note 18), p. 809; see also G. Hornung and T. Goeble, 'Data Ownership im vernetzten Automobil', 31 *CR – Computer und Recht* (2015), p. 270; H. Zech, 'Data as a Tradeable Commodity' (*supra* Chapter IV. note 145), p. 60; M. Dorner, 'Big Data und Dateneigentum' (*supra* Chapter IV. note 23), p. 626.

[175] G. Hornung and T. Goeble, 'Data Ownership im vernetzten Automobil' (*supra* Chap-

tracts could be rendered ineffective, when copyright law, consumer law and data protection law must be considered in contracts concerning personal data.[176] Second, often the data provider itself does not have complete control over the processing of the data, but rather outsources it to an external company.[177] Third, data is processed worldwide and thus in jurisdictions that grant different levels of protection.[178] Fourth, not only the data, interests and rights of the contracting parties are affected, but also those of third parties.[179] The problem is that these are also not *in rem* rights and thus only the contracting parties are bound by the agreement.[180] A third party could access the data and would not be held responsible under contract law.[181] This raises the question of the enforceability of contractual agreements.[182] Ultimately, a contractual arrangement does not clarify to whom the data is to be allocated and to whom it belongs.[183] Consequently, legal certainty is limited.[184] All in all, contractual agreements cannot generally be used to establish the allocation of personal data as an economic asset.

3. Bundle of rights to personal data under the GDPR

On the basis of the preceding explanations, it becomes apparent that ownership-like rights to personal data in the sense of property law do not exist and the creations of such rights is rightly viewed critically. Personal data usually do not fulfil the requirements to be covered by already existing *erga omnes* rights. The allocation and structuring of a property right over personal data, especially in the case of multi-personality, creates legal uncertainty. In addition, data protection law must always be considered in the case of these property rights, insofar as personal data are concerned.

---

ter IV. note 174), p. 271; see also, B. Weber, 'Datenschutz 4.0 – Daten als Wirtschaftsgut in digitalisierten Märkten' (*supra* Chapter IV. note 84), p. 115.

[176] S.-E. Heun and S. Assion, 'Internet(recht) der Dinge – Zum Aufeinandertreffen von Sachen- und Informationsrecht' (*supra* Chapter IV. note 31), p. 818.

[177] T. Heymann, 'Der Schutz von Daten bei der Cloud Verarbeitung' (*supra* Chapter IV. note 18), p. 809.

[178] Ibid.

[179] Ibid.

[180] I. Stepanov, 'Introducing a property right over data in the EU: the data producer's right – an evaluation' (*supra* Chapter IV. note 49), p. 73; H. Zech, 'Daten als Wirtschaftsgut – Überlegungen zu einem Recht des Datenerzeugers' (*supra* Chapter IV. note 4), p. 140.

[181] I. Stepanov, 'Introducing a property right over data in the EU: the data producer's right – an evaluation' (*supra* Chapter IV. note 49), p. 73; H. Zech, 'Data as a Tradeable Commodity' (*supra* Chapter IV. note 145), p. 60.

[182] T. Heymann, 'Der Schutz von Daten bei der Cloud Verarbeitung' (*supra* Chapter IV. note 18), p. 809.

[183] J. Ensthaler, 'Industrie 4.0 und die Berechtigung an Daten' (*supra* Chapter IV. note 50), p. 3474.

[184] H. Zech, 'Data as a Tradeable Commodity' (*supra* Chapter IV. note 145), p. 60.

However, EU data protection law in itself provides numerous rights for data subjects. It should therefore not only be interpreted as a restriction of rights allocation, but rather as a manifestation of numerous rights to personal data.[185] The individual rights of data subjects are described on the following pages and it is argued that they constitute a bundle of rights for data subjects that provides a secure legal position.[186] These rights are thus conceptually similar to the right to informational self-determination, which was defined by the German Federal Constitutional Court in its influential '*Volkszählungsurteil*' in 1983 as the right of individuals to determine in principle for themselves the disclosure and use of their personal data.[187] This right to informational self-determination is also described by *Albers* as a 'bundle of rights and obligations'.[188] It enables the commercialisation of personal data.[189] This bundle of rights strengthens informational self-determination.[190]

Only the rights under the GDPR will be addressed.[191] Especially its new rights have empowered data subjects.[192] Transparency is the underpinning principle of the rights of the data subject and enables control and knowledge of who is collecting personal data and for what purpose.[193] This is especially important for the

---

[185] See similarly P. Bräutigam, 'Das Nutzungsverhältnis bei sozialen Netzwerken – Zivilrechtlicher Austausch von IT-Leistung gegen personenbezogene Daten', 15 *MMR – Zeitschrift für IT-Recht und Recht der Digitalisierung* (2012), p. 639; Victor argues that the GDPR creates propertisation of personal data, J. M. Victor, 'The EU General Data Protection Regulation: Toward a Property Regime for Protecting Data Privacy', 123 *The Yale Law Journal* (2013), p. 522.

[186] In this sense already, W. Kilian, 'Strukturwandel der Privatheit' in H. Garstka and W. Coy (eds.), *Gedächtnisschrift für Wilhelm Steinmüller* (2014), p. 207; see also P.M. Schwartz, 'Property, Privacy, and Personal Data' (*supra* Chapter I. note 14), p. 2094.

[187] See BVerfG, 15.12.1983, I BvR 209/83, DE:BVerfG:1983:rs19831215.1bvr020983; Tzanou describes data protection as informational self-determination, M. Tzanou, 'Data protection as a fundamental right next to privacy? "Reconstructing" a not so new right', 3 *International Data Privacy Law* (2013), p. 89.

[188] See M. Albers, *Informationelle Selbstbestimmung* (*supra* Chapter I. note 22), p. 602; see, by contrast, critically about too much focus on informational self-determination: B.-J. Koops, 'The trouble with European data protection law', 4 *International Data Privacy Law* (2014), pp. 251–253.

[189] N. Czajkowski and M. Müller-ter Jung, 'Datenfinanzierte Premiumdienste und Fernabsatzrecht', 34 *CR – Computer und Recht* (2018), p. 161; P. Bräutigam, 'Das Nutzungsverhältnis bei sozialen Netzwerken – Zivilrechtlicher Austausch von IT-Leistung gegen personenbezogene Daten' (*supra* Chapter IV. note 185), p. 640.

[190] O. Lynskey, 'Deconstructing Data Protection: The "Added-Value" Of A Right To Data Protection in the EU Legal Order', 63 *International & Comparative Law Quarterly* (2014), p. 591; see also V. Reding, 'The European data protection framework for the twenty-first century', 2 *International Data Privacy Law* (2012), p. 125.

[191] See Chapter III 'Rights of the data subject' of the GDPR.

[192] G. De Gregorio, 'The rise of digital constitutionalism in the European Union', 19 *International Journal of Constitutional Law* (2021), p. 64.

[193] H. Greve, 'Artikel 12 Transparente Information, Kommunikation und Modalitäten' in G. Sydow (ed.), *Europäische Datenschutzgrundverordnung*, para. 1; see also Y. McDermott,

economic exploitation of personal data as described in Chapter III. 2., as this use would otherwise be relatively difficult for data subjects to comprehend.[194] These rights also have an impact on the data broker industry, which must act transparently and respect these rights, otherwise they will have to face fines and their business model will eventually perish.[195] This bundle of rights thus creates predictability for data subjects about the economic use of their personal data and strengthens their autonomy and data sovereignty.[196]

In addition, reasons will be given as to why the allocation of personal data as an economic asset to the data subjects and not to the data controllers makes sense. It will be argued that control over personal data in the form of a bundle of rights is an essential characteristic of empowerment over personal data and the economic use thereof.[197] Rights of disposition are provided.[198] They are an assertion of the data subject's control over his or her personal data.[199] There is therefore no need for an ownership right to data. Through the data subject rights, personal data as an economic asset is allocated to the data subject.

a) Right to be informed

Articles 13 and 14 GDPR grant the data subject comprehensive information rights. Article 13 concerns the case where the data controller has collected the data from the data subject.[200] Article 14 grants information rights if the data were not obtained from the data subject.[201] Since the two provisions are almost identical in content, only Article 13 will be discussed in the following paragraphs.

According to Article 13 (1) GDPR, the information to be given to the data subject shall include in particular the name and contact details of the data controller[202], the contact details of the data protection officer[203], the purposes and

---

'Conceptualising the right to data protection in an era of Big Data', 4 *Big Data & Society* (2017), p. 3.

[194] H. Greve, 'Artikel 12 Transparente Information, Kommunikation und Modalitäten' (*supra* Chapter IV. note 193), para. 1.

[195] See G. Birckan et al., 'Personal Data Protection and Its Reflexes on the Data Broker Industry' in R. Mugnaini (ed.), *Data and Information in Online Environments* (Springer Publishing, 2020), pp. 103–117.

[196] H. Greve, 'Artikel 12 Transparente Information, Kommunikation und Modalitäten' (*supra* Chapter IV. note 193), para. 2.

[197] See also C. Lazaro and D. Le Métayer, 'Control over Personal Data: True Remedy or Fairy Tale?' (*supra* Chapter I. note 15), p. 4.

[198] C. Langhanke and M. Schmidt-Kessel, 'Consumer Data as Consideration', 4 *Journal of European Consumer and Market Law* (2015), p. 220.

[199] G. Versaci, 'Personal Data and Contract Law: Challenges and Concerns about the Economic Exploitation of the Right to Data Protection' (*supra* Chapter I. note 8), p. 391.

[200] See Article 13 GDPR.

[201] See Article 14 GDPR.

[202] See Article 13 (1) (a) GDPR.

[203] See Article 13 (1) (b) GDPR.

legal basis of the processing[204], legitimate interests[205], recipients or categories of recipients[206], transfer to recipients in third countries or international organisation.[207] The right to be informed serves the purpose of fair and transparent data processing.[208] The information should be provided when the data is collected from the individual or otherwise within a reasonable time.[209] In addition, the information should principally not cost the data subject anything.[210]

Article 13 (2) GDPR stipulates further information requirements, namely: storage duration,[211] rights of the data subject,[212] withdrawal of consent,[213] right of complaint,[214] provision of personal data,[215] automated decision-making.[216] This paragraph differs from the previous one in that the information has to be necessary to ensure a fair and transparent processing. This implies that this information must be provided only when necessary. The division of the two paragraphs indicates a separate criterion.[217] Recital 60 states that necessity must consider the circumstances and context of the data processing.[218] Consequently, a case-by-case decision will be required.[219]

These information obligations do not apply if the data subject already has this information.[220] Information also does not have to be provided if legal provisions require the disclosure or storage of the data or the provision of information to the data subject is impossible or disproportionately burdensome.[221] The latter may be the case for archiving in the public interest or for scientific research.[222]

This right to be informed serves the purpose of effective legal assertion and is intended to provide the data subject with comprehensive knowledge about the use of personal data.[223] Furthermore, the right to be informed is intended to

---

[204] See Article 13 (1) (c) GDPR.
[205] See Article 13 (1) (d) GDPR.
[206] See Article 13 (1) (e) GDPR.
[207] See Article 13 (1) (f) GDPR.
[208] See Recital 60 GDPR.
[209] See Recital 61 GDPR.
[210] See Article 12 (5) GDPR.
[211] See Article 13 (2) (a) GDPR.
[212] See Article 13 (2) (b) GDPR.
[213] See Article 13 (2) (c) GDPR.
[214] See Article 13 (2) (d) GDPR.
[215] See Article 13 (2) (e) GDPR.
[216] See Article 13 (2) (f) GDPR.
[217] B. Paal and M. Hennemann, 'DSGVO Art. 13 Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person' in B. Paal and D. Pauly (eds.), *DS-GVO BDSG*, para. 22.
[218] See Recital 60 GDPR.
[219] B. Paal and M. Hennemann, 'DSGVO Art. 13 Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person' (*supra* Chapter IV. note 217), para. 23.
[220] See Article 13 (4) GDPR.
[221] See Recital 62 GDPR.
[222] Ibid.
[223] B. Paal and M. Hennemann, 'DSGVO Art. 13 Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person' (*supra* Chapter IV. note 217), para. 4.

reduce information asymmetries and inform data subjects about the consequences and risks of using, sharing and economically exploiting personal data.[224] Data subjects are given a fair and transparent insight into how their personal data is processed.[225] This also gives them insight into the economic use of their personal data. In this respect, this right can be used to argue that personal data as an asset should be attributed to the data subjects, as they would often have knowledge of who processes the data and how. This allocation would not create a society in which citizens can no longer be sure who knows what about them.[226] This right is precisely intended to create the possibility for data subjects to inform themselves at any times and thus create transparency about the data controllers and processors. The ability to maintain a transparent overview of multi-person constellations is ensured in particular through information about third parties. From a technological perspective, transparency enhancing technologies can enable data subjects to be aware of data processing activities and the use of personal data as an economic asset.[227] The right to information gives data subjects control over their personal data as an economic asset.

b) Right of access

The right of access, which is laid down in Article 15 GDPR, is intended to enable data subjects to verify for themselves whether their personal data is being processed lawfully.[228] The right of access differs from the right to be informed insofar as it is at the request of the data subject and the data subject has the right to obtain a confirmation from the data controller.[229]

The right of access should inform the data subject about the purposes of processing,[230] categories of personal data,[231] recipients or categories of recipients,[232] duration of storage and/or processing,[233] rights of the data subject,[234] right

---

[224] C. Lazaro and D. Le Métayer, 'Control over Personal Data: True Remedy or Fairy Tale?' (*supra* Chapter I. note 15), p. 10.

[225] A. Ingold, 'Artikel 13 Informationspflicht bei Erhebung von personenbezogenen Daten' in G. Sydow (ed.), *Europäische Datenschutzgrundverordnung*, para. 1.

[226] This would be incompatible with data protection law, as the German Federal Constitutional Court ruled BVerfG, I BvR 209/83 (*supra* Chapter IV. note 187), para. 146.

[227] C. Lazaro and D. Le Métayer, 'Control over Personal Data: True Remedy or Fairy Tale?' (*supra* Chapter I. note 15), p. 22.

[228] See Recital 63 GDPR.

[229] See Article 15 (1) GDPR.

[230] See Article 15 (1) (a) GDPR.

[231] See Article 15 (1) (b) GDPR.

[232] See Article 15 (1) (c) GDPR.

[233] See Article 15 (1) (d) GDPR.

[234] See Article 15 (1) (e) GDPR; see also Case C-307/22 *FT*, EU:C:2023:811, para. 73; Case C-579/21 *Pankki S*, EU:C:2023:501, para. 58; Case C-487/21 *Österreichische Datenschutzbehörde* (*supra* Chapter II. note 83), para. 35; Case C-154/21 *Österreichische Post*, EU:C:2023:3, para. 38.

of complaint,[235] origin of the personal data[236] and automated decision-making.[237] Recital 63 clarifies that health data are also covered by this right of access.[238] Examples include personal data in findings of the treating doctors, patient files, examination results, diagnoses and information on treatments or interventions.[239]

In addition, information must be provided on the transfer of personal data to a third country or to an international organisation.[240] Moreover, according to this provision, the data subjects are entitled to a free copy of this information.[241] However, the right to receive a copy should not affect the rights and freedoms of other persons.[242] Recital 63 mentions trade secrets, intellectual property rights and copyrights to software as examples of rights to be taken into account.[243] A balancing of fundamental rights can therefore be carried out.[244] However, these considerations should not lead to the exclusion of all information.[245]

Like the right to be informed, the right of access serves the purpose of effective legal protection.[246] It pursues the objective that data subjects receive a notification not only on the processed data, but also on purposes and intentions.[247] It therefore provides insight into whether and how processing takes place.[248] The right to of access is intended to enable data subjects to verify lawful processing.[249] This allows them to check whether and how their personal data is being used economically. Furthermore, the right of access is significant because it is enshrined in the Charter and thus in primary EU law.[250] The right of access is thus also

---

[235] See Article 15 (1) (f) GDPR.
[236] See Article 15 (1) (g) GDPR.
[237] See Article 15 (1) (h) GDPR.
[238] See Recital 63 GDPR.
[239] Ibid.
[240] See Article 15 (2) GDPR.
[241] See Article 15 (3) GDPR.
[242] See Article 15 (4) GDPR.
[243] See Recital 63 GDPR.
[244] B. Paal, 'DSGVO Art. 15 Auskunftsrecht der betroffenen Personen' in B. Paal and D. Pauly (eds.), *DS-GVO BDSG*, para. 41.
[245] See Recital 63 GDPR.
[246] B. Paal, 'DSGVO Art. 15 Auskunftsrecht der betroffenen Personen' (*supra* Chapter IV. note 244), para. 3.
[247] Ibid; See also, Recital 63 GDPR.
[248] B. Paal, 'DSGVO Art. 15 Auskunftsrecht der betroffenen Personen' (*supra* Chapter IV. note 244), para. 3.
[249] See Case C-307/22 *FT* (*supra* Chapter IV. note 234), para. 73; Case C-579/21 *Pankki S* (*supra* Chapter IV. note 234), para. 58; Case C-487/21 *Österreichische Datenschutzbehörde* (*supra* Chapter II. note 83), para. 34; Case C-154/21 *Österreichische Post* (*supra* Chapter IV. note 234), para. 37; L. Specht, 'Artikel 15 Auskunftsrecht der betroffenen Person' in G. Sydow (ed.), *Europäische Datenschutzgrundverordnung*, para. 1.
[250] See Article 8 (2) Charter.

a manifestation of the right to informational self-determination and the control of data subjects over their personal data.[251]

c) Right to rectification

Article 16 GDPR grants the data subject the right to rectify inaccurate personal data relating to them.[252] Personal data can be inaccurate if their content is untrue.[253] This refers to facts, as opinions and evaluations are not universally accurate.[254] In addition, data subjects have the right to have incomplete personal data completed.[255] The completeness of the personal data as such is not relevant, as it is highly unlikely that the data controller actually processes all personal data of a data subject.[256] Rather, it is crucial to have complete data in order to fulfil the purpose of the processing.[257] Furthermore, this leads to the obligation of the data controller to keep the personal data up to date under certain circumstances.[258] One of these circumstances could occur if outdated data would have a negative effect on the data subject, such as outdated data on a customer's (lack of) creditworthiness.[259]

Article 16 GDPR expresses the principle of data accuracy.[260] Accordingly, the CJEU has ruled that an essential characteristic of correct and lawful data processing is the accuracy of the personal data.[261] The right to rectification gives data subjects an essential tool to avert potentially negative consequences, especially in times of misinformation and fake news. It gives them control over their personal data.[262] This can be important if the economic use of inaccurate personal data leads to disadvantages for or discrimination against the data subject. The classification of people as price-sensitive or price-insensitive via cookies, for example, leads to personalised pricing, which can result in online price discrimination.[263]

---

[251] L. Specht, 'Artikel 15 Auskunftsrecht der betroffenen Person' (*supra* Chapter IV. note 249), para. 1.

[252] See Article 16 GDPR.

[253] B. Paal, 'DS-GVO Art. 16 Recht auf Berichtigung' in B. Paal and D. Pauly (eds.), *DS-GVO BDSG*, para. 15.

[254] Ibid.

[255] See Article 16 GDPR.

[256] B. Paal, 'DS-GVO Art. 16 Recht auf Berichtigung' (*supra* Chapter IV. note 253), para. 18.

[257] See Articles 5 (1) (d) and 16 GDPR; European Union Agency for Fundamental Rights and Council of Europe, *Handbook on European data protection law* (*supra* Chapter II. note 26), p. 127.

[258] See Article 5 (1) (d) GDPR.

[259] European Union Agency for Fundamental Rights and Council of Europe, *Handbook on European data protection law* (*supra* Chapter II. note 26), p. 128.

[260] See Article 5 (1) (d) GDPR.

[261] See Case C-553/07 *Rijkeboer* (*supra* Chapter II. note 45), para. 49.

[262] E. Peuker, 'Artikel 16 Recht auf Berichtigung' in G. Sydow (ed.), *Europäische Datenschutzgrundverordnung*, para. 2.

[263] F. Zuiderveen Borgesius and J. Poort, 'Online Price Discrimination and EU Data Privacy Law', 40 *Journal of Consumer Policy* (2017), p. 348.

Such price discrimination leads to higher corporate profits but greater economic and digital inequality.[264] Thus, personalised pricing is generally perceived as unfair.[265] Being able to rectify inaccurate personal data is therefore a step towards counteracting discrimination on the basis of inaccurate personal data. However, data subjects may often make use of the following option: the right to erasure.

d) Right to erasure

The right to erasure is set out in Article 17 GDPR and grants data subjects a comprehensive right to have his or her data deleted. In parentheses in the text of the GDPR and also frequently in academic discourse, it is called the 'right to be forgotten'. The scope and terminology of the right have always been source of debate. The choice of the term 'right to be forgotten' is certainly misleading because the right to erasure does not force anyone to forget, but merely obliges to delete personal data and thus prevents future access possibilities to personal data.[266]

Article 17 (1) GDPR provides legal grounds for erasure. Accordingly, data subject may request the erasure of their personal data if the purpose of the processing is no longer fulfilled[267], consent is withdrawn[268], data processing is objected to[269], data processing is unlawful[270], compliance with a legal obligation requires erasure[271] or personal data of children are concerned[272]. Another essential aspect of Article 17 GDPR is that the controller should also inform other controllers in the best way possible that the data subject has requested erasure.[273] The legislator mentions online networks and the sharing of links or contributions in particular.[274] This takes into account the phenomenon that indeed the Internet does not forget.[275]

---

[264] See for an overview: A.D. Chirita, 'The Rise of Big Data and The Loss of Privacy', 28 *MPI Studies on Intellectual Property and Competition Law* (2018), pp. 153–189.

[265] F. Zuiderveen Borgesius and J. Poort, 'Online Price Discrimination and EU Data Privacy Law' (*supra* Chapter IV. note 263), p. 354.

[266] N. Forgó, 'Daten als Gegenstand von sachenrechtlichen, datenschutz- und urheberrechtlichen Regelungen' (*supra* Chapter IV. note 21), p. 372; see also O. Lynskey, 'Control over Personal Data in a Digital Age: *Google Spain v AEPD and Mario Costeja Gonzalez*', 78 *The Modern Law Review* (2015), p. 528.

[267] See Article 17 (1) (a) GDPR.

[268] See Article 17 (1) (b) GDPR.

[269] See Article 17 (1) (c) GDPR.

[270] See Article 17 (1) (d) GDPR.

[271] See Article 17 (1) (e) GDPR.

[272] See Article 17 (1) (f) GDPR.

[273] See Article 17 (2) GDPR.

[274] See Recital 66 GDPR.

[275] N. Forgó, 'Daten als Gegenstand von sachenrechtlichen, datenschutz- und urheberrechtlichen Regelungen' (*supra* Chapter IV. note 21), p. 373.

The fact that an overly comprehensive right to erasure would be similar to a property claim to personal data harbours potential for conflict because it could interfere with the freedom of information and expression of third parties.[276] It is therefore notable that Article 17 (3) GDPR provides exceptions to deletion and addresses the balancing act between data protection and freedom of information.[277] Controllers are exempt from the obligation to erase personal data if the processing is necessary for the freedom of expression and information[278], a legal obligation or the performance of a task[279], public health[280], archival, scientific or historical research, statistical purposes[281] or the assertion, exercise or defence of legal claims[282].

The CJEU dealt with the right to erasure in the context of the interpretation of the DPD. The *Google Spain* judgment[283] on this issue gained notoriety not only because of the large number of discussions on the judgment,[284] but also because of its legal implications. Given that a detailed discussion of the judgment would go beyond the scope of this chapter, only the essential core statements of the judgment will be discussed in the following paragraphs

Attachment proceedings were held to recover debts from *Costeja González*, a Spanish citizen, in the 1990s due to financial difficulties, and when his name was entered in the Google search engine, links to articles in a daily newspaper about the attachment proceedings were displayed.[285] *Costeja González* requested that Google remove the links to the coverage, as the attachment proceedings had been completed for over 10 years at that point and therefore did not warrant a mention.[286]

First, the application of EU data protection law to search engine operators was affirmed in this judgment.[287] The CJEU then argued that search engines can significantly affect the fundamental rights of the data subject, as the list of search results potentially displays numerous aspects of the person's private life and thus a detailed profile of the person could be created.[288] In particular, the fundamental

---

[276] B. Paal, 'DS-GVO Art. 17 Recht auf Löschung (Recht auf Vergessenwerden)' in B. Paal and D. Pauly (eds.), *DS-GVO BDSG*, para. 9.

[277] Ibid, para. 10.

[278] See Article 17 (3) (a) GDPR.

[279] See Article 17 (3) (b) GDPR.

[280] See Article 17 (3) (c) GDPR.

[281] See Article 17 (3) (d) GDPR.

[282] See Article 17 (3) (e) GDPR.

[283] Case C-131/12 *Google Spain and Google*, EU:C:2014:317.

[284] See for example, the German discourse: J. Kühling, 'Rückkehr des Rechts: Verpflichtung von Google & Co. zu Datenschutz', 14 *EuZW – Europäische Zeitschrift für Wirtschaftsrecht* (2014), pp. 527–532; N. Nolte, 'Das Recht auf Vergessenwerden – mehr als nur ein Hype?', 31 *NJW – Neue Juristische Wochenzeitschrift* (2014), pp. 2238–2242.

[285] Case C-131/12 *Google Spain and Google* (*supra* Chapter IV. note 283), para. 14.

[286] Ibid para. 15.

[287] Ibid para. 68.

[288] Ibid para. 80.

rights of the data subject under Articles 7 and 8 of the Charter must be taken into account.[289] In the balancing process, the interests of the data subject generally outweigh the economic interests of the search engine operator and the interests of the internet users.[290] When weighing the interests of the data subject against the right of internet users to information in particular, consideration must be given to whether the personal data is sensitive or whether the affected person is a public figure.[291] The CJEU affirmed the search engine operator's obligation to delete the links and ruled that this can also be the case if the publication of the information on third party web pages was lawful.[292] In *Costeja González's* case, the sensitive nature of the information and the fact that the articles were 16 years old, in particular, supported the deletion of the links.[293]

The scope of the right to erasure is made evident by this judgment. It 'endorses the individual control over personal data'.[294] However, it must not be understood as a manifestation of an absolute right to personal data. Correctly, the CJEU has ruled several times that the fundamental right to protection of personal data must always be interpreted according to is function in society and balanced against other fundamental rights.[295] Similarly, in the *Volkszählungsurteil*, the German Federal Constitutional Court already ruled in 1983 that individuals do not have absolute, unrestricted sovereignty over their personal data, as personal data is part of social reality and thus must be considered in the relationship between the individual and the society.[296]

Nevertheless, the right to erasure provides the data subject with a comprehensive power of disposition.[297] Firstly, the right to erasure, as part of the fundamen-

---

[289] Ibid para. 81.

[290] Ibid paras. 81, 97, 99.

[291] Ibid.

[292] Ibid paras. 88 and 99.

[293] Ibid, para. 99.

[294] O. Lynskey, 'Control over Personal Data in a Digital Age: *Google Spain v AEPD and Mario Costeja Gonzalez*' (*supra* Chapter IV. note 266), p. 529.

[295] See Case C-154/21 *Österreichische Post* (*supra* Chapter IV. note 234), para. 47; Case C-311/18 *Facebook Ireland and Schrems*, EU:C:2020:559, para. 172; Case C-184/20 *Vyriausioji tarnybinės etikos komisija*, EU:C:2022:601, para. 70; Case C-136/17 *GC and* Others, EU:C:2019:773, para. 57; Case C-507/17 *Google* EUC:2019:772, para. 60; Case C-291/12 *Schwarz* (*supra* Chapter II. note 131), para. 33; Case C-543/09 *Deutsche Telekom*, EU:C:2011:279, para. 51; Case C-92/09 *Volker und Markus Schecke und Eifert* (*supra* Chapter II. note 184), para. 48.

[296] See BVerfG, I BvR 209/83 (*supra* Chapter IV. note 187), para. 148; See also BGH, 23.06.2009, VI ZR 196/08, para. 30.

[297] A. Boerding et al., 'Data Ownership – A Property Rights Approach from a European Perspective' (*supra* Chapter IV. note 5), p. 331; E. Peuker, 'Artikel 17 Recht auf Löschung ("Recht auf Vergessenwerden")' in G. Sydow (ed.), *Europäische Datenschutzgrundverordnung*, para. 1; E. Douilhet and A. P. Karanasiou, 'Legal Responses to the Commodification of Personal Data in the Era of Big Data: The Paradigm Shift From Data Protection Towards Data Ownership' in Information Resources Management Association (ed.), *Web Services:*

tal rights to respect for private life and data protection, provides a person with control over personal data relating to him or her.[298] Due to its fundamental rights character, the right to erasure cannot be waived.[299] Secondly, the CJEU's balancing of fundamental rights is often in favour of the data subject. Thirdly, the right to erasure has practical significance, as data subjects make use of the right to erasure.[300] Since the *Google Spain* judgment in 2014, Google has received 1.5 million requests to delist results for queries on the basis of a person's name .[301] Finally, although the individual cannot be granted unrestricted sovereignty over the data concerning him or her, this does not oppose a control over the data in principle that is limited by corresponding provisions.[302] All in all, the right to erasure provides data subjects with comprehensive control over the economic use of their personal data.

e) Right to restriction of processing

In accordance with Article 18 GDPR, the data subject may request the restriction of processing from the controller if the accuracy of the data is disputed,[303] no deletion is requested,[304] the restriction is necessary for legal claims[305] or an objection has been issued pursuant to Article 21 GDPR.[306] To implement a restriction, the personal data may be transferred to another processing system, made inaccessible to users or temporarily removed.[307] Thus, data subjects can limit how a company uses their personal data and, for example, restrict their economic exploitation. The right to restriction of processing may be considered as a lesser remedy compared to the right to erasure.[308] Nevertheless, it gives data subjects a

---

Concepts, Methodologies, Tools, and Applications (IGI Global, 2019), p. 2079; J. M. Victor, 'The EU General Data Protection Regulation: Toward a Property Regime for Protecting Data Privacy' (*supra* Chapter IV. note 185), p. 524.

[298] See also H.-G. Kamann and M. Braun, 'Art. 17 Recht auf Löschung ("Recht auf Vergessenwerden")' in E. Ehmann and M. Selmayr (eds.), *DS-GVO Datenschutz-Grundverordnung*, para. 8.

[299] Ibid.

[300] Ibid, para. 7.

[301] Google, *Transparency Report*, https://transparencyreport.google.com/eu-privacy/overview?delisted_urls=start:1401235200000;end:1634687999999;country:AT&lu=delisted_urls (accessed 31 January 2024).

[302] L. Specht, 'Ausschließlichkeitsrechte an Daten – Notwendigkeit, Schutzumfang, Alternativen' (*supra* Chapter IV. note 23), p. 293.

[303] See Article 18 (1) (a) GDPR.

[304] See Article 18 (1) (b) GDPR.

[305] See Article 18 (1) (c) GDPR.

[306] See Article 18 (1) (d) GDPR.

[307] See Recital 67 GDPR.

[308] B. Paal, 'DS-GVO Art. 18 Recht auf Einschränkung der Verarbeitung' in B. Paal and D. Pauly (eds.), *DS-GVO BDSG*, para. 3.

complementary means of exercising control and governance over their personal data, in addition to rectification and erasure.[309]

f) Right to data portability

The right to data portability referred to in Article 20 GDPR is intended to enable the data subject both to obtain his or her own personal data from the controller and to transfer the personal data to another controller.[310] The data subject must have provided the personal data to the data controller.[311] In addition, there are two conditions for the applicability of Article 20 GDPR. First, the processing has to be based on either consent or contract.[312] Second, the processing has to be done by automated means.[313] Furthermore, the data subject also has the option of the personal data being transferred directly from one controller to another.[314] This right aims to prevent the so-called 'lock-in effect', i.e. that certain obstacles make it difficult for users to change a product or a provider.[315] Should the personal data concern third parties, the different interests and freedoms must be assessed.[316]

As described in Chapter III. 2., a handful of companies have a hegemony in the digital economy and in the economic use of personal data. The right to data portability is highlighted as a way to give more control to data subjects and to reduce the market power of some companies.[317] Recital 68 GDPR explicitly mentions that the right to data portability is intended to 'further strengthen the control over his or her own data'.[318] Data subjects are thus deliberately empowered to actively dispose of their personal data.[319] The right to data portability, like the other data subject rights, aims to improve the control of data subjects over

---

[309] H.-G. Kamann and M. Braun, 'Art. 18 Recht auf Einschränkung der Verarbeitung' in E. Ehmann and M. Selmayr (eds.), *DS-GVO Datenschutz-Grundverordnung*, para. 2; E. Peuker, 'Artikel 18 Recht auf Einschränkung der Verarbeitung' in G. Sydow (ed.), *Europäische Datenschutzgrundverordnung*, para. 2.

[310] See Article 20 (1) GDPR.

[311] Ibid.

[312] See Article 20 (1) (a) GDPR; Recital 68 GDPR.

[313] See Article 20 (1) (b) GDPR.

[314] See Article 20 (2) GDPR; Recital 68 GDPR.

[315] B. Paal, 'DS-GVO Art. 20 Recht auf Datenübertragbarkeit' in B. Paal and D. Pauly (eds.), *DS-GVO BDSG*, para. 6; G. Sydow and M. Wilhelm, 'Artikel 20 Recht auf Datenübertragbarkeit' in G. Sydow (ed.), *Europäische Datenschutzgrundverordnung*, para. 1.

[316] See Article 20 (4) GDPR; Recital 68 GDPR.

[317] European Data Protection Supervisor, *Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy*, 26 March 2014, p. 36.

[318] See Recital 68 GDPR.

[319] Article 29 Working Party Guidelines on the right to data portability, 5 April 2017 ('WP242'), p. 4; see similarly, A. Boerding et al., 'Data Ownership – A Property Rights Approach from a European Perspective' (*supra* Chapter IV. note 5), p. 331.

their personal data.[320] The right to data portability guarantees more fairness and more control for the data subject.[321] They can withdraw the asset that is personal data from their counterpart and switch it to someone else, just as money can be given from one bank to another. Data portability is thus intended to create synergy effects in competition law and data protection law.[322] It is therefore hardly surprising that the Digital Markets Act, which aims to make the EU markets in the digital sector fairer and more contestable, also stipulates effective data portability continuously and in real-time.[323] The Data Act also provides for a right to data portability.[324]

It is understandable that this can be frustrating for data controllers, as they have made investments to process the data and then even have to transmit the data to the competition.[325] However, it should not be forgotten that the personal data originated because of the data subjects concerned. Without data subjects, there is no personal data. Without data controllers to process and enrich the personal data, they may be worth less, but they nevertheless exist. This may sound like the 'chicken-or-egg'-dilemma, but it is the right approach that data subjects are given control. All in all, the right to data portability helps to 're-balance' the relationship between data controllers and data subjects, strengthens individuals' control over their personal data and thus lets them decide on the economic use of their personal data.[326]

g) Right to object

The right of the data subject to object to the processing of personal data covers three forms of processing: processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority or for the

---

[320] H.-G. Kamann and M. Braun, 'Art. 20 Recht auf Datenübertragbarkeit' in E. Ehmann and M. Selmayr (eds.), *DS-GVO Datenschutz-Grundverordnung*, para. 4; G. Sydow and M. Wilhelm, 'Artikel 20 Recht auf Datenübertragbarkeit' (*supra* Chapter IV. note 315), para. 1; Graef, Husovec and Purtova argue that the right to data portability only provides limited control, I. Graef, M. Husovec and N. Purtova, 'Data Portability and Data Control: Lessons for an Emerging Concept in EU law', 19 *German Law Journal* (2018), p. 1369.

[321] European Data Protection Supervisor, *EDPS Opinion on coherent enforcement of fundamental rights in the age of big data (Opinion 8/2016)*, 23 September 2016, p. 12.

[322] European Data Protection Supervisor, *Privacy and competitiveness in the age of big data* (*supra* Chapter IV. note 317), p. 36.

[323] Article 6 (9) Regulation (EU) 2022/1925 of the European Parliament and the Council 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), [2022] OJ L 265/1.

[324] See Chapter VI Data Act.

[325] N. Forgó, 'Daten als Gegenstand von sachenrechtlichen, datenschutz- und urheberrechtlichen Regelungen' (*supra* Chapter IV. note 21), p. 376.

[326] WP242 (*supra* Chapter IV. note 319), p. 4; see also A. Gärtner and K. Brimsted, 'Let's Talk about Data Ownership' (*supra* Chapter IV. note 111), p. 465.

performance of a legitimate interest of the controller or of a third party[327], processing carried out for the purposes of direct marketing[328] and research or statistics[329]. This right is significant because it does not target unlawful processing, but lawful processing.[330] In addition, other data subject rights refer to the right to object.[331]

The right to object also imposes obligations on the data controller. Firstly, the data controller must prove that its legitimate interest outweighs the interests in the fundamental rights and freedoms of the data subject.[332] Secondly, the right to object must be explicitly and independently communicated to the data subject.[333]

This right also has a comprehensive scope. It strengthens the position of the data subject that it is also possible to object to lawful data processing. Thus, the right to object complements the other data subject rights and gives data subjects control over their personal data.[334] For data controllers, this right also has an impact, as it imposes a burden of proof on them in which they must demonstrate their relevant interests in further data processing.[335] This clear division and allocation of rights and obligations manifests the intention of the EU legislator to strengthen the control of the data subjects over their data and the fundamental right to data protection in times of digitalisation.[336] This intention is another reason why the allocation of personal data as an asset to the data subjects is correct. An allocation to the data controller would be accompanied by obligations and restrictions and would contradict the meaning and purpose of EU data protection law.

h) Right not to be subject to automated individual decision-making, including profiling

For the purpose of completeness, Article 22 GDPR should also be mentioned. It is part of Chapter III 'Rights of the Data Subjects' of the GDPR. However, this is

---

[327] See Article 21 (1) GDPR.

[328] See Article 21 (2) GDPR.

[329] See Article 21 (6) GDPR.

[330] M. Martini, 'DS-GVO Art. 21 Widerspruchsrecht' in B. Paal and D. Pauly (eds.), *DS-GVO BDSG*, para. 2.

[331] Ibid; see Articles 17 (1) (c) and 18 (1) (d) GDPR.

[332] See Article 21 (1) GDPR; Recital 69 GDPR.

[333] See Article 21 (4) GDPR; Recital 70 GDPR.

[334] See also H.-G. Kamann and M. Braun, 'Art. 21 Widerspruchsrecht' in E. Ehmann and M. Selmayr (eds.), *DS-GVO Datenschutz-Grundverordnung*, para. 2; J. M. Victor, 'The EU General Data Protection Regulation: Toward a Property Regime for Protecting Data Privacy' (*supra* Chapter IV. note 185), p. 523.

[335] Joined Cases C-26/22 and C-64/22 *SCHUFA Holding*, EU:C:2023:958, para. 111.

[336] M. Martini, 'DS-GVO Art. 21 Widerspruchsrecht' (*supra* Chapter IV. note 330), para. 81.

less a right of the data subject and more a general prohibition.[337] Only in the rarest of cases should an automated individual decision be made without human involvement.[338]

This provision is particularly significant due to the increasing importance of artificial intelligence in the interconnected society. For the purpose of this chapter, it is sufficient to note that Article 22 GDPR explicitly defines human legal relationships and thus data as an asset allocated to humans as the rule. Whether personal data can be considered an economic asset of artificial intelligence in the future remains to be seen.

Already a reality is the use of artificial intelligence and algorithms to create profiles of individuals, as described in Chapter III. 2. This data processing may involve different types of personal data, such as search results from internet users, data on consumers' habits, activities and lifestyles, as well as personal data originating in particular from social networks.[339] This oftentimes economic exploitation of personal data can have an impact on data subjects by assigning them to predetermined categories, often without their knowledge.[340] To counter this phenomenon, Article 22 GDPR allows data subjects to exercise control over the use they make of their identity without being assigned to categories and subject to automated decisions based on profiling.[341]

i) Strong legal position through GDPR

Of course, not all data subjects are a *Max Schrems* and are aware of their data rights, not all data controllers send detailed information about data processing and even privacy advocates do not always know exactly where, when and how their personal data is processed, as *Koops* correctly points out.[342] Nevertheless, *Boerding et al.* rightly describe the GDPR as 'a step towards "data sovereignty"'.[343] This approach would support a private autonomous interpretation of the GDPR.[344] The GDPR establishes eight data subject rights. This bundle of rights gives the data subject a strong legal position. This is similar to the position of

---

[337] M. Martini, 'DS-GVO Art. 22 Automatisierte Entscheidungen im Einzelfall einschließlich Profiling' in B. Paal and D. Pauly (eds.), *DS-GVO BDSG*, para. 1.

[338] See Recital 71 GDPR.

[339] J. Hladjk, 'Art. 22 Automatisierte Entscheidungen im Einzelfall einschließlich Profiling' in E. Ehmann and M. Selmayr (eds.), *DS-GVO Datenschutz-Grundverordnung*, para. 2.

[340] Ibid.

[341] Ibid, para. 3.

[342] B.-J. Koops, 'The trouble with European data protection law' (*supra* Chapter IV. note 188), p. 252.

[343] A. Boerding et al., 'Data Ownership – A Property Rights Approach from a European Perspective' (*supra* Chapter IV. note 5), p. 331.

[344] See on the private autonomous interpretation in the case of consent, A. Sattler, 'Personenbezogene Daten als Leistungsgegenstand' (*supra* Chapter IV. note 18), p. 1043.

an owner,[345] but not the same, as it is not a matter of *erga omnes* rights per se. Nevertheless, rights of disposition are provided.[346] They are an assertion of the data subject's control over his or her personal data.[347] There is therefore no need for an ownership right to data.

Through the data subject rights, personal data as an economic asset is allocated to the data subject. This allocation is logical. Firstly, the origin of personal data is with the data subjects. Secondly, this is in line with the meaning and purpose of data protection law. Thirdly, the GDPR explicitly assigns the control of personal data to the data subjects in Recital 7.[348] Having control over something is inherent to rights of disposition. Furthermore, this bundle of rights ensures the legal certainty for all stakeholders called for in Recital 7.[349] Consequently, data protection law assigns the value of personal data and the right to determine the use and commercialisation of personal data to the data subjects.[350]

Even though the commercialisation of personal data was described rather negatively in Chapter III., the allocation of personal data and its economic value do have positive effects, provided that personal data is allocated to data subjects and they can decide on its economic exploitation.[351] A positive effect, for example, could be that data subjects would be (more) aware of the value and power of their personal data.[352] *Bottis* and *Bouchagiar* go even further and argue that the economic use of personal data by data subjects would be positive for society and could also counteract poverty, as everyone could exchange their personal data in return for a (financial) benefit.[353]

---

[345] W. Kilian, 'Strukturwandel der Privatheit' (*supra* Chapter IV. note 186), p. 208.

[346] C. Langhanke and M. Schmidt-Kessel, 'Consumer Data as Consideration' (*supra* Chapter IV. note 198), p. 220.

[347] G. Versaci, 'Personal Data and Contract Law: Challenges and Concerns about the Economic Exploitation of the Right to Data Protection' (*supra* Chapter I. note 8), p. 391.

[348] See Recital 7 GDPR.

[349] Ibid.

[350] W. Reiners, 'Datenschutz in der Personal Data Economy – Eine Chance für Europa' (*supra* Chapter IV. note 18), p. 55.

[351] See regarding positive impact of attributing economic value to personal data: M. Bottis and G. Bouchagiar, 'Personal Data v. Big Data: Challenges of Commodification of Personal Data', 8 *Open Journal of Philosophy* (2018), p. 209.

[352] Ibid; G. Malgieri and B. Custers, 'Pricing privacy – the right to know the value of your personal data' (*supra* Chapter III. note 36), p. 302.

[353] M. Bottis and G. Bouchagiar, 'Personal Data v. Big Data: Challenges of Commodification of Personal Data' (*supra* Chapter IV. note 351), p. 211.

4. Conclusion: The data subject as the person entitled to the personal data

The purpose of this chapter was to illustrate that there is no ownership in German-speaking national legal systems and EU law and thus no owners of personal data in the private law sense. The desirability from a normative perspective to construct an allocation of rights on the basis of the storage medium was discussed. However, cloud services highlight that this approach is no longer up to date.

Since it is generally recognised that there is no ownership of personal data in the current German-Speaking legal framework and EU law, there has been a debate for years about whether to introduce an *erga omnes* property right in data. Proponents of this approach emphasise the resulting legal certainty and secure access to data. As has been shown, however, legal uncertainty exists specifically because of multipersonality. Moreover, no proposal as to who should be entitled to this right is fully convincing.

Proposals for investment protection, trade secrets, copyright or patent law as starting points for an *erga omnes* right to personal data are also misguided. Sometimes the personal data is explicitly excluded from the scope of application, then the secret or the originality is missing. Furthermore, contractual agreements may well grant exclusive rights to personal data, but it is inherent in the nature of contracts that they do not apply *erga omnes*, i.e. to everyone.

As the above has shown, EU data protection law grants numerous rights to data subjects. These rights grant them control and disposition over their personal data. These may not be unlimited and *erga omnes*, but they do provide a strong legal position.

Part of the control and disposition should also be the participation in the value of personal data. Data subjects should autonomously decide whether to make their personal data available in return for services. They should be free to decide on the commercialisation of their personal data, a phenomenon that can no longer be ignored. It is they who have the right to use their personal data as an economic asset. If the EU legislator fails to react to this phenomenon, privacy and data protection would be empty words that have nothing to do with reality. So has the EU reacted to this phenomenon and if so, how? This will be analysed in the following chapter.

V. EU regulation of personal data as an economic asset

In a preliminary opinion from 2014, the EDPS stated that data as an asset is the fuel of the digital economy.[1] The opinion also outlines that personal data is being used like a currency for services in the digital age.[2] In another opinion, the EDPS recognised that personal data is *de facto* already used as a means of payment and traded as a commodity.[3] To address the new developments of the data economy, the EU has adopted a number of policy measures in the past years. Its aim is to establish an adequate balance between promoting innovation and protecting fundamental rights: On the one hand, Europe should be an attractive location for companies in the data economy; on the other hand, the public's trust in new, often data-based technologies should be strengthened through a protective, legal framework. *De Gregorio* labels this phase of the EU as the era of 'digital constitutionalism'.[4]

This chapter provides an overview of EU instruments that deal with the data economy and data as an economic asset. What many of these instruments have in common is that they attempt to reconcile data protection and data commercialisation.[5] They demonstrate that the EU recognises personal data as an economic asset.[6] Section 1 is dedicated to the digital single market strategy and the data strategy. Section 2 addresses the GDPR. Section 3 examines the DCD in more detail.[7] Section 4 gives an overview of other EU legal instruments regarding data.

---

[1] European Data Protection Supervisor, *Privacy and competitiveness in the age of big data* (*supra* Chapter IV. note 317), p. 9.

[2] Ibid, p. 10.

[3] European Data Protection Supervisor, *Opinion 8/2016* (*supra* Chapter IV. note 321), p. 6.

[4] G. De Gregorio, 'The rise of digital constitutionalism in the European Union' (*supra* Chapter IV. note 192), pp. 56–60; see also G. De Gregorio, *Digital Constitutionalism in Europe – Reframing Rights and Powers in the Algorithmic Society* (Cambridge University Press, 2022).

[5] See also B. Schmitz, 'Digitale-Gesetze-Strategie – Agilität oder "Act"ionismus?', 12 *ZD – Zeitschrift für Datenschutz* (2022), p. 190; B. Custers and G. Malgieri, 'Priceless data: why the EU fundamental right to data protection is at odds with trade in personal data' (*supra* Chapter I. note 11), p. 11.

[6] See already A. De Franceschi and M. Lehmann, 'Data as Tradeable Commodity and New Measures for their Protection' (*supra* Chapter IV. note 111), p. 62.

[7] Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services, [2019] OJ L 136/1.

1. Digital Single Market Strategy and Data Strategy

With the Digital Single Market Strategy,[8] the EU has entered a new era in the digital age. This strategy set the goal of counteracting the legal fragmentation of digitalisation, i.e. legal frameworks regarding digitalisation differing from Member State to Member State. It aims to create cross-border frameworks. The strategy is based on three pillars: access to digital goods and services, creating a better environment for digital content and services and maximising the potential of the European digital economy. For the access pillar, uniform e-commerce rules,[9] affordable parcel delivery services,[10] no unjustified geo-blocking,[11] better access to digital content[12] and no unnecessary VAT[13] were defined as key objectives. To create the appropriate environment, an adaption of existing legal frameworks was emphasised.[14] The regulation of online platforms and illegal content on them were set as targets.[15] To strengthen the digital economy, the development of a data economy based on competition, interoperability and standardisation was mentioned.[16]

In addition, in 2020, the European Commission published its Data Strategy[17] with a focus on non-personal and personal data. This is a further development compared to the Digital Single Market Strategy, which focused more on access and the digital economy environment. In the Data Strategy, the free flow of data and the respect of the values created by the interplay of data protection law, competition law and consumer protection are presented as the vision.[18] It is to be welcomed that the empowerment of individuals in the exercise of their rights is mentioned as a core problem area.[19] The GDPR, in particular the right to data portability, and the creation of technical tools to decide who does what with personal data ('personal data spaces') are identified as opportunities for empowerment.[20]

---

[8] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – A Digital Single Market Strategy for Europe, COM(2015) 182 final.

[9] Ibid, p. 4.

[10] Ibid, p. 5.

[11] Ibid, p. 6.

[12] Ibid.

[13] Ibid, p. 8.

[14] Ibid, p. 10.

[15] Ibid, p. 11.

[16] Ibid, p. 15.

[17] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – A European strategy for data, COM(2020) 66 final.

[18] Ibid, p. 5.

[19] Ibid, p. 10.

[20] Ibid, p. 20.

These strategies demonstrate that the EU is active in addressing the challenges of the digital economy and data as a driving asset. But without subsequent implementation steps, they would remain mere empty words. The laws that were adopted by the EU to implement the strategies are therefore outlined below. Whether this legal framework facilitates the economic use of personal data remains to be seen.[21]

2. Protection of personal data by the GDPR

As is well known, the GDPR was adopted in 2016. Even though it did not come into force until 2018, it was in a sense a harbinger of things to come. Numerous legal efforts to adjust to the digital age followed the GDPR. One of the main contributions of the GDPR is certainly that it raised awareness about data protection. According to a 2020 study, 69 % of respondents had heard of the GDPR and 60 % were aware that they have a right to access data stored by local authorities.[22] In addition, on the occasion of the second birthday of the GDPR, the European Commission published an interim report whose title 'Data protection as a pillar of citizens empowerment […]' underlines the significance of the GDPR.[23] This report highlighted the enforcement of the GDPR through fines,[24] its mainly uniform application[25] and the empowerment of data subjects as achievements[26]. The latter was achieved through numerous data subject rights, as shown in the last chapter. Furthermore, the exemplary effect of the GDPR should be emphasised. As early as 2016, *Albrecht* correctly predicted that the GDPR would change data protection not only across Europe, but also worldwide.[27] The European Commission's report also argues that the GDPR can be seen as a catalyst for international data protection efforts.[28] The GDPR will not be discussed in further detail here because it is addressed in all parts of this work

[21] B. Custers and G. Malgieri, 'Priceless data: why the EU fundamental right to data protection is at odds with trade in personal data' (*supra* Chapter I. note 11), p. 5.

[22] European Union Agency for Fundamental Rights, *Your rights matter: Data protection and privacy – Fundamental Rights Survey* (Publications Office of the European Union, 2020), p. 12.

[23] See Communication from the Commission to the European Parliament and the Council, 'Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition – two years of application of the General Data Protection Regulation', COM(2020) 264 final ('Communication – two years of application of the General Data Protection Regulation').

[24] Ibid, p. 5.

[25] Ibid, p. 6.

[26] Ibid, p. 8.

[27] See J.P. Albrecht, 'How the GDPR Will Change the World', 2 *European Data Protection Law Review* (2016), pp. 287–289.

[28] Communication – two years of application of the General Data Protection Regulation, p. 3.

in the respective relevant aspects. In addition, the GDPR exclusively governs privacy aspects of data protection, but not economic aspects. This gap in secondary law makes the search for answers in primary law all the more urgent.

3. The Digital Content Directive

The DCD provides a framework for contracts governing the supply of digital content or digital services. It is worth noting that the European Commission's original proposal only referred explicitly to digital content and not to digital services.[29] The DCD defines digital content as 'data which are produced and supplied in digital form'.[30] According to the DCD, digital services include allowing the 'consumer to create, process, store or access data in digital form'[31] or allowing 'any […] interaction with data in digital form uploaded or created by […] users'[32]. This includes computer programmes, video, audio and music files, but also services hosting these files.[33] This means that companies such as Facebook, YouTube or Spotify are covered by the scope of the DCD. Accordingly, the DCD has a broad scope of application.[34] This broad scope of application is to be commended. It is also worth emphasising that the DCD distinguishes between data and their storage medium.[35] Accordingly, certain provisions of the DCD only apply to storage mediums that serve solely as carriers of digital content, as described in Chapter IV. 1. a).[36]

a) Contracting parties according to the DCD

The contracting parties are the trader and the consumer. Therefore, the DCD applies to B2C relationships. A trader provides digital content or digital services to the consumer.[37] Thus, a shop selling a video game to a consumer can also fall within the scope of the DCD.[38] According to the DCD, consumers, on the other

---

[29] See Proposal for a Directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content, COM(2015) 634 final.

[30] See Article 2 (1) DCD.

[31] See Article 2 (2) (a) DCD.

[32] See Article 2 (2) (b) DCD.

[33] See Recital 19 DCD.

[34] K. Sein and G. Spindler, 'The new Directive on Contracts for the Supply of Digital Content and Digital Services – Scope of Application and Trader's Obligation to Supply – Part 1', 15 *European Review of Contract Law* (2019), p. 262.

[35] H. Zech, 'Data as a Tradeable Commodity' (*supra* Chapter IV. note 145), p. 55.

[36] See Article 3 (3) DCD.

[37] See Article 3 (1) DCD.

[38] K. Sein and G. Spindler, 'The new Directive on Contracts for the Supply of Digital Content and Digital Services – Scope of Application and Trader's Obligation to Supply – Part 1' (*supra* Chapter V. note 34), p. 261.

hand, are persons who, in relation to the contract are 'acting […] outside that person's trade, business, craft or profession'.[39] Various rights and obligations are imposed on the two parties. The trader must provide the digital content or service without unnecessary delay.[40] In addition, the trader has an obligation to update the digital content or service in order to meet the conformity requirements.[41] If the trader does not comply with these obligations, he or she is liable.[42] The obligations are distributed quite one-sidedly because the obligations of the consumer are not further mentioned.[43] The rights of the consumer are the focus. The consumer can terminate the contract in case of a failure to provide the digital content or service.[44] In the event of non-conformity, the consumer can also demand that the agreed condition be restored or that the price be reduced.[45]

b) Personal data as an economic asset according to the DCD

The regulatory focus of the DCD are contracts for digital content and digital services. Indeed, the great achievement of the DCD is the scope of application concerning consideration. According to its Article 3, the DCD is applicable when a price is paid for the digital content or digital services. So far nothing new. The major novelty is that the DCD is also applicable if the consumer provides his or her personal data to the trader for the digital content or digital services.[46] The EU hereby recognises that in the digital age, content and services are often made available through 'payment' with personal data. It is thus acknowledged that personal data have an economic value and are used as an asset. This mention of personal data as consideration is an important legal step in the right direction.[47] It raises awareness that many digital contents and digital services are not free, but are financed with one's own personal data. In addition, the DCD refers to the GDPR and addresses the existing reality of the commercialisation of personal data, thus making an important contribution to the protection of data subjects.[48]

---

[39] See Article 2 (6) DCD.

[40] See Article 5 DCD.

[41] See Articles 7 and 8 DCD.

[42] See Article 11 DCD.

[43] A. Metzger, 'Data as Counter-Performance: What Rights and Duties do Parties Have?', 8 *JIPITEC* (2017), p. 6.

[44] See Article 13 DCD.

[45] See Article 14 DCD.

[46] See Article 3 (1) DCD.

[47] K. Sein and G. Spindler, 'The new Directive on Contracts for the Supply of Digital Content and Digital Services – Scope of Application and Trader's Obligation to Supply – Part 1' (*supra* Chapter V. note 34), p. 263; Z. Efroni, 'Gaps and opportunities: The rudimentary protection for "data-paying consumers" under new EU consumer protection law', 57 *Common Market Law Review* (2020), p. 811.

[48] A Metzger et al., 'Data-Related Aspects of the Digital Content Directive', 9 *JIPITEC* (2018), p. 94; N. Helberger, F. Zuiderveen Borgesius and A. Reyna, 'The perfect match? A

However, the classification of personal data as consideration does not only have a symbolic effect. In Austria, for instance, a distinction is made between gratuitous and non-gratuitous contracts. This distinction is important insofar as, for example, Austrian warranty law only applies to non-gratuitous contracts. Since personal data as consideration have not been classified as part of non-gratuitous contracts so far, the legal remedies of warranty law have remained inaccessible. With the implementation of the DCD into Austrian law, the legal provisions on non-gratuitous contracts and thus on warranty law now also apply to contracts in which personal data and not a monetary payment is given in return. Corresponding explicit provisions such as those in the DCD until its implementation into national law did not exist in Austria. Nevertheless, such contracts were covered by a corresponding interpretation of the remuneration requirement in Section 917 ABGB.[49]

The EDPS stressed that personal information should not be considered as a mere economic asset in the EU.[50] According to the EDPS, this concept is not compatible with the case law of the ECtHR on data protection.[51] Furthermore, it would not be in line with Article 8 of the Charter and Article 16 of the TFEU.[52] A more detailed argumentation as to why the concept of personal data as an economic asset is not compatible with data protection is not given.

Not only the EDPS, but also the German Data Ethics Commission has dealt with personal data as an economic asset. They stated that data trade must follow certain ethical principles.[53] The claim that the concept of commercialisation of personal data and thus personal data as an economic asset is incompatible with fundamental rights and data protection principles is not made by the German Data Ethics Commission.

c) Personal data as a counter-performance according to the original DCD proposal

Compared to the European Commission's original proposal of the DCD, the content of Article 3 has changed. Originally, the DCD was intended to apply if the consumer 'actively provides counter-performance other than money in the form of personal data or any other data.'[54] This wording further emphasises that

---

closer look at the relationship between EU consumer law and data protection law', 54 *Common Market Law Review* (2018), p. 1464.

[49] B. Zöchling-Jud, 'Daten als Leistung' in N. Forgó and B. Zöchling-Jud (eds.), *Das Vertragsrecht des ABGB auf dem Prüfstand: Überlegungen im digitalen Zeitalter* (Manz Verlag, 2018), pp. 239–272.

[50] European Data Protection Supervisor, *Opinion 8/2016* (*supra* Chapter IV. note 321), p. 7.

[51] Ibid.

[52] Ibid.

[53] Datenethikkommission, *Gutachten der Datenethikkommission*, 23 October 2019, p. 108.

[54] See Article 3 (1) DCD proposal.

individuals are free to decide about their personal data in the manner of an economic asset.

Presumably the wording has been changed because it has been subject of much criticism. In a 2019 report, the German Data Ethics Commission argued that the notion of personal data as counter-performance should be abandoned.[55] Legal scholars have also addressed the term 'personal data as counter-performance'.[56] Some authors view this concept as contradictory to the GDPR.[57] In particular, the consent of the data subject to data processing has been examined. According to the GDPR, consent must not only be freely given, but can also be withdrawn at any time.[58] This type of consent differs significantly from consent under contract law and the principle of *pacta sunt servanda*.[59] Moreover, consent must not be a condition of a service or contract.[60]

However, consent to contracts using personal data as counter-performance is compatible with both civil law and data protection law, as long as the consent is voluntarily given and does not include a waiver of the right to withdrawal.[61] This view of some legal scholars is to be followed. Within these requirements, it is argued that consent under the GDPR should be interpreted in support of private autonomy.[62]

However, if the 'consideration' is devaluated by the withdrawal shortly after the service has been provided, the question of the consequences under contract law is unavoidable and to what extent such consequences are compatible with EU primary and secondary law. *Custers* and *Malgieri* consider the fact that consent can be withdrawn at any time as one of the main reasons why the use of personal data as an economic asset is in conflict with the Charter.[63] They argue that be-

---

[55] Datenethikkommission, *Gutachten der Datenethikkommission*, 23 October 2019, p. 105.

[56] See *Specht* who favours the declaration of consent under data protection law as a counter-performance rather than the personal data itself; L. Specht, 'Daten als Gegenleistung – Verlangt die Digitalisierung nach einem neuen Vertragstypus?', 72 *JZ – Juristenzeitung* (2017), p. 768.

[57] N. Härting, 'Digital Goods und Datenschutz – Daten sparen oder monetarisieren?', 32 *CR – Computer und Recht* (2016), p. 738; Efroni refers to possible 'tensions' between the GDPR and the DCD, Z. Efroni, 'Gaps and opportunities: The rudimentary protection for "data-paying consumers" under new EU consumer protection law' (*supra* Chapter V. note 47), p. 806.

[58] See Article 7 (3) GDPR.

[59] G. Versaci, 'Personal Data and Contract Law: Challenges and Concerns about the Economic Exploitation of the Right to Data Protection' (*supra* Chapter I. note 8), p. 379.

[60] See Article 7 (4) GDPR.

[61] C. Langhanke and M. Schmidt-Kessel, 'Consumer Data as Consideration' (*supra* Chapter IV. note 198), p. 222; A. Metzger, 'Data as Counter-Performance: What Rights and Duties do Parties Have?' (*supra* Chapter V. note 43), p. 5; A. Metzger, 'Dienst gegen Daten: Ein synallagmatischer Vertrag', 216 *Archiv für civilistische Praxis* (2016), p. 824.

[62] A. Sattler, 'Personenbezogene Daten als Leistungsgegenstand' (*supra* Chapter IV. note 18), p. 1043.

[63] B. Custers and G. Malgieri, 'Priceless data: why the EU fundamental right to data protection is at odds with trade in personal data' (*supra* Chapter I. note 11), p. 10.

cause the prevalent legal basis for personal data processing is consent, individuals can exercise their data subject rights and withdraw their 'payment' at any time, leading to notable legal uncertainty in transactions.[64]

A look at German law offers a possible solution. While the DCD and the Austrian law do not regulate this case (and therefore foreseeably leave it to the judicial development of the law), Section 327q (2) BGB allows the entrepreneur to terminate the contract:

'If the consumer revokes a data protection consent given by him or her or objects to further processing of his or her personal data, the entrepreneur may terminate a contract that obliges him to provide a series of individual digital products or to provide a digital product on a permanent basis without observing a notice period […]'

It could be argued that this termination option *de facto* forces individuals to give their consent, otherwise they lose access to the digital product or digital service. This would indeed restrict the autonomy of data subjects and would not be compatible with the requirements of freely and voluntarily given consent, described in Chapter VII. 4. a) below, within the meaning of Article 8 (2) of the Charter. However, the autonomy of data subjects is secured in cases where there is a reasonable alternative means of access without requiring consent, which is also described in Chapter VII. 4. a) below.[65]

Personal data as a counter-performance, as it was termed in the original DCD proposal, is the subject of a whole chapter of an EDPS' opinion from 2017.[66] Again, the EDPS recognised the importance of personal data for the EU digital economy.[67] The EDPS also welcomed the attempt of the Union legislator to address the phenomenon of providing personal data in return for digital content or services.[68] Yet, the EDPS stressed again that personal data cannot be compared to money and, as part of a fundamental right, must not be monetised and commercialised.[69] Regarding the monetisation of personal data, the EDPS famously stated:

'There might well be a market for personal data, just like there is, tragically, a market for live human organs, but that does not mean that we can or should give that market the blessing of legislation. One cannot monetise and subject a fundamental right to a simple commercial transaction, even if it is the individual concerned by the data who is a party to the transaction.'[70]

---

[64] Ibid.

[65] A. Ingold, 'Artikel 7 Bedingungen für die Einwilligung' in G. Sydow (ed.), *Europäische Datenschutzgrundverordnung*, para. 33.

[66] European Data Protection Supervisor, *Opinion 4/2017* (*supra* Chapter I. note 6).

[67] Ibid, p. 7.

[68] Ibid.

[69] Ibid.

[70] Ibid.

There is surely no clearer criticism of the concept of personal data as commodity than to compare it to illegal organ trafficking. Remaining in this tone, it is also reiterated that terms such as 'digital currency' or 'paying with data' are 'dangerous'.[71] The opinion states that the rationale for this argument is that the concept of personal data as economic asset is not compatible with Article 8 of the Charter and principles provided by the GDPR.[72] The EDPS advised against the term 'personal data as counter-performance' as proposed by the European Commission, as the concept was not clearly defined, there was a lack of transparency and fairness and that the same personal data, unlike money, can also be given to another provider.[73] This topic will be explored in more detail in later chapters.

In the final version of the DCD, 'counter-performance' and 'active provision' are no longer mentioned. Presumably, this wording was not used in the final version in order to avoid clearly defining personal data as a commodity.[74] Ultimately, however, this change is rather of 'semantic, not a substantive' significance, as *Efroni* rightly argues.[75] The value of personal data is still acknowledged by the final version of the DCD.

4. Overview of other EU legal instruments regarding data

A comprehensive examination of all instruments would go beyond the scope of this work. Therefore an overview of the Data Governance Act and Data Act is given.

a) Data Governance Act

The Data Governance Act[76] is intended to regulate the sharing and re-use of public sector data to which third party rights exist (e.g. data protection rights and intellectual property rights). The Data Governance Act is relevant to this examination, as re-use is defined in Article 2 (2) as 'the use by natural or legal persons of data […] for commercial or non-commercial purposes'. It should be highlighted though that the proposal of the Data Governance Act addressed the sharing of data between companies in return for any kind of remuneration, while the final

[71] Ibid, note 27.

[72] Ibid, p. 8.

[73] Ibid, p. 9.

[74] K. Sein and G. Spindler, 'The new Directive on Contracts for the Supply of Digital Content and Digital Services – Scope of Application and Trader's Obligation to Supply – Part 1' (*supra* Chapter V. note 34), p. 263.

[75] Z. Efroni, 'Gaps and opportunities: The rudimentary protection for "data-paying consumers" under new EU consumer protection law' (*supra* Chapter V. note 47), p. 805.

[76] Regulation (EU) 2022/969 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act), OJ L 152/1.

text does not contain the word 'remuneration'.[77] Still, according to the final text, personal data may be used with the support of 'data intermediation services' who help data subjects to exercise their rights.[78] Furthermore, the Data Governance Act aims to promote increased sharing of personal data by introducing a concept of data altruism.[79] In addition to altruistic reasons for data use, the Data Governance Act is focused on strengthening trust in data intermediaries and the use and sharing of data in the EU.[80] From all these objectives, it is clear that the Data Governance Act recognises data as an economic asset and tries to address its better usability and tradability.[81] In addition, the Data Governance Act is remarkable because it refers to the concept of rights to data and virtually equates the protection of personal data with the protection of certain property rights.[82]

Some authors argue that the power derived from aggregated data should be restored to individuals through the legal mechanisms of Data trusts, i.e. a bottom-up approach.[83] Data trusts could act in the interest of the data subject and could provide their personal data to companies.[84] For this, data trusts could charge a fee for access to the personal data and distribute it to the data subject.[85] As a result, data subjects could participate economically in the exploitation of their personal data.[86] A variety of Data trusts would enable data subjects to select a Data trust aligned with their aspirations.[87] Data trusts could empower data subjects to use their personal data as an economic asset.

Data intermediaries are also worth highlighting in this context for the use of personal data as an economic asset. Data intermediaries can cultivate trust among various stakeholders by mitigating information imbalances and overseeing interactions between sellers and buyers.[88] Therefore, their economic signifi-

---

[77] See Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act), COM(2020) 767 final, p. 1.

[78] Recital 3 Data Governance Act.

[79] J. Ruohonen and S. Mickelsson, 'Reflections on the Data Governance Act', 2 *Digital Society* (2023), p. 2.

[80] Recital 3 Data Governance Act.

[81] See also B. Steinrötter, 'Datenaltruismus', 11 *ZD – Zeitschrift für Datenschutz* (2021), p. 61.

[82] See for example, Recital 6 Data Governance Act.

[83] S. Delacroix and N. D. Lawrence, 'Bottom-up data Trusts: disturbing the "one size fits all" approach to data governance', 9 *International Data Privacy Law* (2019), p. 240.

[84] L. Specht-Riemenschneider et al., 'Die Datentreuhand', 24 *MMR-Beilage* (2021), p. 28.

[85] Datenethikkommission, *Gutachten der Datenethikkommission*, 23 October 2019, p. 135; L. Specht-Riemenschneider et al., 'Die Datentreuhand' (*supra* Chapter V. note 84), p. 27.

[86] Datenethikkommission, *Gutachten der Datenethikkommission*, 23 October 2019, p. 135; L. Specht-Riemenschneider et al., 'Die Datentreuhand' (*supra* Chapter V. note 84), p. 27; see also C. Prince, 'Do consumers want to control their personal data? Empirical evidence', 110 *International Journal of Human-Computer Studies* (2018), p. 30.

[87] S. Delacroix and N. D. Lawrence, 'Bottom-up data Trusts: disturbing the "one size fits all" approach to data governance' (*supra* Chapter V. note 83), p. 241.

[88] L. von Ditfurth and G. Lienemann, 'The Data Governance Act: Promoting or Restricting Data Intermediaries', 23 *Competition and Regulation in Network Industries* (2022), p. 274.

cance stems from their capacity to minimise transaction expenses and streamline mutually advantageous and effective transactions.[89] Considering the emerging nature of data intermediaries and the limited scale of their markets, some authors have argued that this legislative intervention in these markets at this early stage is evidence that data intermediaries will play a central role in data markets.[90]

According to the Data Governance Act, data intermediaries have to put the data 'at the disposal of data users'.[91] As mentioned above, they help data subject to exercise their rights as per the GDPR.[92] Data intermediaries could thus theoretically support data subjects in exercising their rights as described in Chapter IV. However, neutrality is a central concept of the Data Governance Act.[93] As dual agents representing both parties in a transaction, intermediaries frequently encounter structural conflicts of interest.[94] The prevalence of conflicts is heightened in digital platforms compared to traditional intermediaries due to their proclivity for vertical and horizontal integration.[95] Furthermore, the final Data Governance Act, like the proposal, does not specify how data intermediaries can specifically assist data subjects in exercising their rights.[96] This lack of clarity could lead to further legal uncertainty in exercising data subject rights.[97]

A practical example for facilitating data intermediaries is *Gaia-X*, which was presented by the German and French Ministries of Economic Affairs in 2019. *Gaia-X* is a secure data infrastructure where data is shared and made available in a fair and trustworthy environment.[98] It aims to put users back in control by maintaining digital sovereignty and data sovereignty.[99] Data is stored and can be used in so-called 'data spaces' that adhere to high standards.[100] Similarly, *Solid* aims to let 'people store their data securely in decentralised data stores'.[101] The team responsible for *Solid* led by *Sir Tim Berners-Lee*, who is considered the inventor of the World Wide Web, claims that these data stores put all data under

[89] Ibid.

[90] L. von Ditfurth and G. Lienemann, 'The Data Governance Act: Promoting or Restricting Data Intermediaries' (*supra* Chapter V. note 88), p. 279.

[91] See Article 12 (a) Data Governance Act.

[92] See Article 10 (b) Data Governance Act.

[93] L. von Ditfurth and G. Lienemann, 'The Data Governance Act: Promoting or Restricting Data Intermediaries' (*supra* Chapter V. note 88), p. 282.

[94] Ibid, p. 276.

[95] Ibid.

[96] European Data Protection Board, *EDPB-EDPS Joint Opinion 03/2021 on the Proposal for a regulation of the European Parliament and of the Council on European data governance (Data Governance Act)*, 10 March 2021, p. 31.

[97] Ibid, p. 32.

[98] Gaia-X, *What is Gaia-X*, https://gaia-x.eu/what-is-gaia-x/ (accessed 31 January 2024).

[99] Ibid.

[100] Ibid.

[101] Solid, *Solid: Your data, your choice.*, https://solidproject.org (accessed 31 January 2024).

the control of the data subjects, empowering them and allowing them to freely decide whether and how their data is shared and accessed.[102]

It is also noteworthy that the Data Governance Act explicitly stipulates that public bodies can charge a fee for allowing the re-use of certain categories of data (which include personal data).[103] According to the Data Governance Act, this fee should be non-discriminatory, proportionate, objectively justified and should not restrict competition.[104] Furthermore, Article 6 (4) of the Data Governance Act imposes an obligation to public sector bodies to 'take measures to incentivise the re-use' of (personal) data.

Before the Data Governance Act was adopted, the EDPB and EDPS argued that it should be included in Article 6 of the Data Governance Act that the fees 'may duly take into account the costs incurred by public sector bodies for the pseudonymisation or anonymisation of personal data', as the pseudonymisation or anonymisation of personal data can be 'a complex, time-consuming and expensive task'.[105] In addition, they called for clarification on the proposed incentives, as they raised questions about consent to the re-use of personal data, as incentives could be an 'inappropriate pressure or influence upon the data subject' and render the consent invalid.[106] Nevertheless, the fee in the final text is certainly also evidence that data has an inherent monetary value, as described in Chapter III.

The requirements of data altruism organisations, the regime for data intermediaries and the conditions for the re-use of personal data will have to be considered also for the applicable data protection regimes.[107] The provisions of the Data Governance Act, support 'the data protection framework, under the common objective of establishing a data sharing environment based on sound fundamental rights'.[108] Consequently, the Data Governance Act will be highly relevant for the economic use of personal data and its compatibility with the Charter.

b) Data Act

While the Data Governance Act creates the processes and structures to facilitate the sharing of data between companies, individuals and the public sector, the Data Act was intended to clarify who can create value from data and under what

---

[102] Ibid.

[103] See Article 6 Data Governance Act.

[104] See Article 6 (2) Data Governance Act.

[105] European Data Protection Board, *EDPB-EDPS Joint Opinion 03/2021* (*supra* Chapter V. note 96), p. 26.

[106] Ibid.

[107] G. Comandé and G. Schneider, 'It's time: Leveraging the GDPR to shift the balance towards research-friendly EU data spaces', 59 *Common Market Law Review* (2022), p. 768.

[108] Ibid.

conditions.[109] It has been described as the centrepiece ('*Herzstück*') of EU data regulation.[110] The key aim of the Data Act has been to ensure 'fairness in the allocation of value from data among actors in the data economy and to foster access to and use of data' since its proposal.[111]

Chapter III of the Data Act states obligations for data holders legally obliged to make data available. Of particular interest is Article 9 of the Data Act which allows for compensation for making data available. This compensation has to be reasonable and, where the data recipient is a small or medium enterprise or a not-for profit research organisation, must not 'exceed the costs incurred in making the data available'.[112] Recital 42 of the proposal stated that 'these provisions should not be understood as paying for the data itself, but in the case of micro, small or medium-sized enterprises, for the costs incurred and investment required for making the data available'. This recital seemed to imply that large companies can use compensation in a way to monetise personal data.[113] In this regard, the EDPB and EDPS argued that personal data cannot be considered as a tradeable commodity.[114] In line with this view, Recital 46 of the adopted Data Act now stipulates that such compensation 'should not be understood to constitute payment for the data itself'. While this blanket assertion is rebutted in this work, it rather could be argued that micro, small or medium-sized enterprises in particular should see compensation as a possible incentive to monetise personal data.

The Data Act also recognises the reality of the data economy, i.e. that individual companies have dominance because of their accumulation of data.[115] It therefore seeks to facilitate data access by listing unfair contractual terms unilaterally imposed on micro, small and medium-sized companies.[116] These include contractual terms that prevent the party to 'access or control […] or exploit the value' of data.[117] Thus, it restricts the contractual freedom of companies, such as Google, Apple, Facebook, Amazon, Microsoft etc., and prevents 'take it or leave it'-contracts.[118] The proposal already stated that these provisions guarantee that contracts 'do not take advantage of imbalances in negotiating power' and protect 'the weaker contractual party in order to avoid unfair contracts'.[119] *Picht* and

[109] See Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act), COM/2022/68 final, p. 2.

[110] M. Hennemann and B. Steinrötter, 'Data Act – Fundament des neuen EU-Datenwirtschaftsrechts?' (*supra* Chapter IV. note 10), p. 1481.

[111] Proposal of the Data Act, p. 2.

[112] See Article 9 (2) and (4) Data Act.

[113] See also European Data Protection Board, *EDPB-EDPS Joint Opinion 2/2022 on the Proposal of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act),* 4 May 2022, p. 18.

[114] Ibid.

[115] See Recital 40 Data Act.

[116] See Chapter IV Data Act.

[117] See Article 13 (5) (c) Data Act.

[118] See already Proposal of the Data Act, p. 13.

[119] Ibid, p. 15.

Richter stress that not only Google, Apple, Facebook, Amazon and Microsoft, but also other companies that are not yet dominant but have or will have market power should be covered by this provision.[120] Notwithstanding this, this provision testifies to the fact that data is used economically.

Moreover, the Data Act aims to give data subjects control over the data they generate *en masse* through the use of products.[121] This is intended to be achieved, for example, through the switching between data processing services laid down in Chapter VI of the Data Act. These provisions are intended to complement the data portability right of the GDPR,[122] which is described in Chapter IV. 3. f). Furthermore, the Data Act states that the recent advance of products connected to the internet has increased the 'potential value of data'.[123] It aims to improve data literacy, i.e. raise awareness of the potential value of the data.[124] The Data Act thus also recognises that data has value and can be an economic asset.

The Data Act gives individuals better control over their personal data and strengthen their digital sovereignty. It is them that should be empowered to actively use their personal data as an asset.

5. Conclusion: The EU recognises (personal) data as an economic asset

The EU has not completely missed the step into the digital age. Strategies have been published to address the challenges of the digital age. While these are often policy agendas, their importance should not be underestimated. The creation of a Digital Single Market through free access to data, the necessary technological landscape and data at its core is a step in the right direction.

These strategies were followed by numerous directives and regulations. These illustrate that the EU recognises that (personal) data can be an economic asset. The Data Governance Act is significant because rights to data are explicitly mentioned. By facilitating the sharing and reuse of data, the Data Governance Act recognises data as an economic asset and tries to address its better usability and tradability. The Data Act aims to allocate the value of data fairly, thus also recognising that data has value.

The DCD, which addresses business models previously recognised as 'free', deserves special attention. As a result, contract law also applies when not only money but also personal data is given for a digital content or digital services. As a

---

[120] P. G. Picht and H. Richter, 'EU Digital Regulation 2022: Data Desiderata', 71 *GRUR International Journal of European and International IP Law* (2022), p. 400.

[121] J. Klink-Straub and T. Straub, 'Data Act als Rahmen für gemeinsame Datennutzung', 12 *ZDAktuell* (2022), p. 01076.

[122] Ibid.

[123] See Recital 1 Data Act.

[124] Recital 19 Data Act.

result, many interactions in everyday digital life now qualify as non-gratuitous contracts. Consequently, consumers now have numerous rights under the DCD and national laws implementing it.

The original proposal of the DCD also drew criticism regarding the expression 'personal data as counter-performance' The EDPS compared the concept to illegal organ trafficking and stressed that fundamental rights must not be commercialised. Moreover, the EDPS said that personal data cannot be compared to money and that such comparisons are dangerous. Legal scholars focused on consent in contracts concerning digital content or digital services. Here, the majority opinion is that personal data can be given in exchange for digital content or services if consent has been freely given and can always be withdrawn.

However, the question of whether personal data may not be commercialised as an outgrowth of the fundamental right to data protection has not yet been fully answered. This question has significance with regard to the criticism of the EDPS in the sense that in the DCD, personal data is *de facto* equated with money. Answering this question requires a more in-depth analysis. The following part of this work is therefore addressing the questions: Can a fundamental right be commercialised? Is the concept of personal data as an economic asset compatible with the Charter?

VI. Applicability of the Charter to the use of personal data as an economic asset

To address the question of whether and, if so, under which conditions the fundamental right to data protection can be commercialised, the Charter merits special consideration. The Charter has been binding since the entry into force of the Lisbon Treaty and it constitutes the EU's own bill of rights.[1] Even before that, it was a cornerstone of the EU's constitutionalisation and integration efforts in the 2000s.[2] As the main source of fundamental rights protection in the EU, the Charter creates legal certainty and strengthens the protection of fundamental rights.[3]

Before this work turns to the question of whether and, if so, under which conditions the concept of personal data as an economic asset is compatible with the Charter, it is necessary to clarify whether the Charter is applicable at all. After all, the constellations described in the preceding chapters concern legal relationships and interactions between private parties. Moreover, the extent of the Charter's field of application is not immediately apparent from its wording.[4] To establish this fundamental premise, Section 1 will examine the EU as an addressee of the Charter. Section 2 will then turn to the Member States as ad-

---

[1] H. D. Jarass, 'Einleitung: Grundlagen und Bedeutung der Grundrechte' in H. D. Jarass (ed.), *Charta der Grundrechte der Europäischen Union* (4th edition, C.H. Beck, 2021), para. 5; R. Schütze, 'Three "Bills of Rights" for the European Union', 30 *Yearbook of European Law* (2011), p. 132.

[2] D. Sarmiento, 'Who's afraid of the Charter? The Court of Justice, national courts and the new framework of fundamental rights protection in Europe', 55 *Common Market Law Review* (2013), p. 1268; K. Lenaerts, 'Exploring the Limits of the EU Charter of Fundamental Rights', 8 *European Constitutional Law Review* (2012), p. 375; P. Eeckhout, 'The EU Charter of Fundamental Rights and the Federal Question', 39 *Common Market Law Review* (2002), p. 945.

[3] E. Hancox, 'The Relationship Between the Charter and General Principles: Looking back and Looking Forward', 22 *Cambridge Yearbook of European Legal Studies* (2020), p. 244; E. Frantziou, 'The Binding Charter Ten Years on: More than a "Mere Entrety"?', 38 *Yearbook of European Law* (2019), p. 89; S. I. Sánchez, 'The Court and the Charter: The impact of the entry into force of the Lisbon Treaty on the ECJ's approach to fundamental rights', 49 *Common Market Law Review* (2012), p. 1588.

[4] A. Poulou, 'Financial assistance conditionality and human rights protection: What is the role of the EU Charter of Fundamental Rights?', 54 *Common Market Law Review* (2017), p. 992.

dressees of the Charter. Section 3 will analyse the horizontal effect of the Charter. It will be shown when the Charter can be applied in the context of personal data as an economic asset.

1. The EU as an addressee of the Charter

Although this work focuses on the economic use of personal data by private companies, this does not mean that the public sector does not also use, share and value personal data. Therefore, the following paragraphs will analyse whether the Charter can apply when institutions and bodies of the EU use and share personal data or even derive economic value from it.

Article 51 (1) of the Charter establishes that the

> 'provisions of this Charter are addressed to the institutions, bodies, offices and agencies of the Union […] and to the Member States only when they are implementing Union law'.

Article 51 (1) of the Charter determines the addressees of the Charter obligations, i.e. those who have certain obligations arising from the fundamental rights of the Charter.[5] In this regard, the term 'addressee triad' is used.[6]

The Explanatory Memorandum to the Charter, which is to be taken into account in its interpretation,[7] indicates that institutions and bodies of the EU are primarily covered by the Charter's obligations, while always respecting the principle of subsidiarity.[8] According to Article 13 TEU, the EU institutions include the European Parliament, the European Council, the Council, the European Commission, the Court of Justice of the European Union, the European Central Bank and the Court of Auditors. 'Bodies, offices and agencies' are authorities established by the Treaties or secondary legislation.[9] Thus, the Charter also applies to the EDPB, for example.

The need for the EU to be bound by fundamental rights is reasonable, since the EU exercises sovereignty over individuals.[10] All areas of activity of the EU are

---

[5] D. Sarmiento, 'Who's afraid of the Charter? The Court of Justice, national courts and the new framework of fundamental rights protection in Europe' (*supra* Chapter VI. note 2), p. 1273; H. D. Jarass, 'EU-Grundrechte-Charta Art. 51 Anwendungsbereich' in H. D. Jarass (ed.), *Charta der Grundrechte der Europäischen Union*, para. 3; M. Holoubek and M. Oswald 'Art 51 GRC. Anwendungsbereich' in M. Holoubek and G. Lienbacher (eds.), *GRC-Kommentar* (2nd edition, Manz, 2019), para. 8; A. Schwerdtfeger, 'Artikel 51 Anwendungsbereich' in J. Meyer and S. Hölscheidt (eds.), *Charta der Grundrechte der Europäischen Union*, para. 1.

[6] K. Stern and A. Hamacher, 'Einführung und Grundlagen' in K. Stern and M. Sachs (eds.), *GRCh – Europäische Grundrechte-Charta* (C.H. Beck, 2016), para. 79.

[7] See Article 52 (7) Charter.

[8] Explanations relating to the Charter of Fundamental Rights [2007] OJ C303/32.

[9] Explanations relating to the Charter of Fundamental Rights [2007] OJ C303/32; C. Ladenburger and J. Vondung, 'Art. 51. Anwendungsbereich' in K. Stern and M. Sachs (eds.), *GRCh – Europäische Grundrechte-Charta* (C.H. Beck, 2016), para. 6.

[10] T. Kingreen, 'Art. 51 GRCh' in C. Calliess and M. Ruffert (eds.), *EUV/AEUV* (6th

covered by the scope of the Charter, as all activities of the EU are within the fundamental rights sphere.[11] This is intended to prevent the EU from evading its obligation to the Charter by choosing and changing the legal form of activity.[12] The CJEU held that the Charter applies to the EU institutions even when they act outside the legal framework of the EU.[13] This is in line with the purpose and genesis of Article 51 (1) of the Charter.[14]

Since the public sector does also use, share and value personal data, it is unsurprising that the EU has adopted and proposed legal and political instruments to facilitate the (economic) use of personal data by public institutions.[15] The ODD[16] establishes a framework to improve the availability of public sector data. It is a legal instrument in response to the phenomenon of data as an economic asset. It is stated in the Directive itself that certain documents (and thus data) are a valuable resource for society.[17] Its scope includes documents from public bodies,[18] public companies[19] and publicly funded research data[20]. A key point is that high-value datasets are to be accessed free of charge throughout Europe.[21] High-quality datasets include those that bring socio-economic benefits.[22] This free access to datasets is designed to benefit the data economy.[23] Start-ups are also to be fostered through this.[24] It is also noteworthy that data are named as assets of a valuable ecosystem.[25]

Furthermore, the Data Governance Act is intended to complement the ODD. As described above, the Data Governance Act aims to regulate the sharing and

---

edition, C.H.Beck, 2022), para. 4; A. Schwerdtfeger, 'Artikel 51 Anwendungsbereich' (*supra* Chapter VI. note 5), para. 28.

[11] H. D. Jarass, 'EU-Grundrechte-Charta Art. 51 Anwendungsbereich' (*supra* Chapter VI. note 5), para. 16; M. Holoubek and M. Oswald 'Art 51 GRC. Anwendungsbereich' (*supra* Chapter VI. note 5), para. 12; C. Ladenburger and J. Vondung, 'Art. 51. Anwendungsbereich' (*supra* Chapter VI. note 9), para. 7; A. Schwerdtfeger, 'Artikel 51 Anwendungsbereich' (*supra* Chapter VI. note 5), para. 31.

[12] K. Stern and A. Hamacher, 'Einführung und Grundlagen' (*supra* Chapter VI. note 6), para. 82.

[13] Case C-8/15 P *Ledra Advertising v Commission and ECB*, EU:C:2016:701, para. 67.

[14] A. Schwerdtfeger, 'Artikel 51 Anwendungsbereich' (*supra* Chapter VI. note 5), para. 29.

[15] See recently the European Health Data Space: European Commission, *European Health Union: A European Health Data Space for people and science*, 3 May 2022, https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2711 (accessed 31 January 2024).

[16] Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information, [2019] OJ L 172/56.

[17] See Recital 8 ODD.

[18] See Article 1 (1) (a) ODD.

[19] See Article 1 (1) (b) ODD.

[20] See Article 1 (1) (c) ODD.

[21] See Article 14 ODD.

[22] See Article 14 (2) (a) ODD.

[23] See Recital 4 ODD.

[24] See Recital 32 ODD.

[25] See Recital 32 ODD.

reuse of public sector data to which third party rights exist (e.g. data protection rights and intellectual property rights). These data do not fall within the scope of the ODD. The Data Governance Act is remarkable because it refers to the concept of rights to data and virtually equates the protection of personal data with the protection of certain property rights.[26]

The Charter is applicable in all these constellations. It can therefore be concluded that the Charter can be applicable to data processing by institutions and bodies of the EU. The binding nature of the Charter also has significance in police and judicial cooperation in criminal matters, in which the exploitation of data is of major importance.[27] The Charter can also be applicable if, for example, the EU arranges data processing by means of contracts under private law.[28] As the economic exploitation of personal data usually involves data processing, this applies accordingly. Consequently, if institutions and bodies of the EU use and share personal data or even derive economic value from it, the Charter can be applicable and its provisions must be respected.

2. The Member States as addressees of the Charter

Not only at EU-level, but also in Member States, data is being used and shared to drive economic growth and create jobs through improved use of (open) data.[29] Article 51 (1) of the Charter states that Member States must respect the rights enshrined in the Charter when implementing EU law. This rule does not only apply to national authorities of the Member States, but also to sub-national authorities of the Member States.[30] The Member States are covered by the Charter's field of application, irrespective of the legal nature of their action as long as they are implementing EU law, which implies that there is no difference between the EU and the Member States in this respect.[31] Therefore, when Member States exploit personal data economically, they might also have to comply with the provisions of the Charter.

As stated above, Article 51 (1) stipulates that the requirement to respect the rights enshrined in the Charter is only binding on the Member States when they are implementing Union law. Within the autonomous action of the Member

---

[26] See for example, Recital 5 Data Governance Act.

[27] T. Riesz, 'Art 8 GRC. Schutz personenbezogener Daten' in M. Holoubek and G. Lienbacher (eds.), *GRC-Kommentar*, para. 89.

[28] Ibid.

[29] See for example in Austria, Digital Austria, https://www.digitalaustria.gv.at (accessed 31 January 2024); Open Data Österreich, https://www.data.gv.at (accessed 31 January 2024).

[30] Explanations relating to the Charter of Fundamental Rights [2007] OJ C303/32; K. Stern and A. Hamacher, 'Einführung und Grundlagen' (*supra* Chapter VI. note 6), para. 91.

[31] M. Holoubek and M. Oswald 'Art 51 GRC. Anwendungsbereich'(*supra* Chapter VI. note 5), para. 15.

States, the Charter is not applicable, which is one of the most fundamental differences to the ECHR or other human rights treaties under international law.[32] The protection of Charter rights in the Member States is weighed against the autonomy of the Member States.[33] *Holoubek/Oswald* consider this provision to be the core of Article 51 of the Charter.[34] This provision therefore requires a more in-depth analysis.

'Union law' is understood to mean primary law, secondary law, decisions, recommendations, opinions, delegated acts and implementing acts, irrespective of any connection with the objectives of the rights set out in the Charter.[35] This would also include the GDPR, which is naturally relevant for personal data and its economic use. In addition, the ODD, DCD, the Data Governance Act and the Data Act are covered by this.

Due to the applicability of the Charter on Member States 'only when they are implementing Union law', a substantial limitation of the applicability of the Charter is established.[36] The numerous fundamental rights of the Charter on the one hand and the Charter's limited scope of application on the other hand were described early on as the 'Charter's paradox'.[37] Nevertheless, the Charter should not be read too restrictively, which stems in particular from a teleological interpretation.[38]

The Explanatory Memorandum to the Charter refers to previous judgments of the CJEU according to which general principles are binding on the Member States if they 'act in the scope of Union law'.[39] This reference to the previous case law of the CJEU constitutes a wider field of application of general principles than the wording of Article 51 (1) of the Charter.[40] However, as will be shown below,

---

[32] C. Ladenburger and J. Vondung, 'Art. 51. Anwendungsbereich' (*supra* Chapter VI. note 9), para. 8; T. Kingreen, 'Art. 51 GRCh' (*supra* Chapter VI. note 10), para. 15.

[33] D. Sarmiento, 'Who's afraid of the Charter? The Court of Justice, national courts and the new framework of fundamental rights protection in Europe' (*supra* Chapter VI. note 2), p. 1274.

[34] M. Holoubek and M. Oswald 'Art 51 GRC. Anwendungsbereich' (*supra* Chapter VI. note 5), para. 16.

[35] H. D. Jarass, 'EU-Grundrechte-Charta Art. 51 Anwendungsbereich' (*supra* Chapter VI. note 5), para. 20; T. Kingreen, 'Art. 51 GRCh' (*supra* Chapter VI. note 10), para. 8.

[36] H. D. Jarass, 'EU-Grundrechte-Charta Art. 51 Anwendungsbereich' (*supra* Chapter VI. note 5), para. 22.

[37] P. Eeckhout, 'The EU Charter of Fundamental Rights and the Federal Question' (*supra* Chapter VI. note 2), p. 958.

[38] S. I. Sánchez, 'The Court and the Charter: The impact of the entry into force of the Lisbon Treaty on the ECJ's approach to fundamental rights' (*supra* Chapter VI. note 3), p. 1584; R. Alonso García, 'The General Provision of the Charter of Fundamental Rights of the European Union', 8 *European Law Journal* (2002), p. 496.

[39] See Explanations relating to the Charter of Fundamental Rights [2007] OJ C303/32 that mention: Case C-5/88 *Wachauf*, EU:C:1989:321; Case C-260/89 *ERT*, EU:C:1991:254; Case C-309/96 *Annibaldi*, EU:C:1997:631.

[40] A. Torres Pérez, 'Rights and Powers in the European Union: Towards a Charter that is

the scope of application of the Charter has been aligned with that of the general principles.[41]

The CJEU had and still has an important role to play in filling the vague wording of Article 51 (1) of the Charter with content.[42] Over decades, even before the Charter entered into force, the CJEU has extended the scope of protected rights and their application.[43] In the following, the contours of Article 51 (1) of the Charter are drawn on the basis of the CJEU's case law, even though it should be noted that the CJEU has not always been convincing in its consistency and clarity regarding Article 51 (1) of the Charter.[44] This may be due to the fact that the CJEU tends to be inclined to adopt a case-by-case approach.[45]

In the *Åkerberg Fransson* case,[46] the CJEU dealt with the interpretation of Article 51 (1) of the Charter. This judgment is considered a landmark in understanding the field of application of the Charter.[47] This case dealt with the question of whether a criminal charge following a tax penalty for the same offence infringes the *ne bis in idem* principle set out in Article 50 of the Charter.[48] The decisive factor in answering this question was whether the Charter was applicable to the Member State concerned.[49]

The CJEU resolved the apparent conflict between 'implementing' and 'acting within the scope of Union law' by emphasising that Article 51 (1) of the Charter

---

Fully Applicable to the Member States?', 22 *Cambridge Yearbook of European Legal Studies* (2020), p. 281.

[41] M. Dougan, 'Judicial review of Member State action under the general principles and the Charter: Defining the "scope of Union law"', 52 *Common Market Law Review* (2015), p. 1206.

[42] A. Ward, 'Art 51 – Field of Application' in S. Peers et al. (eds.), *The EU Charter of Fundamental Rights* (2nd edition, Hart Publishing, 2021), para. 53; A. Torres Pérez, 'Rights and Powers in the European Union: Towards a Charter that is Fully Applicable to the Member States?' (*supra* Chapter VI. note 40), p. 282; M. Holoubek and M. Oswald 'Art 51 GRC. Anwendungsbereich' (*supra* Chapter VI. note 5), para. 16.

[43] E. Hancox, 'The Relationship Between the Charter and General Principles: Looking back and Looking Forward' (*supra* Chapter VI. note 3), p. 234.

[44] A. Torres Pérez, 'Rights and Powers in the European Union: Towards a Charter that is Fully Applicable to the Member States?' (*supra* Chapter VI. note 40), p. 282; H. D. Jarass, 'EU-Grundrechte-Charta Art. 51 Anwendungsbereich' (*supra* Chapter VI. note 5), para. 22.

[45] A. Poulou, 'Financial assistance conditionality and human rights protection: What is the role of the EU Charter of Fundamental Rights?' (*supra* Chapter VI. note 4), p. 1019.

[46] Case C-617/10 *Åkerberg Fransson*, EU:C:2013:105.

[47] A. Ward, 'Art 51 – Field of Application' (*supra* Chapter VI. note 42), para. 72; E. Hancox, 'The meaning of "implementing" EU law under Article 51(1) of the Charter: Åkerberg Fransson', 50 *Common Market Law Review* (2013), p. 1411; D. Sarmiento, 'Who's afraid of the Charter? The Court of Justice, national courts and the new framework of fundamental rights protection in Europe' (*supra* Chapter VI. note 2), p. 1268.

[48] Case C-617/10 *Åkerberg Fransson* (*supra* Chapter VI. note 46), para. 14.

[49] A. Schwerdtfeger, 'Artikel 51 Anwendungsbereich' (*supra* Chapter VI. note 5), para. 44.

'confirms the Court's case-law relating to the extent to which actions of the Member States must comply with the requirements flowing from the fundamental rights guaranteed in the legal order of the European Union'.[50]

The CJEU thus upheld its previous case law and established that the entry into force of the Charter did not change the applicability of EU fundamental rights.[51] This prevents contradictions within a uniform system of fundamental rights.[52] Moreover, the CJEU stated:

'Since the fundamental rights guaranteed by the Charter must therefore be complied with where national legislation falls within the scope of European Union law, situations cannot exist which are covered in that way by European Union law without those fundamental rights being applicable.'[53]

The CJEU further argued that the 'applicability of European Union law entails applicability of the fundamental rights guaranteed by the Charter'.[54] Thus, the scope of the Charter was aligned and is overlapping with that of the general principles.[55] The essential requirement is therefore a connection with Union law that puts the case within the field of application of Union law and consequently of the Charter.[56] This connection was emphasised by the CJEU even before the Charter entered into force.[57] Clearly, the CJEU has interpreted 'implementing' broadly in its case law.[58]

More specifically, the Charter is applicable when Member States apply primary Union law and when Regulations and Directives, thus secondary Union

[50] Case C-617/10 *Åkerberg Fransson* (*supra* Chapter VI. note 46), para. 18.

[51] D. Sarmiento, 'Who's afraid of the Charter? The Court of Justice, national courts and the new framework of fundamental rights protection in Europe' (*supra* Chapter VI. note 2), p. 1277; S. I. Sánchez, 'The Court and the Charter: The impact of the entry into force of the Lisbon Treaty on the ECJ's approach to fundamental rights' (*supra* Chapter VI. note 3), p. 1587.

[52] A. Schwerdtfeger, 'Artikel 51 Anwendungsbereich' (*supra* Chapter VI. note 5), para. 42.

[53] Case C-617/10 *Åkerberg Fransson* (*supra* Chapter VI. note 46), para. 21.

[54] Ibid.

[55] E. Hancox, 'The Relationship Between the Charter and General Principles: Looking back and Looking Forward' (*supra* Chapter VI. note 3), p. 238; K. Lenaerts, 'Exploring the Limits of the EU Charter of Fundamental Rights' (*supra* Chapter VI. note 2), p. 385; M. Dougan, 'Judicial review of Member State action under the general principles and the Charter: Defining the "scope of Union law"' (*supra* Chapter VI. note 41), p. 1206.

[56] Case C-457/09 *Chartry*, EU:C:2011:101, para. 25; Case C-206/13 *Siragusa*, EU:C:2014: 126, para. 24; H. D. Jarass, 'EU-Grundrechte-Charta Art. 51 Anwendungsbereich' (*supra* Chapter VI. note 5), para. 23; M. Holoubek and M. Oswald 'Art 51 GRC. Anwendungsbereich' (*supra* Chapter VI. note 5), para. 17.

[57] See Case C-299/95 *Kremzow*, EU:C:1997:254, para. 16.

[58] A. Torres Pérez, 'Rights and Powers in the European Union: Towards a Charter that is Fully Applicable to the Member States?' (*supra* Chapter VI. note 40), p. 281; D. Sarmiento, 'Who's afraid of the Charter? The Court of Justice, national courts and the new framework of fundamental rights protection in Europe' (*supra* Chapter VI. note 2), p. 1278.

law, are enforced and implemented.[59] The Member States act to a certain extent on behalf and in the interest of the EU.[60] This constellation is referred to as an agency situation, i.e. that Member States act as agents of the EU and thus are a 'helping hand'.[61] In principle, therefore, the GDPR, which is particularly relevant to the issue of this work, would enable the Charter to be applied. The implementation of directives such as the DCD or ODD would also make the Charter applicable. This therefore also concerns national implementation of the DCD rules on the provision of digital services in exchange for personal data.

In addition, the Charter is binding on Member States in cases where they fulfil obligations, in connection with Regulations and Directives, under EU law.[62] Consequently, the Charter is not applicable if the EU law concerned does not impose obligations on the Member States.[63] Such obligations must also be fulfilled by Member States in the case of data processing in third countries and thus renders the Charter applicable.[64] The field of application of the Charter must hence be distinguished from the field of competence of the EU.[65]

The CJEU stated that 'implementing Union law' 'requires a certain degree of connection above and beyond the matters covered being closely related or one of those matters having an indirect impact on the other'.[66] As criteria for determin-

---

[59] Case C-411/10 *N.S. and Others*, EU:C:2011:865, para. 69; Case C-682/15 *Berlioz Investment Fund*, EU:C:2017:373, para. 42; A. Torres Pérez, 'Rights and Powers in the European Union: Towards a Charter that is Fully Applicable to the Member States?' (*supra* Chapter VI. note 40), p. 282; M. Holoubek and M. Oswald 'Art 51 GRC. Anwendungsbereich' (*supra* Chapter VI. note 5), paras. 20, 24; see also before the Charter's draft: Case C-5/88 *Wachauf* (*supra* Chapter VI. note 39), para. 19.

[60] C. Ladenburger and J. Vondung, 'Art. 51. Anwendungsbereich' (*supra* Chapter VI. note 9), para. 34.

[61] E. Hancox, 'The meaning of "implementing" EU law under Article 51(1) of the Charter: Åkerberg Fransson' (*supra* Chapter VI. note 47), p. 1418.

[62] See Case C-617/10 *Åkerberg Fransson* (*supra* Chapter VI. note 46); A. Torres Pérez, 'Rights and Powers in the European Union: Towards a Charter that is Fully Applicable to the Member States?' (*supra* Chapter VI. note 40), p. 283; K. Lenaerts, 'Exploring the Limits of the EU Charter of Fundamental Rights' (*supra* Chapter VI. note 2), p. 378; M. Holoubek and M. Oswald 'Art 51 GRC. Anwendungsbereich' (*supra* Chapter VI. note 5), para. 22; C. Ladenburger and J. Vondung, 'Art. 51. Anwendungsbereich' (*supra* Chapter VI. note 9), para. 46.

[63] Case C-206/13 *Siragusa* (*supra* Chapter VI. note 56), para. 26; Case C-198/13 *Julian Hernández and Others*, EU:C:2014:2055, para. 35; Case C-234/16 *Miravitlles Ciurana and Others*, EU:C:2017:969, para. 34; Case C-152/17 *Consorzio Italian Management e Catania Multiservizi*, EU:C:2018:264, para. 34; Case C-609/17 *TSN*, EU:C:2019:981, para. 53.

[64] Case C-362/14 *Schrems*, EU:C:2015:650, para. 78; H. D. Jarass, 'EU-Grundrechte-Charta Art. 8 Schutz personenbezogener Daten' in H. D. Jarass (ed.), *Charta der Grundrechte der Europäischen Union*, para. 3.

[65] Case C-198/13 *Julian Hernández and Others* (*supra* Chapter VI. note 63), para. 36; H. D. Jarass, 'EU-Grundrechte-Charta Art. 51 Anwendungsbereich' (*supra* Chapter VI. note 5), para. 24; C. Ladenburger and J. Vondung, 'Art. 51. Anwendungsbereich' (*supra* Chapter VI. note 9), para. 37.

[66] Case C-206/13 *Siragusa* (*supra* Chapter VI. note 56), para. 24.

ing whether the connection with Union law is sufficient, the CJEU emphasised that it must be examined

'whether that national legislation is intended to implement a provision of EU law; the nature of the legislation at issue and whether it pursues objectives other than those covered by EU law, even if it is capable of indirectly affecting EU law; and also whether there are specific rules of EU law on the matter or rules which are capable of affecting it.'[67]

The criteria are construed broadly and generally.[68] The CJEU sets standards for its own competence to interpret the rights of the Charter and gives itself a wide margin of discretion.[69] Based on this margin, it is not clear when a connection to Union law is sufficient.[70]

The CJEU would benefit from taking a consistent approach in order to create the consistency criticised above and to establish a comprehensible and precise framework for the protection of fundamental rights.[71] In particular, the detailed explanation as to why a case was decided as it was would provide legal certainty.[72] This range of scenarios blurs the limits of the Charter's field of application.[73] However, when it comes to the economic use of personal data by Member States, these blurred limits are less relevant. Particularly as in these cases, the GDPR, the DCD and the ODD are applicable, which are secondary law instruments of the EU.

3. Horizontal effect of the Charter

It is precisely private companies that use and trade personal data and thus value them as an economic asset. Moreover, private individuals also use their personal data as an asset in order to receive digital content and services from private companies in return. Especially in the field of data, companies gain power

---

[67] Case C-40/11 *Iida*, EU:C:2012:691, para. 79; Case C-87/12 *Ymeraga and Others*, EU:C:2013:291, para. 41; Case C-206/13 *Siragusa* (*supra* Chapter VI. note 56), para. 25; Case C-198/13 *Julian Hernández and Others* (*supra* Chapter VI. note 63), para. 37.

[68] A. Torres Pérez, 'Rights and Powers in the European Union: Towards a Charter that is Fully Applicable to the Member States?' (*supra* Chapter VI. note 40), p. 285; M. Holoubek and M. Oswald 'Art 51 GRC. Anwendungsbereich' (*supra* Chapter VI. note 5), para. 31.

[69] Ibid; A. Schwerdtfeger, 'Artikel 51 Anwendungsbereich' (*supra* Chapter VI. note 5), para. 52.

[70] E. Hancox, 'The meaning of "implementing" EU law under Article 51(1) of the Charter: Åkerberg Fransson' (*supra* Chapter VI. note 47), p. 1426.

[71] A. Torres Pérez, 'Rights and Powers in the European Union: Towards a Charter that is Fully Applicable to the Member States?' (*supra* Chapter VI. note 40), p. 285; see also, P. Eeckhout, 'The EU Charter of Fundamental Rights and the Federal Question' (*supra* Chapter VI. note 2), p. 993.

[72] E. Hancox, 'The meaning of "implementing" EU law under Article 51(1) of the Charter: Åkerberg Fransson' (*supra* Chapter VI. note 47), p. 1422.

[73] Ibid, p. 1431.

through personal data and affect the fundamental right to data protection as much or even more than states.[74] The question therefore arises whether these companies, due to their position of power, could also be bound by the Charter.

Can the Charter also be applied to the economic use of personal data between private parties? As outlined above, the obligations of the Charter are addressed to the Union and the Member States. This follows from the wording of Article 51 (1) of the Charter. The wording is kept very vague and leaves room for interpretation.[75] On the basis of the wording, the Charter does not seem to impose obligations on private individuals and companies.[76]

However, there are rights enshrined in the Charter that are designed to address conflicts between private individuals.[77] This applies for example, to the provisions on consent for medical treatment in Article 3 of the Charter, the prohibition of slavery and forced labour in Article 5 of the Charter, workers' right to information and consultation within the undertaking in Article 27 of the Charter, the protection in the event of unjustified dismissal in Article 30 of the Charter and fair and just working conditions set out in Article 31 of the Charter, which only make sense if they also and especially address private individuals.[78] The same could be argued for the right to data protection under Article 8 of the Charter. For these reasons, it will be examined below whether and how the Charter can have an effect among private parties, and thus whether the rights enshrined therein must also be respected when commercialising personal data.

a) Three levels of horizontality

The effect of fundamental rights among private individuals is referred to as the horizontal effect. There are three levels of horizontality that complement each other.[79] The first level of horizontality is the obligation on private parties by

---

[74] T. Riesz, 'Art 8 GRC. Schutz personenbezogener Daten' (*supra* Chapter VI. note 27), para. 88.

[75] E. Frantziou, 'The Horizontal Effect of the Charter of Fundamental Rights of the EU: Rediscovering the Reasons for Horizontality', 21 *European Law Journal* (2015), p. 661; M. Holoubek and M. Oswald 'Art 51 GRC. Anwendungsbereich' (*supra* Chapter VI. note 5), para. 59.

[76] E. Frantziou, 'The Horizontal Effect of the Charter of Fundamental Rights of the EU: Rediscovering the Reasons for Horizontality' (*supra* Chapter VI. note 75), p. 661; H.D. Jarass, 'Die Bedeutung der Unionsgrundrechte unter Privaten', 25 *ZEuP – Zeitschrift für Europäisches Privatrecht* (2017), p. 315.

[77] H.D. Jarass, 'Die Bedeutung der Unionsgrundrechte unter Privaten' (*supra* Chapter VI. note 76), p. 315.

[78] Ibid.

[79] E. Frantziou, 'The Horizontal Effect of the Charter of Fundamental Rights of the EU: Rediscovering the Reasons for Horizontality' (*supra* Chapter VI. note 75), p. 662; R. Krause, 'Horizontal Effect of the EU Charter of Fundamental Rights: Bauer and Willmeroth, MPG', 58 *Common Market Law Review* (2021), p. 1187.

means of obligations imposed on the state: positive obligations.[80] These positive obligations are invoked against the state for failing, for example, to pass laws that protect fundamental rights, thus affecting horizontal relationships.[81]

The second level of horizontality is indirect horizontal effect.[82] Here, a law applicable to private parties is interpreted by a court in a way that is in conformity with fundamental rights.[83] The CJEU often interprets secondary law between private parties in the light of the Charter.[84] EU law provisions and provisions of the Member States, insofar as they implement Union law, are interpreted in accordance with the Charter.[85] Moreover, provisions governing legal relations between private parties must respect fundamental rights.[86] Consequently, Union law is invalid and Member State provisions are not applicable if they are in breach of the Charter.[87] As a result, the rights and freedoms enshrined in the Charter have an indirect influence on national private law.[88] The CJEU has differentiated on the question of whether interpretation of national implementation laws in light of fundamental rights leads to an indirect horizontal effect between private parties.[89] *Frantziou* points out that through the case law of the CJEU on Article 16 of the Charter, an indirect horizontal effect can be assumed from it.[90]

---

[80] E. Frantziou, 'The Horizontal Effect of the Charter of Fundamental Rights of the EU: Rediscovering the Reasons for Horizontality' (*supra* Chapter VI. note 75), p. 662.

[81] Ibid.

[82] H. D. Jarass, 'EU-Grundrechte-Charta Art. 51 Anwendungsbereich' (*supra* Chapter VI. note 5), para. 36

[83] E. Frantziou, 'The Horizontal Effect of the Charter of Fundamental Rights of the EU: Rediscovering the Reasons for Horizontality' (*supra* Chapter VI. note 75), p. 662; R. Krause, 'Horizontal Effect of the EU Charter of Fundamental Rights: *Bauer and Willmeroth, MPG*' (*supra* Chapter VI. note 79), p. 1187.

[84] Opinion of Advocate General Cruz Villalón in Case C-176/12 *Association de médiation sociale*, EU:C:2013:491, para. 38.

[85] A. Schwerdtfeger, 'Artikel 51 Anwendungsbereich' (*supra* Chapter VI. note 5), para. 58; R. Krause, 'Horizontal Effect of the EU Charter of Fundamental Rights: Bauer and Willmeroth, MPG', (*supra* Chapter VI. note 79), p. 1188; Case C-360/10 *SABAM*, EU:C:2012:85, para. 52; Case C-426/11 *Alemo-Herron*, EU:C:2013:521, para. 30; Case C-131/12 *Google Spain and Google* (*supra* Chapter IV. note 283), para. 73; Case C-580/13 *Coty Germany*, EU:C:2015:485, para. 34.

[86] H. D. Jarass, 'EU-Grundrechte-Charta Art. 51 Anwendungsbereich' (*supra* Chapter VI. note 5), para. 40.

[87] Case C-236/09 *Test-Achats*, EU:C:2011:100, paras. 32 and 33; Case C-555/07 *Kücükdeveci*, EU:C:2010:21, para. 51; Case C-414/16 *Egenberger*, EU:C:2018:257, para. 79; Case C-569/16 *Bauer*, EU:C:2018:871, para. 86.

[88] R. Krause, 'Horizontal Effect of the EU Charter of Fundamental Rights: Bauer and Willmeroth, MPG', (*supra* Chapter VI. note 79), p. 1188.

[89] M. Holoubek and M. Oswald 'Art 51 GRC. Anwendungsbereich' (*supra* Chapter VI. note 5), para. 58.

[90] E. Frantziou, 'The Horizontal Effect of the Charter: Towards an Understanding of Horizontality as a Strucutral Constitutional Principle', *22* Cambridge Yearbook of European

In addition, the third level of horizontality is the direct effect of fundamental rights between private parties, i.e. the direct horizontal effect.[91] Charter rights have direct horizontal effect when they have negative rights enshrined therein, as this is necessary for an effective protection of fundamental rights.[92] The same applies to the rights under Title III of the Charter ('Equality').[93] Social rights and principles in particular have a direct horizontal effect.[94]

Analogous to *Frantziou's* argumentation,[95] the following claims could therefore be possible when invoking the fundamental right to data protection in the context of economic use of personal data: (i) against the Member State, demanding compensation for its failure to ensure compliance with the right to data protection by private parties, e.g. failure to stop unlawful economic exploitation of personal data by establishing thorough checks and balances (positive obligations), (ii) in court, requiring it to interpret certain legal provision, e.g. of the GDPR, in accordance with the fundamental right to data protection (indirect horizontal effect) and (iii) against the data controller who unlawfully exploits personal data (direct horizontal effect).

It should be noted, though, that the CJEU avoids the terms indirect and direct horizontal effect.[96] The CJEU has refrained from applying these three levels of horizontality in a differentiated manner.[97] In particular, the application of the indirect horizontal effect and positive obligations as a stopgap and last resort, did not allow for a nuanced jurisprudence on horizontality in the pre-Lisbon era.[98] Moreover, the question of the horizontal effect of the Charter does not arise when addressees of the rights enshrined therein, e.g. the EU and Member States, operate in a private law form, as the Charter is applicable to them anyway, as described above.[99] The following sections provide an overview of the relevant case law of the CJEU.

Legal Studies (2020), p. 221; see Case C-426/11 *Alemo-Herron* (*supra* Chapter VI. note 85), para. 31

[91] H. D. Jarass, 'EU-Grundrechte-Charta Art. 51 Anwendungsbereich' (*supra* Chapter VI. note 5), para. 36

[92] C. Ladenburger and J. Vondung, 'Art. 51. Anwendungsbereich' (*supra* Chapter VI. note 9), para. 13.

[93] Ibid.

[94] Ibid, para. 16.

[95] See E. Frantziou, 'The Horizontal Effect of the Charter of Fundamental Rights of the EU: Rediscovering the Reasons for Horizontality' (*supra* Chapter VI. note 75), p. 662.

[96] H. D. Jarass, 'EU-Grundrechte-Charta Art. 51 Anwendungsbereich' (*supra* Chapter VI. note 5), para. 36; R. Krause, 'Horizontal Effect of the EU Charter of Fundamental Rights: Bauer and Willmeroth, MPG', (*supra* Chapter VI. note 79), p. 1189; T. Kingreen, 'Art. 51 GRCh' (*supra* Chapter VI. note 10), para. 26.

[97] E. Frantziou, 'The Horizontal Effect of the Charter of Fundamental Rights of the EU: Rediscovering the Reasons for Horizontality' (*supra* Chapter VI. note 75), p. 662.

[98] Ibid, p. 665.

[99] H. D. Jarass, 'EU-Grundrechte-Charta Art. 51 Anwendungsbereich' (*supra* Chapter VI. note 5), para. 37.

b) Pre-Lisbon horizontality

If one were to consider merely the wording of Article 51 (1) of the Charter, a horizontal effect would have to be ruled out.[100] In the opinion of *AG Trstenjak*, this provision indicates a deliberate restriction of the parties to whom the fundamental rights are addressed.[101] She concludes that private individuals are therefore not directly bound by the Charter.[102] However, the question of the Charter's horizontal effect was not discussed during the drafting process in the European Convention, which is why Article 51 (1) of the Charter does not exemplify the intention to exclude the horizontal effect.[103] In contrast, some of the provisions of the Charter could be interpreted as having an intended horizontal effect.[104] Furthermore, the preamble, which stipulates that the 'enjoyment of these rights entails responsibilities and duties with regard to other persons, to the human community and to future generations', can also be read as an indication of a horizontal effect of the Charter.[105]

Moreover, the CJEU has already rejected a narrow textual interpretation regarding the horizontal effect of the Treaties.[106] In *Defrenne*,[107] the CJEU ruled that

> 'the fact that certain provisions of the Treaty are formally addressed to the Member States does not prevent rights from being conferred at the same time on any individual […]'.[108]

This notion was reiterated by the CJEU in *Viking*.[109] Furthermore, the CJEU stated in *Mangold* that the principle of non-discrimination on grounds of age is to be regarded as a general principle of Union law and thus national rules must be brought into conformity with it.[110] In order to disapply a conflicting national provision, the principle of non-discrimination on grounds of age can be invoked

---

[100] M. Holoubek and M. Oswald 'Art 51 GRC. Anwendungsbereich' (*supra* Chapter VI. note 5), para. 59.

[101] Opinion of Advocate General Trstenjak in Case C-282/10 *Dominguez*, EU:C:2011:449, para. 80.

[102] Ibid, para. 83.

[103] C. Ladenburger and J. Vondung, 'Art. 51. Anwendungsbereich' (*supra* Chapter VI. note 9), para. 14.

[104] Ibid, Ladenburger and Vondung refer to Articles 3(2), 5(3), 24(1), 24(2), Art 32(1) of the Charter; A. Schwerdtfeger, 'Artikel 51 Anwendungsbereich' (*supra* Chapter VI. note 5), para. 57; E. Frantziou, 'The Horizontal Effect of the Charter of Fundamental Rights of the EU: Rediscovering the Reasons for Horizontality' (*supra* Chapter VI. note 75), p. 660.

[105] A. Weber, 'Präambel' in K. Stern and M. Sachs (eds.), *GRCh – Europäische Grundrechte-Charta*, para. 41.

[106] E. Frantziou, 'The Horizontal Effect of the Charter of Fundamental Rights of the EU: Rediscovering the Reasons for Horizontality' (*supra* Chapter VI. note 75), p. 659.

[107] Case C-43/75 *Defrenne / SABENA*, EU:C:1976:56.

[108] Ibid, para. 31.

[109] Case C-438/05 *Viking*, EU:C:2007:772, para. 58.

[110] Case C-144/04 *Mangold*, EU:C:2005:709, para. 75.

in horizontal disputes.[111] The Court has thereby closed a constitutional loophole.[112]

Considering that the Charter has the same value as the Treaties, this case law can also be used as a standard of interpretation for the Charter. This is partly because the Charter reproduces some rights that were already granted horizontal effect before the Charter entered into force.[113] In this sense, Advocate General *Cruz Villalón* has also stated that

> 'since the horizontal effect of fundamental rights is not unknown to EU law, it would be paradoxical if the incorporation of the Charter into primary law actually changed that state of affairs for the worse'.[114]

c) First post-Lisbon cases

This notion has been reiterated in *Kükükdeveci*. In this case, the CJEU stated that the secondary law in question 'gives specific expression to that principle [i.e. principle of non-discrimination on grounds of age]' and therefore precludes contradictory national legislation.[115] Secondary law, which 'gives specific expression' to a fundamental right or general principle, thus has an impact on horizontal disputes between individuals.[116] Article 21 of the Charter concerning non-discrimination therefore has a horizontal effect.[117] This judgment ties in with the pre-Lisbon case law on the horizontal effect of the prohibition of discrimination as a general principle of EU law.[118]

AMS[119] concerned Article 27 of the Charter, which states that 'workers or their representatives must, at the appropriate levels, be guaranteed information and consultation in good time in the cases and under the conditions provided for by Union law and national laws and practices'.[120] France, in implementing a directive, had excluded certain workers from this right and thus the French court

---

[111] N. Lazzerini, '(Some of) the fundamental rights granted by the Charter may be a source of obligations for private parties: AMS', 51 *Common Market Law Review* (2014), p. 910.

[112] E. Muir, 'The Horizontal Effects of Charter Rights Given Expression to in EU Legislation, from Mangold to Bauer', 12 *Review of European Administrative Law* (2019), p. 188.

[113] E. Frantziou, 'The Horizontal Effect of the Charter: Towards an Understanding of Horizontality as a Strucutral Constitutional Principle' (*supra* Chapter VI. note 90), p. 211.

[114] Opinion of Advocate General Cruz Villalón in Case C-176/12 *Association de médiation sociale* (*supra* Chapter VI. note 84), para. 35.

[115] Case C-555/07 *Kücükdeveci* (*supra* Chapter VI. note 87), para. 21.

[116] E. Muir, 'The fundamental rights implications of EU legislation: Some constitutional challenges', 51 *Common Market Law Review* (2014), p. 230.

[117] M. Holoubek and M. Oswald 'Art 51 GRC. Anwendungsbereich' (*supra* Chapter VI. note 5), para. 58.

[118] E. Muir, 'The Horizontal Effects of Charter Rights Given Expression to in EU Legislation, from Mangold to Bauer' (*supra* Chapter VI. note 112), p. 188.

[119] Case C-176/12 *Association de médiation sociale*, EU:C:2014:2.

[120] See Article 27 Charter.

turned to the CJEU regarding the horizontal effect of Article 27 of the Charter expressed in that directive.[121] The CJEU has held that Article 27 of the Charter, in order to be fully effective, requires 'more specific expression in European Union or national law'.[122] The CJEU emphasised the non-horizontality of directives and stressed that the indirect effect was inapplicable in the case as it would lead to a *contra legem* interpretation of national law.[123] Therefore Article 27 of the Charter does not confer a right on individuals to rely on in a horizontal dispute. The judgment helped to clarify that some rights enshrined in the Charter have horizontal effect.[124] Furthermore, it answered the question that only provisions of the Charter, which are sufficient in itself, can be invoked in horizontal disputes.[125] However, this judgment is not satisfactory, as there were similarities to the *Kükükdeveci* case and these similarities seem to have been disregarded, leading to a different result and hence legal uncertainty.[126]

d) Egenberger, IR and Bauer

In this context, the CJEU judgments *Egenberger*[127], *IR*[128] and *Bauer*[129] merit mention as they can be regarded as the current position on horizontality of fundamental rights in the EU.[130] Since then, the CJEU has taken a consistent stance.[131] The issue in *Egenberger* was the application of a woman for a position in an ecclesiastical institution, which was rejected, with reference to the church's right to self-determination, according to which a difference of treatment on the grounds of religion was justified.[132] Ms *Egenberger* was without a denomination at the time and took legal action against this rejection to the point where the case was decided by the CJEU. The Court held that

---

[121] Case C-176/12 *Association de médiation sociale* (*supra* Chapter VI. note 119), paras. 13–22.

[122] Ibid, para. 45.

[123] Ibid, para. 39.

[124] N. Lazzerini, '(Some of) the fundamental rights granted by the Charter may be a source of obligations for private parties: AMS' (*supra* Chapter VI. note 111), p. 921.

[125] Ibid, 925.

[126] E. Frantziou, 'The Horizontal Effect of the Charter of Fundamental Rights of the EU: Rediscovering the Reasons for Horizontality' (*supra* Chapter VI. note 75), p. 668.

[127] Case C-414/16 *Egenberger* (*supra* Chapter VI. note 87).

[128] Case C-68/17 *IR*, EU:C:2018:696.

[129] Case C-569/16 *Bauer* (*supra* Chapter VI. note 87).

[130] E. Frantziou, '(Most of) the Charter of Fundamental Rights is Horizontally Applicable', 15 *European Constitutional Law Review* (2019), p. 308.

[131] E. Frantziou, 'The Horizontal Effect of the Charter: Towards an Understanding of Horizontality as a Structural Constitutional Principle' (*supra* Chapter VI. note 90), p. 217.

[132] Case C-414/16 *Egenberger* (*supra* Chapter VI. note 87), para. 28.

'the prohibition of all discrimination on grounds of religion or belief is mandatory as a general principle of EU law. That prohibition, which is laid down in Article 21 (1) of the Charter, is sufficient in itself to confer on individuals a right which they may rely on as such in disputes between them in a field covered by EU law.'[133]

Referring to its *Defrenne* ruling, the CJEU also emphasised that the mandatory effect of Article 21 of the Charter is no different from that of the Treaties, which also prohibit discrimination on various grounds between private parties.[134]

Furthermore, the Court considered that Article 47 of the Charter is sufficient in itself and can be relied upon by individuals.[135] It has been repeatedly confirmed by the Court that Article 47 of the Charter confers a right on individuals and does not need to be specified by EU or national law.[136]

In the similar case of *IR*, a doctor was dismissed from a ecclesiastical company because his second marriage infringed canon law.[137] With reference to *Egenberger*, the CJEU confirmed that Article 21 of the Charter itself confers a right on individuals which they can invoke in legal disputes between them.[138] This position has also been affirmed in more recent case law.[139]

When the CJEU considered the *Bauer* case, the interpretation of Article 31 (2) of the Charter was ambiguous with regard to its possible horizontal effect.[140] In *Bauer*, the employers of Mrs. *Bauer's* and Mrs. *Broßonn's* late husbands refused to pay the widows an allowance in lieu of annual leave not taken by their husbands before their death.[141] The provision of the Charter in question was Article 31 (2) thereof, which states that 'every worker has the right to […] an annual period of paid leave'. Regarding the horizontality of the Charter the CJEU highlighted that

'[…] although Article 51 (1) of the Charter states that the provisions thereof are addressed to the institutions, bodies, offices and agencies of the European Union with due regard for the principle of subsidiarity and to the Member States only when they are implementing EU law, Article 51 (1) does not, however, address the question whether those individuals

---

[133] Ibid, para. 76.

[134] Ibid, para. 77; see also Case C-684/16 *Max-Planck-Gesellschaft*, EU:C:2018:874, para. 77.

[135] Case C-414/16 *Egenberger* (*supra* Chapter VI. note 87), para. 78.

[136] See Case C-556/17 *Torubarov*, EU:C:2019:626, para. 56; Case C-585/18 *A.K.*, EU:C:2019:982, para. 162; Case C-245/19 *État luxembourgeois*, EU:C:2020:795, para. 54; Case C-924/19 PPU *FMS and Others*, EU:C:2020:367, para. 140; Case C-233/19 *CPAS de Liège*, EU:C:2020:757, para. 55; Case C-30/19 *Braathens Regional Aviation*, EU:C:2021:269, para. 57.

[137] Case C-68/17 *IR* (*supra* Chapter VI. note 128), para. 27.

[138] Ibid, para. 69.

[139] See Case C-193/17 *Cresco Investigation*, EU:C:2019:43, para. 76; Case C-243/19 *Veselības ministrija*, EU:C:2020:872, para. 36

[140] D. Leczykiewicz, 'The Judgment in *Bauer* and the Effect of the EU Charter of Fundamental Rights in Horizontal Situations', 16 *European Review of Contract Law* (2020), p. 326.

[141] Case C-569/16 *Bauer* (*supra* Chapter VI. note 87), paras. 10 and 11.

may, where appropriate, be directly required to comply with certain provisions of the Charter and cannot, accordingly, be interpreted as meaning that it would systematically preclude such a possibility.'[142]

The CJEU confirmed its position from *Egenberger*, underlining that Article 31 (2) of the Charter imposed a corresponding obligation to Article 21 of the Charter, allowing private individuals to refer to it in disputes between them.[143] It was thus established that Article 31 (2) of the Charter is an independent right and not only a principle.[144] The CJEU held that the right to annual leave enshrined in Article 31 (2) of the Charter is an essential principle of EU social law.[145] The Court stressed that

'the right to a period of paid annual leave, affirmed for every worker by Article 31 (2) of the Charter, is thus, as regards its very existence, both mandatory and unconditional in nature, the unconditional nature not needing to be given concrete expression by the provisions of EU or national law, which are only required to specify the exact duration of annual leave and, where appropriate, certain conditions for the exercise of that right.'[146]

This was a conclusive differentiation from the *AMS* case.[147] This is because, in contrast to Article 27 of the Charter, Article 31 (2) does not refer to Union law, national laws and practices.[148] Accordingly, Charter provisions that refer to Union or national law for specification do not have horizontal effect.[149] By contrast, it follows from these considerations that Charter provisions that are unconditional and mandatory have a horizontal effect.[150] This applies in particular to the social rights of the Charter in all disputes with a connection to Union law.[151]

---

[142] Ibid, para. 87; see also Case C-684/16 *Max-Planck-Gesellschaft* (*supra* Chapter VI. note 134), para. 76.

[143] Case C-569/16 *Bauer* (*supra* Chapter VI. note 87), paras. 85, 88–90.

[144] R. Krause, 'Horizontal Effect of the EU Charter of Fundamental Rights: Bauer and Willmeroth, MPG', (*supra* Chapter VI. note 79), p. 1189.

[145] Case C-569/16 *Bauer* (*supra* Chapter VI. note 87), para. 84.

[146] Ibid, para. 85; see also Case C-684/16 *Max-Planck-Gesellschaft* (*supra* Chapter VI. note 134), para. 74.

[147] E. Frantziou, 'The Horizontal Effect of the Charter: Towards an Understanding of Horizontality as a Structural Constitutional Principle' (*supra* Chapter VI. note 90), p. 217.

[148] Case C-569/16 *Bauer* (*supra* Chapter VI. note 87), para. 84.

[149] E. Muir, 'The Horizontal Effects of Charter Rights Given Expression to in EU Legislation, from Mangold to Bauer' (*supra* Chapter VI. note 112), p. 202.

[150] E. Frantziou, '(Most of) the Charter of Fundamental Rights is Horizontally Applicable' (*supra* Chapter VI. note 130), p. 313; E. Frantziou, 'The Horizontal Effect of the Charter: Towards an Understanding of Horizontality as a Structural Constitutional Principle' (*supra* Chapter VI. note 90), p. 217; D. Leczykiewicz, 'The Judgment in *Bauer* and the Effect of the EU Charter of Fundamental Rights in Horizontal Situations' (*supra* Chapter VI. note 140), p. 333.

[151] E. Frantziou, '(Most of) the Charter of Fundamental Rights is Horizontally Applicable' (*supra* Chapter VI. note 130), p. 315.

e) Balancing fundamental rights

As mentioned above, the phenomenon of personal data as an economic asset mostly involves private individuals and companies. In these constellations there are parties on both sides who can invoke their rights under the Charter.[152] In the case of horizontal effect of certain Charter provisions, it should be noted that persons bound by the Charter may also invoke their respective fundamental rights.[153] Therefore, the balance of conflicting fundamental rights must be taken into account in the case of a horizontal effect.[154] The impaired fundamental rights of one party must be reconciled with the protected fundamental right of the other party.[155]

An example for this would be the right to data protection on the one hand and the right to freedom of expression and information on the other. Individuals and companies could claim that they use personal data as an economic asset to hold an opinion and/or to receive and impart information and ideas. On the other hand, individuals might invoke their right to data protection, for example to have their personal data deleted. Article 85 GDPR addresses this interaction and states that the right to protection of personal data should be reconciled with the right to freedom of expression and information. In such cases, private autonomy is to be given essential importance.[156]

Moreover, the CJEU has repeatedly emphasised that it is necessary to balance the rights and freedoms enshrined in Article 16 of the Charter on the one hand and Articles 10 or 21 of the Charter on the other.[157] The CJEU seems to favour economic interests over social interests in this regard.[158] Even if modern society requires a horizontal effect of fundamental rights, it must not be limitless and, in particular, the fundamental rights of right-holders must be balanced.[159] A further

---

[152] H.D. Jarass, 'Die Bedeutung der Unionsgrundrechte unter Privaten' (*supra* Chapter VI. note 76), p. 311.

[153] H. D. Jarass, 'EU-Grundrechte-Charta Art. 51 Anwendungsbereich' (*supra* Chapter VI. note 5), para. 42; T. Kingreen, 'Art. 51 GRCh' (*supra* Chapter VI. note 10), para. 27.

[154] A. Schwerdtfeger, 'Artikel 51 Anwendungsbereich' (*supra* Chapter VI. note 5), para. 59; E. Frantziou, 'The Horizontal Effect of the Charter of Fundamental Rights of the EU: Rediscovering the Reasons for Horizontality' (*supra* Chapter VI. note 75), p. 672; C. Ladenburger and J. Vondung, 'Art. 51. Anwendungsbereich' (*supra* Chapter VI. note 9), para. 43.

[155] C. Ladenburger and J. Vondung, 'Art. 51. Anwendungsbereich' (*supra* Chapter VI. note 9), para. 43; E. Muir, 'The Horizontal Effects of Charter Rights Given Expression to in EU Legislation, from Mangold to Bauer' (*supra* Chapter VI. note 112), p. 185.

[156] E. Frantziou, 'The Horizontal Effect of the Charter of Fundamental Rights of the EU: Rediscovering the Reasons for Horizontality' (*supra* Chapter VI. note 75), p. 673; C. Ladenburger and J. Vondung, 'Art. 51. Anwendungsbereich' (*supra* Chapter VI. note 9), para. 43.

[157] Case C-157/15 *Achbita*, EU:C:2017:203, paras. 37–38; Case C-804/18 *WABE*, EU:C:2021:594, para. 70.

[158] S. Garben, 'Balancing social and economic fundamental rights in the EU legal order', 11 *European Labour Law Journal* (2020), p. 382.

[159] E. Frantziou, 'The Horizontal Effect of the Charter of Fundamental Rights of the EU: Rediscovering the Reasons for Horizontality' (*supra* Chapter VI. note 75), p. 677.

analysis of the balancing of different fundamental rights in the commercial use of personal data is provided below in Chapter VIII. 2.

f) Horizontal effect of Article 8 of the Charter

The CJEU had originally been reluctant to recognise the horizontal effect beyond the scope of the prohibition of discrimination.[160] In *Dominguez*[161] and *Fenoll*[162] only secondary law was discussed and its interplay with constitutional norms was not addressed, despite the similarities to *Kükükdeveci*.[163] Extending the horizontal effect excessively could run the risk of the CJEU being accused of exceeding its powers.[164]

The CJEU has not yet examined a horizontal effect of Article 8 of the Charter after *Egenberger, IR* and *Bauer*. Keeping this in mind, the essential question for this work is whether other fundamental rights, in addition to those already identified by the CJEU, also have horizontal effect. Nowadays, virtually everyone is confronted with search engines or social networks. These companies have an impact on access to fundamental rights that cannot be ignored.[165] In particular, their use of personal data as an economic asset affects the fundamental right to data protection. Does the fundamental right to data protection set out in Article 8 of the Charter therefore also have horizontal effect?

As already discussed above, national laws that violate provisions of the Charter are inapplicable.[166] Furthermore, secondary EU and national law must be interpreted and applied in the light of the respective fundamental right, i.e. in conformity with the Charter.[167] Secondary law, as mentioned above, which 'gives specific expression' to a fundamental right or general principle, thus has an impact on horizontal disputes between individuals.[168] This approach, which *Muir* calls the 'Kücükdeveci effect', could also be used accordingly for the fundamental right to data protection, since secondary law, i.e. the GDPR, 'gives specific ex-

---

[160] E. Muir, 'The Horizontal Effects of Charter Rights Given Expression to in EU Legislation, from Mangold to Bauer' (*supra* Chapter VI. note 112), p. 194.

[161] Case C-282/10 *Dominguez*, EU:C:2012:33.

[162] Case C-316/13 *Fenoll*, EU:C:2015:200.

[163] E. Muir, 'The Horizontal Effects of Charter Rights Given Expression to in EU Legislation, from Mangold to Bauer' (*supra* Chapter VI. note 112), p. 195.

[164] Ibid, p. 213.

[165] E. Frantziou, 'The Horizontal Effect of the Charter of Fundamental Rights of the EU: Rediscovering the Reasons for Horizontality' (*supra* Chapter VI. note 75), p. 675.

[166] H. D. Jarass, 'EU-Grundrechte-Charta Art. 8 Schutz personenbezogener Daten' (*supra* Chapter VI. note 64), para. 3.

[167] Ibid.

[168] E. Muir, 'The fundamental rights implications of EU legislation: Some constitutional challenges' (*supra* Chapter VI. note 116), p. 230; V. Boehme-Neßler, 'Das Recht auf Vergessenwerden – Ein neues Internet-Grundrecht im Europäischen Recht', 33 *NVwZ – Neue Zeitschrift für Verwaltungsrecht* (2014), p. 828.

pression' to that fundamental right.[169] Article 8 of the Charter thus has horizontal effect through the interpretation of secondary data protection law (e.g. the GDPR), which is also addressed to private individuals, in conformity with the right to data protection, whereby the contents of Article 8 become relevant for horizontal disputes between individuals via secondary law.[170] This would correspond to the second level in *Frantziou*'s three-level system mentioned above, i.e. the indirect horizontal effect.

This approach was already adopted by Advocate General *Kokott* in *Promusicae* when she argued that

> 'the secondary legislation gives concrete expression to the requirements as regards fundamental rights to data protection and extends them […] and gives concrete expression to an objective of protection resulting from the fundamental right to data protection'.[171]

She further explained that the fundamental right to data protection provides important guidance for the interpretation of secondary law provisions.[172] The fundamental right to data protection was used to interpret the DPD, which itself covered not only state but also private data processing activities.[173]

The CJEU has since used Article 8 of the Charter several times to interpret secondary data protection law.[174] Thus, the fundamental right to data protection enshrined in Article 8 of the Charter has horizontal effect as a standard of inter-

---

[169] E. Muir, 'The fundamental rights implications of EU legislation: Some constitutional challenges' (*supra* Chapter VI. note 116), p. 226.

[170] T. Riesz, 'Art 8 GRC. Schutz personenbezogener Daten' (*supra* Chapter VI. note 27), para. 89.

[171] Opinion of Advocate General Kokott Case C-275/06 *Promusicae*, EU:C:2007:454, para. 57.

[172] Ibid.

[173] R. Streinz and W. Michl, 'Die Drittwirkung des europäischen Datenschutzgrundrechts (Art. 8 GRCh) im deutschen Privatrecht', 22 *EuZW – Europäische Zeitschrift für Wirtschaftsrecht* (2011), p. 386.

[174] See Case C–543/09 *Deutsche Telekom* (*supra* Chapter IV. note 295); Case C–468/10 *ASNEF*, EU:C:2011:777; Case C–70/10 *Scarlet* (*supra* Chapter II. note 130); Case C–291/12 *Schwarz* (*supra* Chapter II. note 131); Case C–293/12 *Digital Rights Ireland* (*supra* Chapter II. note 130); Case C–131/12 *Google Spain and Google* (*supra* Chapter IV. note 283); Case C–141/12 *Y.S.* (*supra* Chapter II. note 65); Case C–212/13 *Ryneš* (*supra* Chapter II. note 34); Case C-446/12 *Willems and Others*, EU:C:2015:238; Case C-362/14 *Schrems* (*supra* Chapter VI. note 64); Case C-203/15 *Tele2 Sverige*, EU:C:2016:970; Case C-398/15 *Manni*, EU:C:2017:197; Case C-207/16 *Ministerio Fiscal*, EU:C:2018:788; Case C-136/17 *GC and Others* (*supra* Chapter IV. note 295); Case C-708/18 *Asociatia de Proprietari bloc M5A-ScaraA*, EU:C:2019:1064; Case C-311/18 *Facebook Ireland and Schrems* (*supra* Chapter IV. note 295); Case C-623/17 *Privacy International*, EU:C:2020:790; Joined Cases C-511/18, C-512/18 and C-520/18 *La Quadrature du Net and Others*, EU:C:2020:791; Case C-746/18 *Prokuratuur*, EU:C:2021:152; Case C-645/19 *Facebook Ireland and Others*, EU:C:2021:483; Joined Cases C-339/20 and C-397/20 *VD*, EU:C:2022:703; Joined Cases C-793/19 and C-794/19 *SpaceNet*, EU:C:2022:702; Case C-460/20 *Google*, EU:C:2022:962; Case C-333/22 *Ligue des droits humains,* EU:C:2023:874.

pretation and through the objective of protection.[175] This could, for example, lead to the CJEU deciding that certain provisions of the GDPR, interpreted in the light of Article 8 of the Charter, preclude the use of personal data as an economic asset.

Another argument speaks for the direct horizontal effect of Article 8 of the Charter, which would correspond to the third level in *Frantziou*'s three-level system. As discussed above, Charter provisions that are unconditional and mandatory have a horizontal effect. This is the current stance of the CJEU on the horizontal effect of the Charter provisions. If one examines Article 8 of the Charter, it becomes clear that it is unconditional and mandatory. This follows from the fact that Article 8 of the Charter does not refer to Union or national law for specification. In light of its wording, Article 8 of the Charter does not require any further specification or supplementary measure to be adopted. An argument that was also made regarding the direct effect of Article 31 (2) of the Charter[176] and Articles 21 and 47 of the Charter[177]. In contrast to Article 27 of the Charter, which, in order to be fully effective, requires 'more specific expression in European Union or national law',[178] Article 8 of the Charter does not refer to Union law, national laws and practices.

Furthermore, the fact that Article 8 of the Charter is concretised by the GDPR and national data protection laws does not exclude a horizontal effect of Article 8 of the Charter. The adoption of an act of secondary EU law or implementing measures by Member States is rather helpful for the exercise of the fundamental right to data protection.[179] All in all, a sophisticated application of horizontality would favour an effective and uniform application of Union law and subsequently lead to greater social inclusion, prosperity and ultimately, equality.[180]

Streinz/Michl argue that a horizontal effect of the fundamental right to data protection can also arise through the applicability of the fundamental freedoms of the EU.[181] They refer to the *Viking* case, in which the restriction of freedom of establishment by a trade union's right to strike was addressed. Here, Advocate General *Poiares Maduro* clearly supported a horizontal effect.[182] Already in *Fa-*

---

[175] R. Streinz and W. Michl, 'Die Drittwirkung des europäischen Datenschutzgrundrechts (Art. 8 GRCh) im deutschen Privatrecht' (*supra* Chapter VI. note 173), p. 386.

[176] Case C-569/16 *Bauer* (*supra* Chapter VI. note 87), para. 84; Opinion of Advocate General Bot in Case C-569/16 *Bauer*, EU:C:2018:337, para. 83.

[177] Case C-414/16 *Egenberger* (*supra* Chapter VI. note 87), para. 78.

[178] Case C-176/12 *Association de médiation sociale* (*supra* Chapter VI. note 119), para. 45.

[179] See regarding Article 31(2) of the Charter: Opinion of Advocate General Bot in Case C-569/16 *Bauer* (*supra* Chapter VI. note 176), para. 83.

[180] E. Frantziou, 'The Horizontal Effect of the Charter of Fundamental Rights of the EU: Rediscovering the Reasons for Horizontality' (*supra* Chapter VI. note 75), p. 674.

[181] R. Streinz and W. Michl, 'Die Drittwirkung des europäischen Datenschutzgrundrechts (Art. 8 GRCh) im deutschen Privatrecht' (*supra* Chapter VI. note 173), p. 387.

[182] Opinion of Advocate General Poiares Maduro in Case C-438/05 *Viking*, EU:C:2007:292, para. 40.

miliapress, fundamental freedoms were examined in the light of fundamental rights.[183] Thus, fundamental freedoms and fundamental rights are intertwined in horizontal disputes between individuals.[184] *Streinz/Michl* point out that it would be feasible for employees to rely on Article 8 of the Charter against companies that make use of their freedom of establishment in order to challenge job applications or working conditions that are in conflict with data protection law.[185] They argue that the possibility of such a use of fundamental freedoms becomes apparent if the *Angonese*[186] case concerning the horizontal effect of the free movement of workers is reshaped in a way that the bank concerned would have requested information on sensitive data of the applicant instead of proof of bilingualism.[187]

In *Angonese*, the CJEU emphasised that the discrimination on grounds of nationality applies in horizontal disputes between individuals, too.[188] The CJEU held that limiting the applicability to the public sector would lead to inequality between the public and private sector.[189] In addition, the Court found that the abolition of obstacles of the fundamental freedoms would not be effective if individuals and/or private entities were free to create new obstacles.[190] Fundamental rights and freedoms are of great importance among private individuals, especially in the case of social media platforms or search engines on the Internet.[191]

Normative arguments due to a frequent imbalance of power also indicate that Article 8 of the Charter has horizontal effect. Private actors can accumulate enormous power through personal data on data subjects.[192] Private companies and individuals endanger the privacy and personal data of those affected just as much as states.[193] Taking up *Angonese*'s line of argument, in order to guarantee

---

[183] See Case C-368/95 *Familiapress*, EU:C:1997:325.

[184] R. Streinz and W. Michl, 'Die Drittwirkung des europäischen Datenschutzgrundrechts (Art. 8 GRCh) im deutschen Privatrecht' (*supra* Chapter VI. note 173), p. 387.

[185] Ibid.

[186] Case C-281/98 *Angonese*, EU:C:2000:296.

[187] R. Streinz and W. Michl, 'Die Drittwirkung des europäischen Datenschutzgrundrechts (Art. 8 GRCh) im deutschen Privatrecht' (*supra* Chapter VI. note 173), p. 388.

[188] Case C-281/98 *Angonese* (*supra* Chapter VI. note 186), para. 36; see also T. Kingreen, 'Art. 51 GRCh' (*supra* Chapter VI. note 10), para. 25; now laid down in Article 15 (2) of the Charter.

[189] Case C-281/98 *Angonese* (*supra* Chapter VI. note 186), para. 33; see also, Case C-36/74 *Walrave*, EU:C:1974:140, para. 19; Case C-415/93 *Bosman*, EU:C:1995:463, para. 84.

[190] Case C-281/98 *Angonese* (*supra* Chapter VI. note 186), para. 32; see also Case C-36/74 *Walrave* (*supra* Chapter VI. note 189), para. 18; Case C-415/93 *Bosman* (*supra* Chapter VI. note 189), para. 83.

[191] H. D. Jarass, 'EU-Grundrechte-Charta Art. 8 Schutz personenbezogener Daten' (*supra* Chapter VI. note 64), para. 3.

[192] M. von Grafenstein, 'Refining the Concept of the Right to Data Protection in Article 8 ECFR – Part III', 7 *EDPL – European Data Protection Law Review* (2021), p. 375.

[193] T. Riesz, 'Art 8 GRC. Schutz personenbezogener Daten' (*supra* Chapter VI. note 27),

truly effective data protection, the fundamental right to data protection must be addressed not only to state authorities, bodies and institutions, but also to private individuals.[194]

In order to balance power asymmetries, it must not matter whether an employee works for the State or a private employer, for example.[195] The horizontal effect of the Charter has so far only been assumed at the expense of employers, which would suggest that only predominant private individuals in asymmetrical relationships are directly bound by the Charter.[196] Thus, a direct horizontal effect could also arise vis-à-vis businesses who operate transnationally in a sector that is harmonised by secondary law.[197]

This imbalance of power between companies and individuals is particularly evident in the data economy. *Roßnagel* argues that private providers who operate infrastructures of the digital world are all the more subject to a fundamental rights obligation, the more dependent society is on these infrastructure services and the more profoundly the service interferes with fundamental rights, in particular informational self-determination and social communication.[198] Moreover, data processing is harmonised across the EU by the GDPR, i.e. secondary law. The constitutionalisation of private law, potentially causing legal uncertainty in cases governed by directives, does not pose a similar concern in the context of the GDPR, which, when interpreted in light of the Charter, is inherently directly applicable. The argument could thus be made that data processing and therefore the commercialisation of data trigger a horizontal effect of the Charter.

4. Conclusion: The Charter can be applied to the use of personal data as an economic asset

It can be concluded that the Charter can be applied to the economic exploitation of personal data by institutions and bodies of the EU. The Charter applies regardless of the nature of the Union's action.

---

para. 89; R. Streinz and W. Michl, 'Die Drittwirkung des europäischen Datenschutzgrundrechts (Art. 8 GRCh) im deutschen Privatrecht' (*supra* Chapter VI. note 173), p. 385; V. Boehme-Neßler, 'Das Recht auf Vergessenwerden – Ein neues Internet-Grundrecht im Europäischen Recht' (*supra* Chapter VI. note 168), p. 828.

[194] I. Augsberg, 'Art 8. Schutz personenbezogener Daten', in H. von der Groeben, J. Schwarze and A. Hatje (eds.), *Europäisches Unionsrecht* (7th edition, Nomos, 2015), para. 9.

[195] R. Krause, 'Horizontal Effect of the EU Charter of Fundamental Rights: Bauer and Willmeroth, MPG', (*supra* Chapter VI. note 79), p. 1197.

[196] Ibid.

[197] C. Ladenburger and J. Vondung, 'Art. 51. Anwendungsbereich' (*supra* Chapter VI. note 9), para. 13.

[198] A. Roßnagel, 'Kein "Verbotsprinzip" und kein "Verbot mit Erlaubnisvorbehalt" im Datenschutzrecht', 72 *NJW – Neue Juristische Wochenschrift* (2019), p. 3.

Member States are covered by the Charter when they are implementing Union law. 'Implementing Union law' requires a connection to Union law, e.g. the implementation and enforcement of secondary Union law. When it comes to the economic use of personal data by Member States, there is a lot of relevant secondary law and therefore the Charter often applies because secondary law, such as the GDPR and other pieces of secondary law, is implemented.

Since personal data is mostly used by private companies as an economic asset, the case law of the CJEU in this regard was examined, which assumes an applicability of the Charter beyond the actual wording. It follows from the relevant case law that Charter provisions that are unconditional and mandatory have a horizontal effect. It was argued above that Article 8 of the Charter has such unconditional and mandatory nature. Furthermore, the fundamental right to data protection enshrined in Article 8 of the Charter has horizontal effect as a standard of interpretation of secondary data protection law.

From a normative perspective, in order to guarantee truly effective data protection and redress power asymmetries, the fundamental right to data protection must be addressed not only to state authorities, bodies and institutions, but also to private individuals and companies. They have acquired tremendous economic and informational power through the accumulation of personal data.

VII. Personal data as an economic asset in the light of Article 8 of the Charter

Article 8 of the Charter establishes the right to protection of personal data as an independent, innovative and modern fundamental right.[1] As the world and society become more and more digitalised and connected, the fundamental right to protection of personal data becomes, in a sense, a 'super fundamental right'.[2] The right to protection of personal data has its roots in the right to privacy, but, despite common roots and similarities, is distinct from it, as the right to protection of personal data is an active right, including rights and obligations, and does not merely state general principles.[3] This active right has as its overarching theme the protection of the autonomy of data subjects.[4] In order to protect the autonomy of data subjects, Article 8 of the Charter addresses the challenges of advancing technological progress and its implications for data protection.[5] One of these challenges is the commercialisation of personal data.[6]

The use of personal data as an economic asset will be examined in this chapter with regard to its compatibility with Article 8 of the Charter. The GDPR will also be referenced for this purpose. The GDPR concretises the fundamental right to data protection and regulates data processing for public and private actors in the Member States.[7] This reference to the GDPR is appropriate because the Expla-

---

[1] H. Johlen, 'Art. 8 Schutz personenbezogener Daten' in K. Stern and M. Sachs (eds.), *GRCh – Europäische Grundrechte-Charta*, para. 1; N. Bernsdorff, 'Artikel 8 Schutz personenbezogener Daten' in J. Meyer and S. Hölscheidt (eds.), *Charta der Grundrechte der Europäischen Union*, para. 12.

[2] M. von Grafenstein, 'Refining the Concept of the Right to Data Protection in Article 8 ECFR – Part I', 6 *EDPL – European Data Protection Law Review* (2020), p. 511.

[3] C. Docksey, 'Four fundamental rights: finding the balance', 6 *International Data Privacy Law* (2016), p. 198; Mostert et al. describe the right to data protection as a more positive approach, i.e. positive obligation, M. Mostert et al., 'From Privacy to Data Protection in the EU: Implications for Big Data Health Research', 25 *European Journal of Health and Law* (2018), p. 49.

[4] M. von Grafenstein, 'Refining the Concept of the Right to Data Protection in Article 8 ECFR – Part I' (*supra* Chapter VII. note 2), p. 516.

[5] H. Johlen, 'Art. 8 Schutz personenbezogener Daten' (*supra* Chapter VII. note 1), para. 1.

[6] See Custers and Malgieri who argue that the fundamental right to data protection stands in the way of the commodification of personal data, B. Custers and G. Malgieri, 'Priceless data: why the EU fundamental right to data protection is at odds with trade in personal data' (*supra* Chapter I. note 11), p. 7.

[7] H.D. Jarass, 'Art. 8 Schutz personenbezogener Daten' (*supra* Chapter VI. note 64), para. 5.

nations to Article 8 of the Charter state that Article 8 of the Charter is based on the DPD and, as already described in Chapter II., the GDPR closely follows the DPD in many regards.[8] Thus, the GDPR can be used as an interpretative guidance for the fundamental right to data protection enshrined in Article 8 of the Charter.[9] The Explanations also indicate that secondary law includes 'conditions and limitations for the exercise of the right to the protection of personal data'.[10] Moreover, Article 8 of the Charter is noticeably based on the concepts and definitions of the DPD and the GDPR.[11] Furthermore, the GDPR itself acknowledges in Recital 10 that the GDPR establishes rules for data processing in respect of fundamental rights. A factor to which the CJEU itself refers, too.[12] Consequently, secondary law can be used for the interpretation and concretisation of a fundamental right, even if this must be done with caution to avoid giving secondary law precedence over primary law.[13]

In this chapter, the scope of application and protection of Article 8 of the Charter will be set out in Section 1. This is followed by an examination of the requirements of lawful data processing and with regard the use of personal data as an economic asset in Sections 2 – 6. It will be shown that the economic use of personal data is not per se incompatible with Article 8 of the Charter. The conditions under which an economic use of personal data is compatible with Article 8 of the Charter will be discussed.

1. Scope of protection

The right to data protection, as set out in Article 8 of the Charter, has a very broad scope.[14] The scope of protection of the right to data protection goes beyond that of the right to privacy set out in Article 7 of the Charter.[15] Secondary law, e.g.

---

[8] Explanations relating to the Charter of Fundamental Rights [2007] OJ C303/21.

[9] T. Riesz, 'Art 8 GRC. Schutz personenbezogener Daten' (*supra* Chapter VI. note 27), para. 20.

[10] Explanations relating to the Charter of Fundamental Rights [2007] OJ C303/20.

[11] T. Riesz, 'Art 8 GRC. Schutz personenbezogener Daten' (*supra* Chapter VI. note 27), para. 20.

[12] Case C-311/18 *Facebook Ireland and Schrems* (*supra* Chapter IV. note 295), para. 101; Joined Cases C-511/18, C-512/18 and C-520/18 *La Quadrature du Net and Others* (*supra* Chapter VI. note 174), para. 207.

[13] H.D. Jarass, 'Art. 8 Schutz personenbezogener Daten' (*supra* Chapter VI. note 64), paras. 63 and 64; T. Riesz, 'Art 8 GRC. Schutz personenbezogener Daten' (*supra* Chapter VI. note 27), para. 20.

[14] H. Kranenborg, 'Art 8 Protection of Personal Data' in S. Peers et al. (eds.), *The EU Charter of Fundamental Rights* (2nd edition, Hart Publishing, 2021), para. 18; O. Lynskey, 'Delivering Data Protection: The Next Chapter', 21 *German Law Journal* (2020), p. 81; for general remarks on the scope of application of the Charter and the GDPR as a trigger, see Chapter VI.

[15] J. Kokott and C. Sobotta, 'The distinction between privacy and data protection in the

the GDPR, establishes the scope of the right to data protection for the area protected by the instrument.[16] Processing of personal data that falls outside the scope of EU law is not covered by Article 8 of the Charter.[17]

a) Territorial scope

Article 3 GDPR stipulates that data protection rules apply

'to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not'.

For example, the activities of an e-commerce website based outside the EU, which processes personal data exclusively there, and those of a subsidiary in the EU for market research and marketing campaigns, are inextricably linked and thus EU data protection rules apply.[18] In this example, the revenue raising through the activity in the EU is relevant.[19] In addition, the processing of personal data by controllers or processors not established in the EU, fall under EU data protection rules, where goods or services are offered to data subjects in the EU.[20] The use of a language or a currency of a Member State or the remark to customers or users in the EU is sufficient to ascertain an intention to offer goods or services to data subject in the EU.[21] Therefore, a certain targeting criterion is needed.[22]

The CJEU also established a broad territorial scope, as it held that Google's data processing activities in the US took place in the framework of Google's subsidiary in Spain, although the Spanish establishment was only responsible for marketing and did not process any personal data in the present case.[23] The CJEU highlighted that data processing does not require that it is carried out 'by' the establishment, but only 'in the context of the activities of' the establishment.[24]

---

jurisprudence of the CJEU and the ECtHR', p. 225; T. Riesz, 'Art 8 GRC. Schutz personenbezogener Daten' (*supra* Chapter VI. note 27), para. 28; O. Lynskey, 'Deconstructing Data Protection: The "Added-Value" Of A Right To Data Protection in the EU Legal Order' (*supra* Chapter IV. note 190), p. 578.

[16] H. Kranenborg, 'Art 8 Protection of Personal Data' (*supra* Chapter VII. note 14), para. 104.

[17] Ibid, para. 18.

[18] EDPB, *Guidelines 3/2018 on the territorial scope of the GDPR (Article 3)*, 12 November 2019, p. 8.

[19] Ibid.

[20] See Article 3 (2) (a) GDPR.

[21] See Recital 23 GDPR.

[22] EDPB, *Guidelines 3/2018* (*supra* Chapter VII. note 18), p. 13.

[23] Case C-131/12 *Google Spain and Google* (*supra* Chapter IV. note 283), para 60; H. Kranenborg, 'Art 8 Protection of Personal Data' (*supra* Chapter VII. note 14), para. 108.

[24] Case C-131/12 *Google Spain and Google* (*supra* Chapter IV. note 283), para. 52; Case C-230/14 *Weltimmo*, EU:C:2015:639, para. 35; Case C-191/15 *Verein für Konsumenteninfor-*

Regarding search engines, dereferencing must be done EU-wide, but not worldwide.[25] The objective of achieving a high level of protection for personal data throughout the Union was cited as the justification for the broad interpretation.[26] Consequently, the territorial scope is very broad.[27]

In the case of the processing of personal data for its use as an economic asset, the territorial scope of Article 8 of the Charter is thus triggered in the following constellations: firstly, if there is an establishment in the EU, even if personal data is not processed by the establishment but in the context of its activities, and secondly, if there is no establishment in the EU but products or services are offered in a targeted manner to EU citizens.

b) Material scope

In terms of its material scope, Article 8 of the Charter protects the informational self-determination of the data subject and the control over his or her personal data.[28] With this control over one's own personal data comes the ability of data subjects to exclude third parties from using the personal data, to obtain information, to request the erasure of the personal data and to use personal data as an economic asset themselves.[29] An interference with this informational self-determination and the right to data protection could occur when personal data are processed.[30] It is the autonomy of data subjects that could be at risk from data processing.[31]

The Charter does not have its own definition of processing but builds on the concept of processing as defined in the GDPR (originally DPD).[32] Data processing means

---

mation, EU:C:2016:612, para. 78; Case C-210/16 *Wirtschaftsakademie Schleswig-Holstein*, EU:C:2018:388, para. 57.

[25] Case C-507/17 *Google* (*supra* Chapter IV. note 295), para. 62.

[26] Case C-131/12 *Google Spain and Google* (*supra* Chapter IV. note 283), para. 53; Case C-507/17 *Google* (*supra* Chapter IV. note 295), para. 54; Lynskey questions this approach, O. Lynskey, 'Delivering Data Protection: The Next Chapter' (*supra* Chapter VII. note 14), p. 82.

[27] H. Kranenborg, 'Art 8 Protection of Personal Data' (*supra* Chapter VII. note 14), para. 107.

[28] T. Kingreen, 'Art. 8 GRCh' in C. Calliess and M. Ruffert (eds.), *EUV/AEUV* (6th edition, C.H.Beck, 2022), para. 10; A. Roßnagel, 'Kein "Verbotsprinzip" und kein "Verbot mit Erlaubnisvorbehalt" im Datenschutzrecht' (*supra* Chapter VI. note 198), p. 2.

[29] See Chapter IV; see also T. Kingreen, 'Art. 8 GRCh' (*supra* Chapter VII. note 28), para. 10.

[30] H.D. Jarass, 'Art. 8 Schutz personenbezogener Daten' (*supra* Chapter VI. note 64), para. 9; T. Kingreen, 'Art. 8 GRCh' (*supra* Chapter VII. note 28), para. 13.

[31] M. von Grafenstein, 'Refining the Concept of the Right to Data Protection in Article 8 ECFR – Part II', 7 *EDPL – European Data Protection Law Review* (2021), p. 196.

[32] A. Roßnagel, 'Kein "Verbotsprinzip" und kein "Verbot mit Erlaubnisvorbehalt" im Datenschutzrecht' (*supra* Chapter VI. note 198), p. 2.

'any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;'[33]

Processing covers the entire life cycle of personal data, i.e. from collection to deletion.[34] The means or method by which personal data is ultimately processed is not important for the application of Article 8 of the Charter.[35] Moreover, the data processing need not lead to any detriment to trigger the applicability of Article 8 of the Charter.[36] Any data processing constitutes a limitation on the fundamental right to data protection.[37] The term 'processing' must therefore be understood broadly.[38] *Von Grafenstein* thus argues that 'the more social interaction is based on data processing, the greater the scope of (data) protection' and therefore of Article 8 of the Charter.[39] *Brkan* demonstrates that EU data protection in general is expanding both as a fundamental right and at the level of secondary legislation.[40]

As shown in Chapter III., the processing of personal data is the source of creating value, no matter how one measures the value of personal data. For a stringent protection of fundamental rights, it is therefore necessary and right that the economic use of personal data is covered by the Charter. As to what is considered personal data, see the discussion in Chapter II. and the examples provided there.

---

[33] See Article 4 (2) GDPR.

[34] H. Kranenborg, 'Art 8 Protection of Personal Data' (*supra* Chapter VII. note 14), para. 117; H. Johlen, 'Art. 8 Schutz personenbezogener Daten' (*supra* Chapter VII. note 1), para. 34.

[35] N. Bernsdorff, 'Artikel 8 Schutz personenbezogener Daten' (*supra* Chapter VII. note 1), para. 22; T. Riesz, 'Art 8 GRC. Schutz personenbezogener Daten' (*supra* Chapter VI. note 27), para. 47.

[36] N. Bernsdorff, 'Artikel 8 Schutz personenbezogener Daten' (*supra* Chapter VII. note 1), para. 22.

[37] A. Roßnagel, 'Kein "Verbotsprinzip" und kein "Verbot mit Erlaubnisvorbehalt" im Datenschutzrecht' (*supra* Chapter VI. note 198), p. 2.

[38] H. Johlen, 'Art. 8 Schutz personenbezogener Daten' (*supra* Chapter VII. note 1), para. 34; N. Bernsdorff, 'Artikel 8 Schutz personenbezogener Daten' (*supra* Chapter VII. note 1), para. 22.

[39] M. von Grafenstein, 'Refining the Concept of the Right to Data Protection in Article 8 ECFR – Part I' (*supra* Chapter VII. note 2), p. 510.

[40] M. Brkan, 'The Unstoppable Expansion of the EU Fundamental Right to Data Protection: Little Shop of Horrors?', 23 *Maastricht Journal of European and Comparative Law* (2016), p. 840.

c) Personal scope

In principle, every data subject, i.e. natural person can invoke the fundamental right to data protection.[41] Not only EU citizens, but also third-country nationals could invoke it.[42] The extent to which legal persons can also invoke Article 8 of the Charter is disputed.[43] On the basis of literal and systematic considerations, there are good reasons for including legal persons in the scope of protection of Article 8 of the Charter.[44] As already described in Chapter II., the CJEU has also supported the partial inclusion of legal persons.[45]

Essential for the personal scope in Article 8 of the Charter are also the controller and the processor.[46] The former decides on the purposes and means of the processing of personal data, while the latter processes the personal data on behalf of the controller.[47] For the data subject, the controller and processor are important as addressees of the right to data protection, but the exact constellation and relationship of controller and processor is often obscure.[48] This has been illustrated by the example of Facebook in Chapter III. It is therefore unsurprising that the CJEU has developed a wide line of case law in this regard. The Court held that operators of a search engine,[49] a petition committee[50] and a religious community with its members who engage in preaching[51] can be controllers. In addition, the CJEU acknowledged that the operator of a fan page on Facebook is also

---

[41] H. Kranenborg, 'Art 8 Protection of Personal Data' (*supra* Chapter VII. note 14), para. 127; T. Riesz, 'Art 8 GRC. Schutz personenbezogener Daten' (*supra* Chapter VI. note 27), para. 48; H.D. Jarass, 'Art. 8 Schutz personenbezogener Daten' (*supra* Chapter VI. note 64), para. 8.

[42] T. Riesz, 'Art 8 GRC. Schutz personenbezogener Daten' (*supra* Chapter VI. note 27), para. 48.

[43] See H. Johlen, 'Art. 8 Schutz personenbezogener Daten' (*supra* Chapter VII. note 1), paras. 25–28; N. Bernsdorff, 'Artikel 8 Schutz personenbezogener Daten' (*supra* Chapter VII. note 1), para. 25.

[44] T. Kingreen, 'Art. 8 GRCh' (*supra* Chapter VII. note 28), para. 12; H.D. Jarass, 'Art. 8 Schutz personenbezogener Daten' (*supra* Chapter VI. note 64), para. 8; T. Riesz, 'Art 8 GRC. Schutz personenbezogener Daten' (*supra* Chapter VI. note 27), para. 48.

[45] Case C-92/09 *Volker und Markus Schecke und Eifert* (*supra* Chapter II. note 184), para. 45; Case C-419/14 *WebMindLicenses* (*supra* Chapter II. note 185), para. 79; H.D. Jarass, 'Art. 8 Schutz personenbezogener Daten' (*supra* Chapter VI. note 64), para. 8; T. Riesz, 'Art 8 GRC. Schutz personenbezogener Daten' (*supra* Chapter VI. note 27), para. 48.

[46] H. Kranenborg, 'Art 8 Protection of Personal Data' (*supra* Chapter VII. note 14), para. 128.

[47] See Article 4 (7) and (8) GDPR.

[48] H. Kranenborg, 'Art 8 Protection of Personal Data' (*supra* Chapter VII. note 14), para. 130.

[49] Case C-131/12 *Google Spain and Google* (*supra* Chapter IV. note 283), para. 41; Case C-136/17 *GC and Others* (*supra* Chapter IV. note 295), para. 35; Case C-460/20 *Google* (*supra* Chapter VI. note 174), para. 49; Case C-129/21 *Proximus*, EU:C:2022:833, para. 95.

[50] Case C-272/19 *Land Hessen*, EU:C:2020:535, para. 74.

[51] Case C-25/17 *Jehovan todistajat*, EU:C:2018:551, para. 75.

considered a controller.[52] It argued that a fan page operator can demand demographic data about its target group (including age, gender, relationship status, professional situation, information about the lifestyle and the interests) and thus the processing of personal data.[53] The fan page operator thus has a say in the means and purposes of processing the personal data.[54] Moreover, the role as controller is justified, especially since even persons who do not have a user account on Facebook automatically trigger the processing of their personal data through the mere accessing of the fan page.[55]

Furthermore, the CJEU held that the operator of a website who embeds in that website a social plugin which transmits personal data of the website's visitor to the provider of the social plugin is to be considered as a controller.[56] In this judgment, too, the CJEU based its decision on whether the website operator could have a say in the purpose and means of data processing.[57] The CJEU emphasised that the integration of the social plugin gives the operator of the website a commercial advantage by increasing publicity for its goods.[58] The CJEU stressed that the use of those personal data are in the economic and commercial interest of the website operator and the provider of the social plugin.[59] This rationale is particularly worth highlighting, as the CJEU in other words ruled that the commercial use of and economic interest in personal data, as described in Chapter III., may be decisive in triggering the application of data protection rules.

2. Data processing as limitation of Article 8 of the Charter

A limitation on the exercise of the right to data protection is the processing of personal data as such.[60] Thus, in principle, any use of personal data as an economic asset is a limitation. An exception to this rule is valid consent. Valid consent to the use of personal data as an economic asset, as explained below in Chapter VII. 4., excludes a limitation of the right to data protection.[61] Thus, there is no need to examine whether a limitation is justified, as there is no limitation.

---

[52] Case C-210/16 *Wirtschaftsakademie Schleswig-Holstein* (*supra* Chapter VII. note 24), para. 44.

[53] Ibid, para. 37.

[54] Ibid, para. 39.

[55] Ibid, para. 41.

[56] Case C-40/17 *Fashion ID*, EU:C:2019:629, para. 85.

[57] Ibid, para. 76.

[58] Ibid, para. 80.

[59] Ibid, para. 80.

[60] Case C-293/12 *Digital Rights Ireland* (*supra* Chapter II. note 130), para. 36; H. Krämer, 'Art. 52 Tragweite und Auslegung der Rechte und Grundsätze' in K. Stern and M. Sachs (eds.), *GRCh – Europäische Grundrechte-Charta*, para. 31.

[61] H.D. Jarass, 'Art. 8 Schutz personenbezogener Daten' (*supra* Chapter VI. note 64), para. 9; A. Ingold, 'Artikel 7 Bedingungen für die Einwilligung' (*supra* Chapter V. note 65),

Nevertheless, the economic use of personal data is not limitless. Under no circumstances should Article 8 of the Charter legitimise exploitative and unfair business models, as *Lynskey* rightly points out.[62] The limits to the use of personal data as an economic asset can be found in Article 8 (2) of the Charter and Article 52 (1) thereof, as outlined in Chapter VIII. Article 8 (2) of the Charter states that personal data 'must be processed fairly for specified purposes and on the basis of consent of the person concerned or some other legitimate basis laid down by law'. There are thus two conditions for data processing to be in compliance with the fundamental right to data protection:[63] (i) It requires the consent of the data subject or another legal basis. (ii) In any case, personal data must be processed fairly and for specific purposes. The possible limitation by 'some other legitimate basis' laid down in Article 8 (2) of the Charter specifies the general limitation clause in Article 52 (1) of the Charter and represents a manifestation of the principle of proportionality set out there.[64]

Docksey calls these conditions the 'digital Highway Code', which is meant to regulate, not prohibit, the processing of personal data.[65] Likewise, *Roßnagel* emphasises that according to Article 8 of the Charter, data processing is not prohibited per se, but rather socially desirable and undesirable data processing activities have to be distinguished from each other.[66] Data protection law thus allows interferences with the fundamental right to data protection on the basis of their social necessity or desirability.[67]

Véliz argues that 'personal data is toxic' and that 'it can ruin your life'.[68] However, not every processing of personal data limits the exercise of the fundamental right to data protection.[69] As the German *Datenethikkommission* rightly points out, the processing and use of personal data as an economic asset by the data subject or even third parties does not in itself necessarily constitute a limitation.[70] A limitation may arise from the context or purpose of data processing.[71]

---

para. 9; T. Kingreen, 'Art. 8 GRCh' (*supra* Chapter VII. note 28), para. 14; T. Riesz, 'Art 8 GRC. Schutz personenbezogener Daten' (*supra* Chapter VI. note 27), para. 69.

[62] O. Lynskey, 'Delivering Data Protection: The Next Chapter' (*supra* Chapter VII. note 14), p. 84

[63] T. Riesz, 'Art 8 GRC. Schutz personenbezogener Daten' (*supra* Chapter VI. note 27), para. 60.

[64] Ibid.

[65] C. Docksey, 'Four fundamental rights: finding the balance' (*supra* Chapter VII. note 3), p. 199.

[66] A. Roßnagel, 'Kein "Verbotsprinzip" und kein "Verbot mit Erlaubnisvorbehalt" im Datenschutzrecht' (*supra* Chapter VI. note 198), p. 4.

[67] Ibid.

[68] C. Véliz, *Privacy Is Power* (*supra* Chapter III. note 42), p. 108.

[69] M. von Grafenstein, 'Refining the Concept of the Right to Data Protection in Article 8 ECFR – Part II' (*supra* Chapter VII. note 31), p. 196.

[70] Datenethikkommission, *Gutachten der Datenethikkommission*, p. 104.

[71] Ibid.

Or as *Prins* put it: 'it is not so much *whether* personal data are processed […] the problem is *how* personal data are processed.'[72]

In the following, the lawful use of personal data will be analysed on the basis of these conditions. The limits of the economic use of personal data are those of common processing of personal data and are neither stricter nor more generous.[73] When considering the requirements for lawful data processing, economic aspects must be taken into account, e.g. economic pressure can be relevant for the freely given consent.[74] Although consent is considered to be only one of the grounds for legitimate processing,[75] it will be shown that the consent of the data subject is the only legitimate basis when using personal data as an economic asset.[76]

3. Fair use of personal data as an economic asset for specified purposes

a) Fairly processed personal data

Clifford/Ausloos emphasise that 'fairness' is one of the core elements of data protection law.[77] This principle of fairness is unique to the right to data protection.[78] Different language versions of Article 8 (2) of the Charter make it clear that personal data should be processed 'fairly', which is a nuanced difference from the German language version which refers to '*Treu und Glauben*' (good faith).[79] Fairness is to be understood as a safeguarding of interests and thus represents a form of the principle of proportionality.[80] In this context, the principle of fairness has a fall-back function.[81] This is in order to be able to qualify

---

[72] C. Prins, 'Property and Privacy: European Perspectives and the Commodification of our Identity' in L. Guibault and P.B. Hugenholtz (eds.), *The Future of the Public Domain, Identifying the Commons in Information Law* (Kluwer Law International, 2006), p. 255.

[73] Datenethikkommission, *Gutachten der Datenethikkommission*, p. 104.

[74] Ibid.

[75] H. Kranenborg, 'Art 8 Protection of Personal Data' (*supra* Chapter VII. note 14), para. 34.

[76] See also B. Custers and G. Malgieri, 'Priceless data: why the EU fundamental right to data protection is at odds with trade in personal data' (*supra* Chapter I. note 11), p. 9; see also concerning behavioural targeting: F. Zuiderveen Borgesius, 'Legal basis for behavioural targeting', 5 *International Data Privacy Law* (2015), p. 165.

[77] D. Clifford and J. Ausloos, 'Data Protection and the Role of Fairness', 37 *Yearbook of European Law* (2018), p. 133.

[78] C. Docksey, 'Four fundamental rights: finding the balance' (*supra* Chapter VII. note 3), p. 198.

[79] See T. Riesz, 'Art 8 GRC. Schutz personenbezogener Daten' (*supra* Chapter VI. note 27), para. 63 referring to the English version of the Charter of 'fairly', the French version of 'loyalement' or the Italian of 'lealtá'.

[80] Ibid, para. 63.

[81] Ibid; H. Kranenborg, 'Art 8 Protection of Personal Data' (*supra* Chapter VII. note 14),

data processing that may be contrary to the interests or the will of the data subject as unlawful, even if consent or other legal bases are given.[82] In this sense, the CJEU has also used the principle of fairness to hold that contractual provisions relating to consent to data processing should not be misleading.[83]

To ensure the principle of fairness, the data subject must be informed about the identity of the data controller, the purposes of the processing, the recipients of the personal data and the existence of a right of access to and the right to rectify the personal data.[84] The data subject must therefore be informed about the existence of data processing in a transparent manner.[85] To some extent, this illustrates the principle of fairness, lawfulness and transparency, which is enshrined in Article 5 (1) (a) GDPR, which is similar to and can be used to interpret Article 8 of the Charter.[86] Fairness is thus strongly connected with transparency.[87] This link comes into play in the balancing of asymmetrical relationships regarding data processing.[88] In order to comply with the principle of fairness in a transparent manner, information must be provided in simple and understandable language.[89] Furthermore, data subjects must be informed about risks and safeguards in relation to the data processing and the exercise of their rights.[90] In essence, the principle of fairness is thus also closely interwoven with the right to be informed as described in Chapter IV. 3. a).[91] This is conclusive, as fair data processing can only take place *vis-à-vis* an informed data subject who has full clarity about the data processing activities and his or her own rights.[92]

---

para. 127; T. Riesz, 'Art 8 GRC. Schutz personenbezogener Daten' (*supra* Chapter VI. note 27), para. 135 who refers to Case C-201/14 *Bara* (*supra* Chapter II. note 53), para. 34; H. Johlen, 'Art. 8 Schutz personenbezogener Daten' (*supra* Chapter VII. note 1), para. 48.

[82] W. Hötzendorfer, C. Tschohl and M. Kastelitz, 'Art 5 DSGVO. Grundsätze für die Verarbeitung personenbezogener Daten' in R. Knyrim (ed.), *Der DatKomm* (Manz, 2022), para. 17; T. Riesz, 'Art 8 GRC. Schutz personenbezogener Daten' (*supra* Chapter VI. note 27), note 344.

[83] Case C-61/19 *Orange Romania*, EU:C:2020:901, para. 48; H. Kranenborg, 'Art 8 Protection of Personal Data' (*supra* Chapter VII. note 14), para. 135.

[84] Case C-201/14 *Bara* (*supra* Chapter II. note 53), para. 32.

[85] T. Riesz, 'Art 8 GRC. Schutz personenbezogener Daten' (*supra* Chapter VI. note 27), para. 63.

[86] D. Clifford and J. Ausloos, 'Data Protection and the Role of Fairness' (*supra* Chapter VII. note 77), p. 134; T. Riesz, 'Art 8 GRC. Schutz personenbezogener Daten' (*supra* Chapter VI. note 27), para. 63; H.D. Jarass, 'Art. 8 Schutz personenbezogener Daten' (*supra* Chapter VI. note 64), para. 13.

[87] D. Clifford and J. Ausloos, 'Data Protection and the Role of Fairness' (*supra* Chapter VII. note 77), p. 138; H. Johlen, 'Art. 8 Schutz personenbezogener Daten' (*supra* Chapter VII. note 1), para. 49.

[88] Ibid, p. 139.

[89] See Recital 39 GDPR.

[90] Ibid.

[91] D. Clifford and J. Ausloos, 'Data Protection and the Role of Fairness' (*supra* Chapter VII. note 77), p. 140.

[92] H. Kranenborg, 'Art 8 Protection of Personal Data' (*supra* Chapter VII. note 14), para. 161.

Clifford/Ausloos emphasise that there is also an implicit fairness that stems from protection against asymmetric relationship and results in 'fair balancing'.[93] To achieve 'fair balance', data processing must be necessary and proportionate.[94] Here, ex ante balancing mechanisms, i.e. the reasons for lawful data processing, and ex post balancing mechanisms, i.e. the protection of data subjects' rights, play an important role.[95] These 'fair balancing' mechanisms are needed to meet the proportionality and necessity requirements of Article 52 (1) of the Charter, as described in Chapter VIII. 1. e).[96] These 'fair balancing' mechanisms in the context of personal data as an economic asset will be analysed in more detail in Chapter VIII. 2. below.

From all this, it can be deduced that the use of personal data as an economic asset, in order to comply with the explicit principle of fairness of Article 8 (2) of the Charter, must fulfil two conditions: First, the economic use of personal data must be clear, transparent and comprehensible to data subjects. Second, data subjects must be fully informed about the economic use of personal data in all its forms. This includes information about the risks involved in the commercial use of personal data, about the sharing with third parties and about the rights of data subjects.

Recalling the example of Experian from Chapter III. 2. b), the ICO has rightly decided that Experian violated the principle of transparency because personal data was traded and augmented without the awareness of the data subject and without them expecting it ('invisible' processing). As the data subjects were not aware and informed, and personal data was processed 'invisibly', i.e. in a non-transparent manner, the principle of fairness set out in Article 8 (2) of the Charter was also violated in this example.

The same can be stated about the exploitation of personal data in the wake of the *Cambridge Analytica scandal*. Facebook indicates in its data policy that data is shared with third parties, in particular advertisers, and personal data identifying an individual is only shared if the data subject consents to this.[97] It is questionable whether this reference is sufficient to comply with the principle of fairness. In view of the data subject-friendly case law of the CJEU, this is probably not the case. Whether and how consent meets the requirements of Article 8 (2) of the Charter is examined in Chapter VII. 4. a) below.

---

[93] D. Clifford and J. Ausloos, 'Data Protection and the Role of Fairness' (*supra* Chapter VII. note 77), p. 141.

[94] Ibid, p. 181.

[95] Ibid, p. 179.

[96] Ibid.

[97] Facebook, *Privacy Policy*, 3 November 2023, https://en-gb.facebook.com/policy.php (accessed 31 January 2024).

b) Processing personal data for specified purposes

Moreover, according to Article 8 (2) of the Charter, data processing may only be carried out for specified purposes. Here too, the GDPR can be used as an aid to interpretation. The purpose of processing must be clearly defined before processing.[98] In addition, the purpose must be explicit and legitimate.[99] An illegal purpose is therefore not compatible with Article 8 (2) of the Charter. The purpose must be narrowly defined so that it does not also cover uses which no longer constitute a legitimate purpose of the original data collection.[100] In this sense, personal data should be relevant to the purpose, limited to what is necessary for the purpose for which they are processed and the duration of the storage of the personal data should be minimised.[101] Therefore, the purpose determines the entire data processing operation.[102] Consequently, the purpose of the data processing activities determines the accuracy, timeliness and completeness of the personal data concerned as well as the duration of storage.[103] Purpose limitation restricts the possibilities of processing personal data.[104]

These requirements are also expressed in the GDPR as principles of purpose limitation and data minimisation.[105] Privacy enhancing technologies, e.g. cryptographic protocols, can be used to ensure data minimisation and data subject control over personal data.[106] Purpose limitation is an expression of the requirement of predictability of interferences with fundamental rights.[107] The purpose also determines the data processing principles, the grounds for data processing, the rights of the data subjects and legal consequences.[108] If the economic use of personal data is specified as the purpose, this has numerous implications under data protection law.

---

[98] See Recital 39 GDPR; T. Riesz, 'Art 8 GRC. Schutz personenbezogener Daten' (*supra* Chapter VI. note 27), para. 63.

[99] See Recital 39 GDPR.

[100] T. Riesz, 'Art 8 GRC. Schutz personenbezogener Daten' (*supra* Chapter VI. note 27), para. 63.

[101] See Recital 39 GDPR.

[102] U. Spies, 'Zweckfestlegung der Datenverarbeitung durch den Verantwortlichen', 12 *ZD – Zeitschrift für Datenschutz* (2022), p. 80.

[103] H. Johlen, 'Art. 8 Schutz personenbezogener Daten' (*supra* Chapter VII. note 1), para. 50.

[104] T. Riesz, 'Art 8 GRC. Schutz personenbezogener Daten' (*supra* Chapter VI. note 27), para. 63.

[105] See Article 5 (1) (b) and (c).

[106] C. Lazaro and D. Le Métayer, 'Control over Personal Data: True Remedy or Fairy Tale?' (*supra* Chapter I. note 15), p. 26.

[107] T. Riesz, 'Art 8 GRC. Schutz personenbezogener Daten' (*supra* Chapter VI. note 27), para. 63.

[108] M. von Grafenstein, 'Refining the Concept of the Right to Data Protection in Article 8 ECFR – Part I' (*supra* Chapter VII. note 2), p. 513.

The facilitations of the GDPR, through which data can also be processed for a purpose other than the one originally specified when the data was collected, are not unproblematic with regard to Article 8 (2) of the Charter.[109] Among other factors, the expectations of the data subject and the impact of the changed purpose must be taken into account.[110] Thus, processing health data for commercial purposes not directly related to the health service and original purpose is not a legitimate change of purpose.[111]

The CJEU has ruled that the processing of working time records may be a sufficient purpose because of the necessity to comply with a legal obligation.[112] The purpose of processing fingerprints must also be proportionate.[113] The Court held that the use and storage of biometric personal data for the purpose of verifying the authenticity of the document or the identity of the holder is compatible with Articles 7 and 8 of the Charter.[114] Similarly, the processing of financial data is a legitimate purpose for combating tax evasion if the processing is appropriate and necessary.[115] The requirement of the necessity and proportionality of the data processing for the purpose pursued has also been emphasised by the CJEU in further judgments.[116] Two points can be made on the basis of these judgments: First, the processing of personal data is not in itself unlawful, provided that certain conditions are met. Second, the data processing must be necessary and proportionate to achieve the purpose. These conditions are reminiscent of those of Article 52 (1) of the Charter, as described in Chapter VIII. 1.

The question is therefore whether the economic use of personal data can be a specified purpose. First of all, it should be noted that the economic use of personal data can be a legitimate purpose and is not excluded in principle. Otherwise, the entire data economy would be illegitimate in its purpose and the steps taken by the EU, as described in Chapter V., would be pointless. This is not the case. Nevertheless, the processing of personal data can only have economic exploitation as a purpose under certain conditions. For personal data to be used as an economic asset, the purpose of the data processing (i.e. economic exploitation) must be explicitly disclosed before the personal data is collected, must be limited to the purpose and it must be limited in time. It must be legitimate, proportionate

---

[109] See Article 6 (4) GDPR; T. Riesz, 'Art 8 GRC. Schutz personenbezogener Daten' (*supra* Chapter VI. note 27), para. 63.

[110] Article 29 Working Party opinion 03/2013 on purpose limitation, 2 April 2013 ('WP203'), p. 23.

[111] Ibid, p. 58.

[112] Case C–342/12 *Worten* (*supra* Chapter II. note 56), para. 35.

[113] Case C–291/12 *Schwarz* (*supra* Chapter II. note 131), para. 58.

[114] Case C–446/12 *Willems and Others* (*supra* Chapter VI. note 174), para. 46.

[115] Case C–73/16 *Puškár*, EU:C:2017:725, para. 117.

[116] Case C-708/18 *Asociatia de Proprietari bloc M5A-ScaraA* (*supra* Chapter VI. note 174), paras. 46 and 47; Case C-439/19 *Latvijas Republikas Saeima*, EU:C:2021:504, para. 110; Case C-184/20 *Vyriausioji tarnybinės etikos komisija* (*supra* Chapter IV. note 295), para. 85; Case C-205/21 *Ministerstvo na vatreshnite raboti*, EU:C:2023:49, para. 126.

and necessary. Subsequently, it is unsurprising that the use of personal data as an economic asset in the black market, as described in Chapter III. 4., violates Article 8 of the Charter, as black markets are illegal in themselves and thus their purpose. Offering data of persons who have been victims of rape, as described in Chapter III. 3., is also not a legitimate purpose, even if the purpose would have been explicitly stated before data collection.

The context determines how purposes are specified, e.g. Facebook, which operates across the world, needs to keep in mind its international users with different cultures.[117] Furthermore, purposes such as 'improving users' experience', 'marketing', 'IT-security' or 'future research' are too ambiguous and too vague.[118] In this sense, the specified purposes by Facebook might be too general when referring to the use of personal data to 'provide, personalise and improve our products', to promote 'safety, integrity and security' and to 'provide information and content to research partners and academics', among others.[119] The same is arguably the case with Amazon's privacy notice.[120]

Admittedly, it is a balancing act to fulfil the requirements of Article 8 (2) of the Charter, on the one hand the data processing and its purpose must be indicated clearly and in simple language, thus not too detailed and extensive, on the other hand this indication must not be too vague and general, thus adapted to the target group. It therefore boils down, as so often, to a case-by-case decision as to whether personal data as an economic asset are actually processed fairly, i.e. clearly, transparently and comprehensibly with fully informed data subjects, and for a specified purpose, i.e. legitimate, proportionate and necessary.

4. Consent to the use of personal data as an economic asset

If personal data as an economic asset are processed fairly and for a specified purpose and, in addition, the consent of the data subject has been obtained, the requirements of Article 8 (2) of the Charter are met. The key role of consent in data processing is evident from its explicit mention in Article 8 (2) of the Charter.[121] Valid consent excludes interference with the fundamental right to data protection under Article 8 of the Charter.[122] Consequently, valid consent to the

[117] WP203 (*supra* Chapter VII. note 110), p. 52.

[118] Ibid.

[119] See Facebook, *Data Policy*, 4 January 2022.

[120] See Amazon, *Privacy Notice*, 11 August 2023, https://www.amazon.com/gp/help/customer/display.html?nodeId=GX7NJQ4ZB8MHFRNJ (accessed 31 January 2024).

[121] A. Ingold, 'Artikel 7 Bedingungen für die Einwilligung' (*supra* Chapter V. note 65), para. 9; Y. McDermott, 'Conceptualising the right to data protection in an era of Big Data' (*supra* Chapter IV. note 193), p. 3.

[122] H.D. Jarass, 'Art. 8 Schutz personenbezogener Daten' (*supra* Chapter VI. note 64), para. 9; A. Ingold, 'Artikel 7 Bedingungen für die Einwilligung' (*supra* Chapter V. note 65), para. 9; T. Kingreen, 'Art. 8 GRCh' (*supra* Chapter VII. note 28), para. 14; T. Riesz, 'Art 8 GRC. Schutz personenbezogener Daten' (*supra* Chapter VI. note 27), para. 69.

use of personal data as an economic asset precludes interference with the fundamental right to data protection. The central legal consequence of valid consent is thus the lawful processing and use of personal data as an economic asset in accordance with Article 8 of the Charter.[123]

The advantages of consent are that the decision is entirely up to the data subjects whether or not to allow the processing of their personal data.[124] By means of consent, the data subject exploits his or her personal data, as he or she consents to the processing of his or her personal data in exchange for receiving, for example, 'free' online services.[125] Furthermore, compared to 'any other legitimate basis laid down by law', obtaining consent creates transparency for the data subject and does not require a balancing test by the data controller, as is the case with legitimate interest, for example (see Chapter VII. 5. b) below).[126] In fact, in many constellations where personal data are used as an economic asset, consent might be the only reliable and practicable legitimate basis for data processing, thus ensuring compatibility with the Charter.[127] This is also emphasised by the CJEU when it ruled that justifications for the processing of personal data in the absence of the data subject's consent must be interpreted restrictively.[128]

Consent is the central form of expression of informational self-determination.[129] Consent gives data subjects control over the risks to their personal data.[130]

---

[123] See regarding the central consequence of valid consent in general, A. Ingold, 'Artikel 7 Bedingungen für die Einwilligung' (*supra* Chapter V. note 65), para. 50; See C. Langhanke, *Daten als Leistung – Eine rechtsvergleichende Untersuchung zu Deutschland, Österreich und der Schweiz* (*supra* Chapter I. note 10), pp. 104, 108, who opts for the mandatory necessity of consent to authorise data processing in the context of paying with data.

[124] D. Jahnel, 'Art 6 Rechtmäßigkeit der Verarbeitung' in D. Jahnel (ed.), *DSGVO Datenschutz-Grundverordnung*, para. 12; see also A. P. Karanasiou and E. Douilhet, 'Never Mind the Data: The Legal Quest over Control of Information & the Networked Self', *IEEE International Conference on Cloud Engineering Workshop (IC2EW)* (2016), p. 102.

[125] B. Buchner, 'Die Einwilligung im Datenschutzrecht – vom Rechtfertigungsgrund zum Kommerzialisierungsinstrument', 34 *DuD – Datenschutz und Datensicherheit* (2010), p. 39.

[126] D. Jahnel, 'Art 6 Rechtmäßigkeit der Verarbeitung' (*supra* Chapter VII. note 124), para. 19.

[127] See also B. Buchner, 'Die Einwilligung im Datenschutzrecht – vom Rechtfertigungsgrund zum Kommerzialisierungsinstrument' (*supra* Chapter VII. note 125), p. 40; F. Zuiderveen Borgesius, 'Legal basis for behavioural targeting' (*supra* Chapter VII. note 76), p. 172.

[128] Case C-252/21 *Meta Platforms and Others*, EU:C:2023:537, para. 93.

[129] Datenethikkommission, *Gutachten der Datenethikkommission*, p. 96; H. Johlen, 'Art. 8 Schutz personenbezogener Daten' (*supra* Chapter VII. note 1), para. 51; N. Bernsdorff, 'Artikel 8 Schutz personenbezogener Daten' (*supra* Chapter VII. note 1), para. 28; D. Jahnel, 'Art 6 Rechtmäßigkeit der Verarbeitung' (*supra* Chapter VII. note 124), para. 12; A. Ingold, 'Artikel 7 Bedingungen für die Einwilligung' (*supra* Chapter V. note 65), para. 10; D. Jahnel, 'Art 4 Z 11 Einwilligung' in D. Jahnel (ed.), *DSGVO Datenschutz-Grundverordnung*, para. 2.

[130] M. von Grafenstein, 'Refining the Concept of the Right to Data Protection in Article 8 ECFR – Part II' (*supra* Chapter VII. note 31), p. 201; C. Langhanke, *Daten als Leistung – Eine rechtsvergleichende Untersuchung zu Deutschland, Österreich und der Schweiz* (*supra* Chapter I. note 10), p. 103.

Thus, if data subjects themselves decide to use their personal data as an economic asset, they are expressing their self-determination and private autonomy. This informational self-determination, which is entrenched in the right to data protection, should only be restricted or prohibited in a few cases.[131] *Berndorff* refers to informational self-determination as the cornerstone of the right to data protection.[132] Consequently, it is inconclusive to want to prohibit the economic use of personal data from the outset. By consenting to the use of personal data as an economic asset, it is not the fundamental right to data protection that is waived, but the fundamental right to data protection that is exercised.[133]

Of course, the law as such does not recognise any unrestricted right of self-determination, e.g. unrestrained right to self-injury.[134] However, also in this respect a tendency towards self-determination can be seen in some Member States (e.g. 'right to die').[135] Similarly, not every use of personal data can be consented to: For this purpose, the provision of fair processing for a specified purpose exists, meaning that if this principle is infringed, even if the data subject consents, the fundamental right to data protection is infringed. Furthermore, the essence of the right to data protection must be respected. Apart from that, however, data subjects are free to decide whether to consent to the use of personal data as an economic asset. Consent must meet certain conditions, which will be analysed in the following.

a) General requirements for consent

For the interpretation of consent within the meaning of Article 8 (2) of the Charter, Article 4 (11) GDPR can be consulted. Compared to the DPD, the consent requirements have been strengthened and clarified.[136] The high standards for consent are required by the scope of protection under Article 8 of the Charter.[137] The requirements for consent help to ensure that the autonomy of those giving consent is secured.[138] The GDPR states that

---

[131] Datenethikkommission, *Gutachten der Datenethikkommission*, p. 96.

[132] N. Bernsdorff, 'Artikel 8 Schutz personenbezogener Daten' (*supra* Chapter VII. note 1), para. 28.

[133] See also A. Ingold, 'Artikel 7 Bedingungen für die Einwilligung' (*supra* Chapter V. note 65), para. 10.

[134] N. Bernsdorff, 'Artikel 8 Schutz personenbezogener Daten' (*supra* Chapter VII. note 1), para. 28.

[135] BVerfG, 26.02.2020, 2 BvR 2347/15, DE:BVerfG:2020:rs20200226.2bvr234715; VfGH, 11.12.2020, G 139/2019–71, AT:VFGH:2020:G139.2019; Corte Costituzionale, 22.11.2019, 242/2019.

[136] H. Kranenborg, 'Art 8 Protection of Personal Data' (*supra* Chapter VII. note 14), para. 148.

[137] A. Ingold, 'Artikel 7 Bedingungen für die Einwilligung' (*supra* Chapter V. note 65), para. 15.

[138] Ibid, para. 2.

'consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;'[139]

In general, consent must be given prior to data processing, i.e. consent cannot be given to an already existing commercial use of personal data.[140] How long consent is valid depends on the scope and context of the data processing activities and the expectations of the data subject.[141] The requirement for consent to be 'freely' given means that data subjects have genuine freedom and power over it.[142] There must therefore be no coercion when giving consent.[143] Logically, the provision of consent to the economic use of personal data must not be coerced by physical or verbal force.[144] If there is an imbalance of power between the data subject and the controller, consent is not considered 'freely' given, especially if the controller is a public authority.[145] For example, the processing of fingerprints from passports cannot be based on consent, as data subjects are not free to object to the processing when applying for a passport.[146] An imbalance of power is not limited to public authorities, but can also occur in employment or in other situations, so that data subjects have no genuine alternative – without experiencing negative consequences – but to consent.[147] It follows that employees can only give their consent if they do not have to face any negative consequences.[148]

Furthermore, consideration must be given to whether the performance of a service or contract depends on consent to data processing which is not necessary for the performance.[149] In such a case, consent is deemed not to have been freely given.[150] This is intended to cover 'take it or leave it'-constellations in which one does not have to agree to data processing, but if one does not give consent, one cannot, for example, become a member of a social network.[151] Another example

---

[139] See Article 4 (11) GDPR.

[140] A. Ingold, 'Artikel 7 Bedingungen für die Einwilligung' (*supra* Chapter V. note 65), para. 17.

[141] D. Jahnel, 'Art 7 Bedingungen für die Einwilligung' in D. Jahnel (ed.), *DSGVO Datenschutz Grundverordnung*, para. 7.

[142] EDPB, *Guidelines 05/2020 on consent under Regulation 2016/679*, 13 May 2020, p. 7; Recital 42 GDPR; D. Jahnel, 'Art 4 Z 11 Einwilligung' (*supra* Chapter VII. note 129), para. 6.

[143] F. Zuiderveen Borgesius, 'Legal basis for behavioural targeting' (*supra* Chapter VII. note 76), p. 171; A. Ingold, 'Artikel 7 Bedingungen für die Einwilligung' (*supra* Chapter V. note 65), para. 26.

[144] Ibid, para. 27; Elliott calls this 'undue influence', see D. Elliott, 'Data Protection Is More Than Privacy', 5 *European Data Protection Law Review* (2019), p. 15.

[145] Recital 43 GDPR.

[146] Case C-291/12 *Schwarz* (*supra* Chapter II. note 131), para. 32.

[147] EDPB, *Guidelines 05/2020* (*supra* Chapter VII. note 142), p. 9.

[148] D. Jahnel, 'Art 4 Z 11 Einwilligung' (*supra* Chapter VII. note 129), para. 9.

[149] See Article 7 (4) GDPR.

[150] See Recital 43 GDPR.

[151] B. Buchner, 'Die Einwilligung im Datenschutzrecht – vom Rechtfertigungsgrund zum Kommerzialisierungsinstrument' (*supra* Chapter VII. note 125), p. 41.

would be a roller coaster, where, if one does not consent to being photographed by a camera during the ride, one would not be able to use the ride.[152] The EDPB argues that if online behavioural advertising is not necessary for the provision of an app, but the app cannot be used without consent to online behavioural advertising, consent has not been freely given.[153] The same applies to cookie walls, i.e. consent to cookies in order to be able to use a homepage, according to the EDPB.[154] This is significant in cases where personal data is given as consideration for a gratuitous service.[155]

However, the autonomy of data subjects is secured in cases where there is a reasonable alternative means of access without requiring consent.[156] *Jahnel* uses the term 'track or pay' or 'pay or okay' solutions in this context.[157] In the online world, data subjects have the freedom to decide whether they want to use 'free', innovative and widely used services while possibly sacrificing privacy, or whether they would prefer to switch to more privacy-friendly services instead, even if these may be subject to a fee, less innovative or less popular.[158] This is also the case with Facebook, as one can still have a normal social life without being part of this social network.[159] Compulsory consent to the provision of a service only becomes a problem when data subjects are actually dependent on a certain service.[160]

Another requirement for valid consent to be 'freely given' is that it has to be given separately for different data processing operations.[161] If a data processing activity has several purposes, the data subject must have the choice to give consent separately.[162] For example, consent to data processing for marketing purposes must be separate from others and clearly separated from the signature to sign up for a membership.[163] In addition, not only in cases of power imbalance, but in all data processing operations, data subjects must be able to refuse or

---

[152] D. Jahnel, 'Art 7 Bedingungen für die Einwilligung' (*supra* Chapter VII. note 141), para. 25 who refers to DSB, 16.04.2019, DSB-D213.679/0003-DSB/2018, AT:DSB:2019:DSB.D213.679.0003.DSB.2018.

[153] EDPB, *Guidelines 05/2020* (*supra* Chapter VII. note 142), p. 8.

[154] Ibid, p. 12.

[155] A. Ingold, 'Artikel 7 Bedingungen für die Einwilligung' (*supra* Chapter V. note 65), para. 33.

[156] Ibid.

[157] D. Jahnel, 'Art 7 Bedingungen für die Einwilligung' (*supra* Chapter VII. note 141), para. 26.

[158] B. Buchner, 'Die Einwilligung im Datenschutzrecht – vom Rechtfertigungsgrund zum Kommerzialisierungsinstrument' (*supra* Chapter VII. note 125), p. 41.

[159] Ibid.

[160] Ibid.

[161] See Recital 43 GDPR.

[162] See Recital 32 GDPR.

[163] D. Jahnel, 'Art 7 Bedingungen für die Einwilligung' (*supra* Chapter VII. note 141), para. 14 who refers to DSB, 31.07.2018, DSB-D213.642/0002-DSB/2018, AT:DSB:2018:DSB.D213.642.0002.DSB.2018.

withdraw consent without suffering disadvantages.[164] In order to grant genuine freedom of choice and thus freely given consent, data subjects must not be misled about the possibility of concluding a contract, even if the processing of personal data is refused.[165]

In respect of the economic exploitation of personal data, this implies that data subjects must have the freedom to choose whether to consent to or refuse the economic use of their personal data. With Facebook, for example, one cannot refuse the economic use of personal data. Its Terms of Service state that personal data are processed in order to provide and fund the service.[166] This is misleading, especially since the sharing of personal data with third parties and the economic exploitation are hardly necessary to provide a social network. Even if the operation of a social network would not be possible without the economic use of personal data, due to funding issues, a version for which one has to pay with money, where no personal data is economically exploited and no personalised ads are shown, could be offered as an alternative.[167] In this case, people could choose to pay with money for a version that does not economically exploit personal data or use a version without paying with money but 'paying' with personal data.

In this sense, the Austrian data protection authority has ruled that a not disproportionately expensive paid version without economic exploitation of personal data is a real alternative to the version with data processing and thus consent to data processing was freely given.[168] In this case, the version without economic exploitation of personal data cost € 6 per month.[169] How much a proportionate fee-based alternative costs in other constellations depends on the individual case. The calculation methods of the value of personal data in Chapter III. could be used for this purpose. With such alternatives, funding issues would be resolved. It would also make it clear to people how much their personal data is worth. A subscription-based social network called 'HalloApp', which does not rely on online advertising and the economic use of personal data, was launched by former Facebook employees, for example.[170]

Thus, to meet the requirement of 'freely given' consent, data subjects must have a genuine free choice to consent, consent must in general not be compulsory for a service or a contract, and it must be possible to give consent separately for different data processing operations.

---

[164] See Recital 42 GPDR.

[165] Case C-61/19 *Orange Romania* (*supra* Chapter VII. note 83), para. 41.

[166] Facebook, *Terms of Service*, 12 January 2024, https://www.facebook.com/terms.php (accessed 31 January 2024).

[167] See also B. Custers and G. Malgieri, 'Priceless data: why the EU fundamental right to data protection is at odds with trade in personal data' (*supra* Chapter I. note 11), p. 38.

[168] DSB, 30.11.2018, DSB-D122.931/0003-DSB/2018, AT:DSB:2018: DSB.D122.931.0003.DSB.2018.

[169] Ibid.

[170] D. Seetharaman, 'Former Facebook, WhatsApp Employees Lead New Push to Fix Social Media' (*supra* Chapter III. note 92).

Another requirement for consent is that it must be 'specific'. The content of the consent and the modalities of the declaration of consent must be specific.[171] Article 6 (1) (a) of the GDPR states that consent must be given for one or more specific purposes. Thus, no blanket consent can be given for future changes in the purpose of the data processing operations.[172] This is intended to give data subjects transparency and control over their personal data.[173] Hence, there must be a purpose limitation to prevent function creep after the data subjects have consented to the original purpose of the data processing.[174] This is a reiteration of the purpose limitation of Article 8 (2) of the Charter, which must be complied with regardless of the ground for data processing, as described in Chapter VII. 3. b) above. Furthermore, it must be possible to give separate consent for each purpose in order to give both free and specific consent.[175] Specific consent refers to specific personal data and specific processing purposes.[176] As to what specific consent means for personal data as an economic asset, readers may refer to the examples given in Chapter VII. 3. b) on the specified purpose. Due to the similarity of the requirements, 'specific' consent and examples will not be discussed further in this chapter.

Consent must also be 'informed'. Data subjects must be informed about all matters relevant to the granting of consent.[177] Valid consent requires information provided by the data controller prior to consent given by the data subjects.[178] Data subjects must at least be aware of the purposes of the data processing and the identity of the controller for consent to be 'informed'.[179] In addition, the EDPB also requests that information on what data is collected and used, the right to withdraw consent, automated decision-making where relevant and the risks of data transfers is provided.[180] The CJEU held that information must be provided in

---

[171] A. Ingold, 'Artikel 7 Bedingungen für die Einwilligung' (*supra* Chapter V. note 65), para. 37.

[172] H. Johlen, 'Art. 8 Schutz personenbezogener Daten'(*supra* Chapter VII. note 1), para. 53; A. Ingold, 'Artikel 7 Bedingungen für die Einwilligung' (*supra* Chapter V. note 65), para. 39; D. Jahnel, 'Art 4 Z 11 Einwilligung' (*supra* Chapter VII. note 129), para. 11.

[173] EDPB, *Guidelines 05/2020* (*supra* Chapter VII. note 142), p. 14.

[174] Ibid.

[175] Ibid.

[176] P. Reimer, 'Artikel 6 Rechtmäßigkeit der Verarbeitung' in G. Sydow (ed.), *Europäische Datenschutzgrundverordnung*, para. 16.

[177] H. Johlen, 'Art. 8 Schutz personenbezogener Daten' (*supra* Chapter VII. note 1), para. 52.

[178] A. Ingold, 'Artikel 7 Bedingungen für die Einwilligung' (*supra* Chapter V. note 65), para. 35.

[179] See Recital 42 GDPR.

[180] EDPB, *Guidelines 05/2020* (*supra* Chapter VII. note 142), p. 15.

'an intelligible and easily accessible form, using clear and plain language, allowing the data subject to be aware of, inter alia, the type of data to be processed, the identity of the controller, the period and procedures for that processing and the purposes of the processing'.[181]

This information should enable data subjects to assess the consequences of their consent.[182] This is not the case if the information is incomprehensible or has to be searched for in different places within a document or even in different documents.[183] The information must also not be full of legal jargon and technicalities.[184] Often, however, privacy policies are uninformative, confusing and overwhelming.[185] Facebook's privacy policy, for example, is 12,000 words.[186] Depending on the target group, data controllers must decide what information to provide and how to provide it.[187] Moreover, a pre-ticked checkbox on a website does not constitute informed consent.[188] This is due to the fact that in most cases users of a website do not read information relating to a pre-ticked checkbox and continue visiting the website uninformed.[189]

When using unverified lists acquired from third parties, a company should provide the user with an informative notice, explaining the origin of the personal data and – only after obtaining consent – proceed with the economic exploitation of the personal data.[190] This has significance for those companies that receive lists of customers from third parties in order to place personalised advertisements, as examined in Chapter III. 2.

In many cases, consent is not an expression of a self-determined and informed decision about the economic use of personal data precisely because data subjects are not made aware of the details of consent at all and thus no transparent decision can be made.[191] Companies that use personal data as an economic asset present their services as 'free of charge', although in fact it is a contract in the

---

[181] Case C-61/19 *Orange Romania* (*supra* Chapter VII. note 83), para. 40.

[182] Ibid; Case C-673/17 *Planet49* (*supra* Chapter II. note 133), para. 74.

[183] D. Jahnel, 'Art 4 Z 11 Einwilligung' (*supra* Chapter VII. note 129), para. 10.

[184] D. Jahnel, 'Art 7 Bedingungen für die Einwilligung' (*supra* Chapter VII. note 141), para. 10.

[185] G. A. Fowler, 'I tried to read all my app privacy policies. It was 1 million words.', *The Washington Post* (2022), https://www.washingtonpost.com/technology/2022/05/31/abolish-privacy-policies/ (accessed 31 January 2024).

[186] Ibid.

[187] EDPB, *Guidelines 05/2020* (*supra* Chapter VII. note 142), p. 17.

[188] See Recital 32 GDPR; Case C-61/19 *Orange Romania* (*supra* Chapter VII. note 83), para. 37; Case C-673/17 *Planet49* (*supra* Chapter II. note 133), para. 55.

[189] Case C-61/19 *Orange Romania* (*supra* Chapter VII. note 83), para. 37; Case C-673/17 *Planet49* (*supra* Chapter II. note 133), para. 55; see also D. Elliott, 'Data Protection Is More Than Privacy' (*supra* Chapter VII. note 144), p. 15.

[190] See GPDP, 16.09.2021, 9706389.

[191] B. Buchner, 'Die Einwilligung im Datenschutzrecht – vom Rechtfertigungsgrund zum Kommerzialisierungsinstrument' (*supra* Chapter VII. note 125), p. 41.

form of an exchange of consent for service.[192] In order to meet the requirements of informed consent, companies must therefore clearly indicate that they intend to use personal data as an economic asset.[193] This puts the data subjects in the position of balancing advantages, e.g. 'free' service, with disadvantages, e.g. large-scale, intrusive data processing and disclosure to third parties.[194]

Furthermore, consent must be given by a 'clear affirmative act'.[195] It thus requires an active declaration or motion that makes it clear that the data subject has consented to the data processing.[196] The data controller should thereby be able to prove that consent was given to the data processing.[197] The burden of proof therefore lies with the data controller.[198] This unambiguous consent can be given in writing, electronically or orally.[199] The request for written consent to data processing should be clearly separated from other written concerns.[200] This includes the active ticking of a box.[201] In contrast, inactivity, silence or pre-ticked boxes do not constitute valid consent.[202]

In this sense, the CJEU has held that pre-ticked boxes do not constitute valid consent and that there must always be active behaviour on the part of the data subject in terms of consent.[203] This makes an opt-in model acceptable, whereas an opt-out model does not allow enable valid consent.[204] In the online world, the 'double-opt-in' method can be used to provide proof of consent.[205] After consent has been given on a website, an e-mail is sent to the address given, which contains a confirmation link that must be actively clicked before the personal data can be processed and possibly used as an economic asset.[206] This means that data subjects must actively consent to the economic exploitation of their personal data and data controllers must be able to prove that consent has been given. This opt-in model is an important step towards more transparency and towards creat-

---

[192] Ibid.

[193] See also, F. Zuiderveen Borgesius, 'Legal basis for behavioural targeting' (*supra* Chapter VII. note 76), p. 171.

[194] M. von Grafenstein, 'Refining the Concept of the Right to Data Protection in Article 8 ECFR – Part III' (*supra* Chapter VI. note 192), p. 387.

[195] See Recital 32 GDPR.

[196] EDPB, *Guidelines 05/2020* (*supra* Chapter VII. note 142), p. 18; F. Zuiderveen Borgesius, 'Legal basis for behavioural targeting' (*supra* Chapter VII. note 76), p. 171.

[197] See Article 7 (1) GDPR.

[198] EDPB, *Guidelines 05/2020* (*supra* Chapter VII. note 142), p. 22.

[199] See Recital 32 GDPR.

[200] See Article 7 (2) GDPR.

[201] Ibid.

[202] Ibid.

[203] Case C-673/17 *Planet49* (*supra* Chapter II. note 133), para. 52; Case C-61/19 *Orange Romania* (*supra* Chapter VII. note 83), para. 37.

[204] D. Jahnel, 'Art 4 Z 11 Einwilligung' (*supra* Chapter VII. note 129), para. 4.

[205] D. Jahnel, 'Art 7 Bedingungen für die Einwilligung' (*supra* Chapter VII. note 141), para. 6.

[206] Ibid.

ing more awareness for data subjects when it comes to the economic use of personal data.[207]

Another requirement is that consent can be withdrawn at any time.[208] Withdrawal of consent must be distinguished from the right to object, as the latter articulates the disapproval of data processing without consent.[209] Withdrawal of consent should be simple.[210] For example, if consent was given by mouse click, it should also be possible to withdraw it by mouse click.[211] The right to withdraw consent cannot be waived and the withdrawal itself does not require any justification by the data subject.[212] The withdrawal of consent does not jeopardise the lawfulness of the data processing up to that point.[213] However, another legal ground must exist for the data processing after the withdrawal, otherwise the data processing must be stopped and the personal data must be erased.[214] As stated above, the possibility of withdrawal must be disclosed before consent is given.[215] The possibility of withdrawing consent is, like consent itself, a manifestation of informational self-determination.[216] Withdrawing consent to the use of personal data as an economic asset is thus an expression of the fundamental right to data protection as set out in Article 8 of the Charter.

In summary, consent to the use of personal data as an economic asset must meet five requirements in order to exclude interference with the fundamental right to data protection under Article 8 of the Charter: (i) consent (freely given, specific, informed, unambiguous), (ii) in the form of a statement or unambiguous affirmative act, (iii) indication by the data controller of the right to withdraw consent, (iv) intelligible, easily accessible, clear and simple language, as well as distinction of the different data processing purposes, and (v) consideration that

---

[207] B. Buchner, 'Die Einwilligung im Datenschutzrecht – vom Rechtfertigungsgrund zum Kommerzialisierungsinstrument' (*supra* Chapter VII. note 125), p. 42.

[208] See Article 7(3) GDPR; Schwartz already argued for a 'right to exit' in 2004, P.M. Schwartz, 'Property, Privacy, and Personal Data' (*supra* Chapter I. note 14), p. 2106.

[209] A. Ingold, 'Artikel 7 Bedingungen für die Einwilligung' (*supra* Chapter V. note 65), para. 45.

[210] See Article 7(3) GDPR.

[211] EDPB, *Guidelines 05/2020* (*supra* Chapter VII. note 142), p. 23; A. Ingold, 'Artikel 7 Bedingungen für die Einwilligung' (*supra* Chapter V. note 65), para. 48.

[212] D. Jahnel, 'Art 7 Bedingungen für die Einwilligung' (*supra* Chapter VII. note 141), para. 17.

[213] See Article 7 (3) GDPR; P. Reimer, 'Artikel 6 Rechtmäßigkeit der Verarbeitung' (*supra* Chapter VII. note 176), para. 16; D. Jahnel, 'Art 7 Bedingungen für die Einwilligung' (*supra* Chapter VII. note 141), para. 17.

[214] H. Kranenborg, 'Art 8 Protection of Personal Data' (*supra* Chapter VII. note 14), para. 149; P. Reimer, 'Artikel 6 Rechtmäßigkeit der Verarbeitung' (*supra* Chapter VII. note 176), para. 16; D. Jahnel, 'Art 7 Bedingungen für die Einwilligung' (*supra* Chapter VII. note 141), para. 21.

[215] See Article 7 (3) GDPR.

[216] A. Ingold, 'Artikel 7 Bedingungen für die Einwilligung' (*supra* Chapter VII. note 141), para. 46.

the performance of a contract or service is not conditional on consent for data processing purposes that are not necessary for the contract.[217] These five conditions generally apply to exclude interference with the fundamental right to data protection under Article 8 of the Charter and the use of personal data as an economic asset does not change this legal assessment, especially since the economic use of personal data is a legitimate purpose, as described in Chapter VII. 3. b).

Taking all these facets into account, it is clear that the data subjects themselves must be able to decide whether and under what conditions they are prepared to use their personal data as an economic asset.[218] Even though some reservations about the commercialisation of personal data may be justified, these reservations cannot justify depriving the data subjects of self-determination and control over their personal data.[219] Informational self-determination also means self-determination as to how much individuals value their privacy and the confidentiality of their personal data, and, possibly, acting as a data broker on one's own behalf and with one's own personal data in accordance with Article 8 of the Charter.[220]

b) Child's consent to the use of personal data as an economic asset

Children are particularly in need of protection with regard to their personal data, as the risks, rights and consequences of data processing are generally less comprehensible to them.[221] The GDPR stresses that such protection of children's personal data must be in place especially when personal data is processed for marketing or profiling where a service is offered directly to them.[222] Indicator for a direct offer to children can be child-friendly language or content.[223] Services that are directly offered to children are learning platforms, children's news portals as well as online social networks for children.[224] Services such as Facebook, Instagram, Snapchat and TikTok are also directly offered to children, as they intentionally target underage users in addition to adult users.[225]

---

[217] See D. Jahnel, 'Art 7 Bedingungen für die Einwilligung' (*supra* Chapter VII. note 141), para. 30.

[218] See also B. Buchner, 'Die Einwilligung im Datenschutzrecht – vom Rechtfertigungsgrund zum Kommerzialisierungsinstrument' (*supra* Chapter VII. note 125), p. 43.

[219] Ibid.

[220] Ibid; see also G. Hornung, 'Ökonomische Verwertung und informationelle Selbstbestimmung' in A. Roßnagel and G. Hornung (eds.), *Grundrechtschutz im Smart Car* (Springer Verlag, 2019), p. 119.

[221] See Recital 38 GDPR.

[222] Ibid.

[223] D. Jahnel, 'Art 8 Einwilligung eines Kindes in Bezug auf Dienste der Informationsgesellschaft' in D. Jahnel (ed.), *DSGVO Datenschutz Grundverordnung*, para. 8.

[224] D. Kampert, 'Artikel 8 Einwilligung eines Kindes bei Diensten der Informationsgesellschaft' in G. Sydow (ed.), *Europäische Datenschutzgrundverordnung*, para. 9.

[225] Ibid.

As described above, the provision of information regarding consent must be target group oriented and thus easily understandable for children in this context.[226] Where consent is given by a child, the processing of personal data in relation to information society services can be lawful if the child is over 16 years of age.[227] Information society services include contracts and other services that are concluded online.[228] Data controllers must check and verify the age declaration when a child consents.[229] The age limit of 16 years provides legal certainty, but it is questionable how practice-oriented this provision is, since many online offers are aimed at younger children and are also used by them.[230] The GDPR therefore allows Member States to set a lower age limit, which, however, cannot be lower than the age of thirteen.[231] As some Member States have made use of this option, there is no EU-wide harmonisation with regard to the age limit.[232]

If personal data of children under 16 years of age is processed, the consent of the legal guardian is required.[233] Consent may be given by the legal guardians themselves or they may authorise the child's own consent.[234] This also requires technical control mechanisms to determine whether the adult is actually the legal guardian and thus may give consent for the child.[235] This may include an electronic or scanned signature or a passport copy of the legal guardian.[236] Only 'reasonable efforts' to verify the consent are required of the data controller, which is intended not to impose unfulfillable obligations and is an expression of the principle of proportionality.[237] The consent of the legal guardians to data processing is valid even against the express will of the child, unless they abuse their rights or endanger the best interests of the child.[238] Thus, legal guardians can consent to the economic use of their child's personal data against the child's will. Once a child turns 16, in the essence of informational self-determination and control over

[226] EDPB, *Guidelines 05/2020* (*supra* Chapter VII. note 142), p. 26.

[227] See Article 8 (1) GDPR.

[228] EDPB, *Guidelines 05/2020* (*supra* Chapter VII. note 142), p. 27.

[229] Ibid.

[230] D. Kampert, 'Artikel 8 Einwilligung eines Kindes bei Diensten der Informationsgesellschaft' (*supra* Chapter VII. note 224), para. 18.

[231] See Article 8 (1) GDPR; Austria, for example, has set the age limit at the age of 14, see Section 4 (4) DSG.

[232] D. Jahnel, 'Art 8 Einwilligung eines Kindes in Bezug auf Dienste der Informationsgesellschaft' (*supra* Chapter VII. note 223), para. 11.

[233] See Article 8 (1) GDPR.

[234] D. Kampert, 'Artikel 8 Einwilligung eines Kindes bei Diensten der Informationsgesellschaft' (*supra* Chapter VII. note 224), para. 10.

[235] EDPB, *Guidelines 05/2020* (*supra* Chapter VII. note 142), p. 28.

[236] D. Kampert, 'Artikel 8 Einwilligung eines Kindes bei Diensten der Informationsgesellschaft' (*supra* Chapter VII. note 224), para. 13.

[237] Ibid.

[238] Ibid, para. 10.

one's own personal data, the consent of the parent or guardian can be confirmed, revised or withdrawn by the child.[239]

The requirements for consent, i.e. freely given, specific, informed and unambiguous, described above naturally also apply to the consent of children. Here, a strict approach must be taken with regard to consent, as children require particular protection. Children spend more and more time online and represent a large and important target group for companies. Online gaming and especially the advance of eSports attract children, particularly because they can exchange ideas and talk with peers and other people. This phenomenon was certainly promoted by the pandemic, when people had to stay at home in lockdown and could not meet their peers in real life. A Human Rights Watch report found that during the Covid-19 pandemic, numerous online learning products may have tracked children online without their consent or the consent of their parents and harvested personal data.[240]

Due to this increase in importance of the online world for children and their vulnerability, it is therefore essential that strict and additional requirements are placed on both the consent to data processing and the economic use of children's personal data. TikTok and YouTube, two platforms popular with children, have already been fined $ 5.7 million and $ 170 million US dollars respectively in the USA for unlawfully processing children's personal data, including for commercial purposes.[241] On average, the fines in the USA amount to $ 50,120 US dollars per privacy violation per child.[242] In the Netherlands, TikTok was fined € 750,000 because the information on the processing of personal data was provided in English and not in Dutch and was therefore not easily understandable and not suitable for children.[243] These high fines are hardly surprising, especially considering that, as described in Chapter III. 3., sensitive personal data and personal data concerning vulnerable people are of higher value to companies and this is consequently also taken into account when authorities assess the severity of the fines.

---

[239] EDPB, *Guidelines 05/2020* (*supra* Chapter VII. note 142), p. 29.

[240] Human Rights Watch, *How Dare They Peep into My Private Life?,* 25 May 2022, https://www.hrw.org/report/2022/05/25/how-dare-they-peep-my-private-life/childrens-rights-violations-governments (accessed 31 January 2024).

[241] C. Kang, 'F.T.C. Hits Musical.ly With Record Fine for Child Privacy Violation', *The New York Times* (2019), https://www.nytimes.com/2019/02/27/technology/ftc-tiktok-child-privacy-fine.html?module=inline (accessed 31 January 2024); N. Singer and K. Conger, 'Google is Fined $170 Million for Violating Children's Privacy on YouTube', *The New York Times* (2019), https://www.nytimes.com/2019/09/04/technology/google-youtube-fine-ftc.html (accessed 31 January 2024).

[242] PRIVO, *History of COPPA Violations*, 18 February 2022, https://www.privo.com/history-of-coppa-violations (accessed 31 January 2024).

[243] Dutch Data Protection Authority, *TikTok fined for violating children's privacy*, 22 July 2021, https://autoriteitpersoonsgegevens.nl/en/news/tiktok-fined-violating-children's-privacy (accessed 31 January 2024).

c) Consent to the use of sensitive personal data as an economic asset

In some constellations, consent must be explicit. According to the GDPR, this is the case when sensitive data is processed[244], automated decision-making including profiling takes place[245] and personal data is transferred to third countries[246]. Consent for these processing operations must also meet the requirements described above. The higher requirement for 'explicit consent' is that it must be expressed in a clear statement.[247] Consent inferred from a person's actions is not explicit and thus implied consent is not sufficient.[248]

Explicit consent may be given in writing, orally or electronically.[249] In the latter case, an explicit consent box that can be ticked is sufficient.[250] In the case of oral consent, it can be difficult to prove that it was expressly given.[251] It is therefore important that the data subject is unambiguously informed of the intended data processing and it purposes, and that the consent is formulated in such a way that there can be no doubt that it was given.[252] Two-factor authentication could be used as a verification mechanism and proof that consent is valid and explicit.[253]

Due to the high data protection risk in these situations, explicit consent allows data subjects to maintain control over their personal data in the best possible way.[254] This control is at odds with the fact that Article 9 (2) (a) GDPR grants Union or Member state law the possibility to determine that explicit consent cannot be given to processing of sensitive data. Rather, it is in the essence of informational self-determination, autonomy and control of one's own data that data subjects can deliberately disclose sensitive personal data.[255] It is reasonable

---

[244] See Article 9 (2) (a) GDPR.

[245] See Article 22 (2) (c) GDPR.

[246] See Article 49 (1) (a) GDPR.

[247] EDPB, *Guidelines 05/2020* (*supra* Chapter VII. note 142), p. 20.

[248] A. Schiff, 'Art. 9 Verarbeitung besonderer Kategorien personenbezogener Daten' in E. Ehmann and M. Selmayr (eds.), *DS-GVO Datenschutz-Grundverordnung*, para. 33; D. Kampert, 'Artikel 9 Verarbeitung besonderer Kategorien personenbezogener Daten' in G. Sydow (ed.), *Europäische Datenschutzgrundverordnung*, para. 14; D. Jahnel, 'Art 9 Verarbeitung besonderer Kategorien personenbezogener Daten' in D. Jahnel (ed.), *DSGVO Datenschutz Grundverordnung*, para. 52.

[249] EDPB, *Guidelines 05/2020* (*supra* Chapter VII. note 142), p. 21; D. Jahnel, 'Art 9 Verarbeitung besonderer Kategorien personenbezogener Daten' (*supra* Chapter VII. note 248), para. 53.

[250] EDPB, *Guidelines 05/2020* (*supra* Chapter VII. note 142), p. 21.

[251] Ibid; D. Jahnel, 'Art 9 Verarbeitung besonderer Kategorien personenbezogener Daten' (*supra* Chapter VII. note 248), para. 53.

[252] A. Schiff, 'Art. 9 Verarbeitung besonderer Kategorien personenbezogener Daten' (*supra* Chapter VII. note 248), para. 33; D. Kampert, 'Artikel 9 Verarbeitung besonderer Kategorien personenbezogener Daten' (*supra* Chapter VII. note 248), para. 14.

[253] EDPB, Guidelines 05/2020 (*supra* Chapter VII. note 142), p. 21.

[254] Ibid, p. 20.

[255] D. Kampert, 'Artikel 9 Verarbeitung besonderer Kategorien personenbezogener Daten' (*supra* Chapter VII. note 248), para. 15.

to prohibit consent to some processing operations on the basis of public interest or ethical or moral grounds, but this possibility should be used with restraint.[256] In most cases, data subjects should be allowed to decide for themselves whether and how to disclose their sensitive data.

Especially in the case of sensitive data, it is important that explicit consent is given for the processing and economic use of personal data in order to be compatible with Article 8 of the Charter. However, this is often not the case, as not only the example in Chapter III. 3. shows, but also a report by the Federal Trade Commission in the United States reveals. It outlines how a wide range of sensitive data, such as 'race, religion, national origin, sexual orientation, financial status, health and political beliefs', is being used without consent from the data subjects and for purposes that they would not expect and which could cause harm.[257] These sensitive data are used for targeted advertising and profiling of users, a phenomenon described in detail in Chapter III. 2. b). Consequently, explicit consent would have to be given due to the sensitive data and profiling. Considering that personal data is also transferred to third countries such as the US, explicit consent is almost inevitable.

5. Other legal bases for the economic use of personal data

Article 8 (2) of the Charter states that 'some other legitimate basis laid down by law' can provide a justification for an interference with the fundamental right to data protection. Article 6 GDPR provides such legitimate basis and it can be assumed that Article 8 (2) of the Charter, with its reference to 'some other legitimate basis laid down by law', confirms the lawful grounds of processing already set out in the DPD and now laid down in Article 6 GDPR.[258] In the case of these other legitimate bases, however, the decision on data processing, in contrast to consent, does not lie with the data subject.[259] The legitimate bases for data processing set out in Article 6 GDPR allow data controllers to carry out almost any data processing activity that does not ignore the control of the data subject over his or her personal data.[260] As soon as the data processing is justified by one of the

[256] Ibid.

[257] Federal Trade Commission, *A Look At What ISPs Know About You: Examining the Privacy Practices of Six Major Internet Service Providers*, 21 October 2021, p. 34.

[258] N. Bernsdorff, 'Artikel 8 Schutz personenbezogener Daten' (*supra* Chapter VII. note 1), para. 29; T. Riesz, 'Art 8 GRC. Schutz personenbezogener Daten' (*supra* Chapter VI. note 27), para. 70.

[259] D. Jahnel, 'Art 6 Rechtmäßigkeit der Verarbeitung' (*supra* Chapter VII. note 124), para. 18; Karansiou and Douilhet therefore argue that these bases 'temper the power of the data subject over the data': A. P. Karanasiou and E. Douilhet, 'Never Mind the Data: The Legal Quest over Control of Information & the Networked Self' (*supra* Chapter VII. note 124), p. 102.

[260] A. Roßnagel, 'Kein "Verbotsprinzip" und kein "Verbot mit Erlaubnisvorbehalt" im Datenschutzrecht' (*supra* Chapter VI. note 198), p. 5.

following legitimate bases, it is not necessary to fall within the scope of another legitimate basis.[261] Justification by one legitimate basis is sufficient.

a) Personal data as an economic asset for the performance of a contract

In the following, Article 6 (1) (b) GDPR will be examined. According to this provision, data processing is lawful if it is necessary for the performance of a contract with the data subject or necessary for pre-contractual steps taken at the request of the data subject.[262] Data controllers could rely on this ground for data processing and argue that the economic use of personal data, e.g. behavioural advertising, is necessary for the performance of a contract. However, it will be illustrated subsequently that the use of personal data as an economic asset for the performance of a contract does not, in general, constitute a legitimate basis within Article 6 (1) (b) GDPR and Article 8 (2) of the Charter.[263]

Necessity is rooted in the principle of proportionality.[264] This provision is appealing to data controllers as it does not require the consent of the data subject or a balancing of interests in his or her favour for the intended data processing activities.[265] However, to a certain extent, this legitimate basis for data processing has similarities with that of consent.[266] Although consent is not explicitly given for data processing, consent is given voluntarily for the conclusion of a contract.[267] Similarly, giving consent to the processing of personal data does not create a contractual relationship.[268] The EDPB has issued a guideline on this provision which, due to its explicit reference to online services, is highly relevant to the question of the economic use of personal data.[269] The EDPB interprets the provision in a restrictive manner.[270] This may be due to the intransparency of data

---

[261] Case C-252/21 *Meta Platforms and Others* (*supra* Chapter VII. note 128), para. 94.

[262] See Article 6 (1) (b) GDPR.

[263] See also concerning behavioural targeting: F. Zuiderveen Borgesius, 'Legal basis for behavioural targeting' (*supra* Chapter VII. note 76), p. 167.

[264] H. Kranenborg, 'Art 8 Protection of Personal Data' (*supra* Chapter VII. note 14), para. 145.

[265] P. Heinzke and L. Engel, 'Datenverarbeitung zur Vertragserfüllung – Anforderungen und Grenzen', 10 *ZD – Zeitschrift für Datenschutz* (2020), p. 189.

[266] P. Reimer, 'Artikel 6 Rechtmäßigkeit der Verarbeitung' (*supra* Chapter VII. note 176), para. 18; P. Heinzke and L. Engel, 'Datenverarbeitung zur Vertragserfüllung – Anforderungen und Grenzen' (*supra* Chapter VII. note 265), p. 189.

[267] P. Reimer, 'Artikel 6 Rechtmäßigkeit der Verarbeitung' (*supra* Chapter VII. note 176), para, 18.

[268] D. Jahnel, 'Art 6 Rechtmäßigkeit der Verarbeitung' (*supra* Chapter VII. note 124), para. 25.

[269] See EDPB, *Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects*, 9 April 2019.

[270] P. Heinzke and L. Engel, 'Datenverarbeitung zur Vertragserfüllung – Anforderungen und Grenzen' (*supra* Chapter VII. note 265), p. 190.

processing in the digital economy, the power imbalance between data controllers and data subjects, and the increasing monetisation of personal data.[271]

It follows from the wording 'necessary' that this ground of justification cannot be invoked if the data processing is useful but not necessary for the performance of a contract with the data subject or pre-contractual steps taken at the request of the data subject.[272] Consequently, it is not sufficient if the data processing is helpful or profitable for the data controller.[273] The data processing must be objectively necessary for the contractual performance and the data controller must be able to demonstrate that the main purpose of the specific contract with the data subject cannot be fulfilled without the intended data processing.[274] If there are feasible, less intrusive alternatives to achieve the purpose, data processing is not necessary for the performance of a contract.[275]

When determining whether data processing is necessary, particular consideration must be given to the characteristics and essential elements of the services as well as the expectations of the data subject.[276] For the performance of a contract, it is arguably always necessary to collect and store some sort of contact details of a contractual partner.[277] The collection of contact details is most likely also necessary for potential future contractual partners.[278] *Heinzke/Engel* emphasise that the requirement of necessity should give the parties the necessary leeway for drafting a contract so that the entrepreneurial freedom set out in Article 16 of the Charter is respected.[279] The provision of online services and products in return for the economic exploitation of personal data could be within the scope of this leeway.[280] They note that a transparent contract enables data subjects to exercise their right to informational self-determination and to decide whether or not to conclude a contract.[281] This transparency is important because otherwise the data subjects are not aware of the economic use of their personal data and conse-

---

[271] Ibid.

[272] EDPB, *Guidelines 2/2019* (*supra* Chapter VII. note 269), p. 7.

[273] F. Zuiderveen Borgesius, 'Legal basis for behavioural targeting' (*supra* Chapter VII. note 76), p. 166.

[274] Case C-252/21 *Meta Platforms and Others* (*supra* Chapter VII. note 128), para. 98; EDPB, *Guidelines 2/2019* (*supra* Chapter VII. note 269), p. 8; P. Reimer, 'Artikel 6 Rechtmäßigkeit der Verarbeitung' (*supra* Chapter VII. note 176), para. 20.

[275] Case C-252/21 *Meta Platforms and Others* (*supra* Chapter VII. note 128), para. 99; D. Jahnel, 'Art 6 Rechtmäßigkeit der Verarbeitung' (*supra* Chapter VII. note 124), para. 26.

[276] EDPB, *Guidelines 2/2019* (*supra* Chapter VII. note 269), p. 9.

[277] P. Reimer, 'Artikel 6 Rechtmäßigkeit der Verarbeitung' (*supra* Chapter VII. note 176), para. 20.

[278] Ibid.

[279] P. Heinzke and L. Engel, 'Datenverarbeitung zur Vertragserfüllung – Anforderungen und Grenzen' (*supra* Chapter VII. note 265), p. 192.

[280] Ibid, p. 191.

[281] Ibid, p. 192.

quently do not make a conscious decision but merely remain silent, which is not an indication of wishes necessary for the conclusion of a contract.[282]

Based on the core of Article 6 (1) (b) GDPR, it is clear that after the termination or fulfilment of the contract, the data processing can no longer be necessary for the contractual performance and therefore the interference with the fundament right of data protection can no longer be justified on the basis of this provision.[283] However, this does not mean that the data processing per se infringes the right to data protection, as the data processing can be based on another 'legitimate basis', for example because the data subject has consented to further data processing after the termination of the contract.[284]

In e-commerce, the processing of credit card details and home addresses is necessary for the performance of the contract when payment is made online and the product is to be delivered to the data subject's home.[285] However, if the data subject does not want the product to be delivered to his or her home but wants to pick it up, the processing of the home address is not necessary for the performance of the contract and consequently the data controller cannot rely on the necessity of the data processing with regard to the home address.[286]

Data processing for behavioural advertising, tracking and profiling, as described in Chapter III., is generally not necessary for the performance of the contract, e.g. social network, as it primarily finances the service and is not objectively necessary to fulfil the purpose of the contract.[287] Moreover, a contract is concluded to receive products or services, not to receive profiling and personalised advertisements.[288] In addition, a contract would probably have been concluded by the data subject even without behavioural ads, tracking or profiling, especially since Article 21 (3) GDPR also provides for an explicit right to object to marketing purposes.[289] *Heinzke/Engel* also identify difficulties in reconciling advertising-based online business models with Article 6 (1) (b) GPDR, as the principles of transparency and data processing must always be respected and data controllers must clearly outline that the services are not 'free', but that the personal data provided are used as consideration.[290] However, big online companies usually do not fulfil these requirements, as described above.

---

[282] See also, F. Zuiderveen Borgesius, 'Legal basis for behavioural targeting' (*supra* Chapter VII. note 76), p. 166.

[283] EDPB, *Guidelines 2/2019* (*supra* Chapter VII. note 269), p. 11.

[284] Ibid, p. 12.

[285] Ibid, p. 9.

[286] Ibid.

[287] F. Zuiderveen Borgesius, 'Legal basis for behavioural targeting' (*supra* Chapter VII. note 76), p. 166; EDPB, *Guidelines 2/2019* (*supra* Chapter VII. note 269), p. 13.

[288] Ibid.

[289] Ibid.

[290] P. Heinzke and L. Engel, 'Datenverarbeitung zur Vertragserfüllung – Anforderungen und Grenzen' (*supra* Chapter VII. note 265), p. 193.

Likewise, the personalisation of an online service to increase user engagement is not an essential element of the service and therefore cannot be necessary for the performance of a contract.[291] A narrow understanding of the concept of 'performance of a contract' is appropriate in order to balance the interests, namely the fundamental right to data protection and private autonomy, of data subjects and data controllers.[292] At the same time, the EDPB notes that personalisation of content may be necessary in certain other scenarios for the performance of a contract.[293] This notion that personalisation of content can be an intrinsic and expected part of a service is vague and will have to be clarified by the CJEU.[294]

The question of whether Facebook can rely on the necessity for the performance of the contract for data processing for personalisation, advertising and product improvement was referred to the CJEU. The CJEU highlighted that while such personalisation enhances user experience by allowing them to access content closely aligned with their interests, the fact remains that personalised content is not essential for providing the user with the online social network's services.[295] It is conceivable that equivalent alternatives, devoid of such personalisation, could be offered to the user, rendering it not objectively indispensable for a purpose integral to those services.[296]

Likewise, the CJEU will address the question of whether, with regard to the claim that advertisements are shown instead of payment for a service and that these are therefore necessary, one can rely on the necessity of advertising for the performance of the contract instead of obtaining consent.[297] In view of the considerations above, the answer to these questions is and will most likely be no. For the use of personal data as an economic asset, this means that the necessity to perform a contract cannot be relied upon to justify interference with Article 8 of the Charter.

b) Legitimate interests in the economic use of personal data

Another legitimate basis on which the use of personal data as an economic asset can be based is legitimate interest pursued by the data controller or a third party. This legitimate interest is set out in Article 6 (1) (f) of the GDPR. This ground is intended to cover situations where data processing cannot be based on other

---

[291] EDPB, *Guidelines 2/2019* (*supra* Chapter VII. note 269), p. 16.

[292] P. Heinzke and L. Engel, 'Datenverarbeitung zur Vertragserfüllung – Anforderungen und Grenzen' (*supra* Chapter VII. note 265), p. 191.

[293] EDPB, *Guidelines 2/2019* (*supra* Chapter VII. note 269), p. 15.

[294] Ibid; D. Jahnel, 'Art 6 Rechtmäßigkeit der Verarbeitung' (*supra* Chapter VII. note 124), para. 38.

[295] Case C-252/21 *Meta Platforms and Others* (*supra* Chapter VII. note 128), para. 102.

[296] Ibid.

[297] Referral C-446/21 *Schrems*.

legitimate bases.[298] This ground applies to data processing 'inter privatos' and not to data processing activities with public authorities and their institutions and agencies as data controllers on the one hand and citizens as data subjects on the other.[299] Therefore, this ground of lawful data processing is of great importance in the private sector.[300] The provision follows a three-part structure: (i) that there is a legitimate interest of the controller or a third party, (ii) that the processing is necessary for the purposes of the legitimate interests, and (iii) that the interest or fundamental rights and freedoms of the data subject which require the protection of personal data do not override those legitimate interests.[301] Thus, if the interests of the data controller override the interests of the data subject, the personal data may be processed on the basis of legitimate interest.[302] Likewise, if the interests are balanced, the personal data may be processed.[303] If, on the contrary, the interests of the data subjects override the interests of the data controller, the personal data may not be processed.[304] Consequently, a balancing test must be applied. In the following, it will be argued that the balancing test regarding the economic use of personal data by data controllers generally tips in favour of the data subjects. Subsequently, it will be discussed that an interest in the economic use of personal data by data controllers does not, in general, constitute a legitimate basis within Article 6 (1) (f) GDPR and Article 8 (2) of the Charter.[305]

---

[298] D. Jahnel, 'Art 6 Rechtmäßigkeit der Verarbeitung' (*supra* Chapter VII. note 124), para. 67.

[299] E.M. Frenzel, 'DS-GVO Art. 6 Rechtmäßigkeit der Verarbeitung' in B. Paal and D. Pauly (eds.), *DS-GVO BDSG* para. 26; D. Jahnel, 'Art 6 Rechtmäßigkeit der Verarbeitung' (*supra* Chapter VII. note 124), para. 70.

[300] H. Kranenborg, 'Art 8 Protection of Personal Data', para. 154; D. Jahnel, 'Art 6 Rechtmäßigkeit der Verarbeitung' (*supra* Chapter VII. note 124), para. 69.

[301] M. Kastelitz, W. Hötzendorfer and C. Tschohl, 'Art 6 DSGVO. Rechtmäßigkeit der Verarbeitung' in R. Knyrim (ed.), *Der DatKomm,* para. 51; H. Kranenborg, 'Art 8 Protection of Personal Data' (*supra* Chapter VII. note 14), para. 154; E.M. Frenzel, 'DS-GVO Art. 6 Rechtmäßigkeit der Verarbeitung' (*supra* Chapter VII. note 299), para. 27; H. Heberlein 'DS-GVO Art. 6 Rechtmäßigkeit der Verarbeitung' in E. Ehmann and M. Selmayr (eds.), *DS-GVO Datenschutz-Grundverordnung*, para. 25; D. Jahnel, 'Art 6 Rechtmäßigkeit der Verarbeitung' (*supra* Chapter VII. note 124), para. 71; Case C-13/16 *Rīgas satiksme*, EU:C:2017:336, para. 28; Case C-40/17 *Fashion ID* (*supra* Chapter VII. note 56), para. 95; Case C-708/18 *Asociatia de Proprietari bloc M5A-ScaraA* (*supra* Chapter VI. note 174), paras. 40–60; Case C-252/21 *Meta Platforms and Others* (*supra* Chapter VII. note 128), para. 106; Joined Cases C-26/22 and C-64/22 *SCHUFA Holding* (*supra* Chapter IV. note 335), para. 75.

[302] D. Jahnel, 'Art 6 Rechtmäßigkeit der Verarbeitung' (*supra* Chapter VII. note 124), para. 67.

[303] Ibid.

[304] Ibid.

[305] See also concerning behavioural targeting: F. Zuiderveen Borgesius, 'Legal basis for behavioural targeting' (*supra* Chapter VII. note 76), p. 170.

Legitimate interest is to be understood broadly.[306] The term is broader than that of vital interest set out in Article 6 (1) (d) GDPR.[307] Vital interests may be protected without further ado, whereas legitimate interests have to undergo a balancing test.[308] 'Interest' is closely linked to the purpose of data processing.[309] Furthermore, according to Article 6 (1) (f) GDPR, data processing must be necessary for the purposes of the legitimate interests. The requirement of necessity must be interpreted in the light of Article 52 (1) of the Charter and thus implies that no less intrusive means is available to achieve the purpose of the legitimate interest.[310] The need for processing must be examined in connection with the data minimization principle.[311] The WP29 points out that the nature of interests can vary greatly: from interests for the public good or the exercise of fundamental rights to economic interests to learn more about users in order to be able to target advertising.[312] The WP29 has set out in a non-exhaustive list that legitimate interests may be considered, inter alia, in IT security, expression of opinion and information and in various forms of marketing and advertising.[313] Moreover, the CJEU has also held that a third party's interest in obtaining personal information about a person who has damaged his or her property in order to exercise legal claims is legitimate.[314] In order to establish, exercise or defend legal claims, sensitive data may also be processed according to Article 9 (2) (f) GDPR.[315] Recital 47 GDPR also includes marketing as a possible legitimate interest. Similarly, the relationship between the data subject and the data controller, especially if the former is a customer or in the service of the data controller, may constitute a legitimate interest in data processing.[316] This may

---

[306] Joined Cases C-26/22 and C-64/22 *SCHUFA Holding* (*supra* Chapter IV. note 335), para. 76; M. Kastelitz, W. Hötzendorfer and C. Tschohl, 'Art 6 DSGVO. Rechtmäßigkeit der Verarbeitung' (*supra* Chapter VII. note 301), para. 54; E.M. Frenzel, 'DS-GVO Art. 6 Rechtmäßigkeit der Verarbeitung' (*supra* Chapter VII. note 299), para. 28.

[307] P. Reimer, 'Artikel 6 Rechtmäßigkeit der Verarbeitung' (*supra* Chapter VII. note 176), para. 54.

[308] Ibid.

[309] Article 29 Data Protection Working Party opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, 14 November 2014 ('WP217'), p. 24.

[310] Ibid, p. 29; F. Zuiderveen Borgesius, 'Legal basis for behavioural targeting' (*supra* Chapter VII. note 76), p. 168; D. Jahnel, 'Art 6 Rechtmäßigkeit der Verarbeitung' (*supra* Chapter VII. note 124), para. 76; Case C-252/21 *Meta Platforms and Others* (*supra* Chapter VII. note 128), para. 108; Joined Cases C-26/22 and C-64/22 *SCHUFA Holding* (*supra* Chapter IV. note 335), para. 77.

[311] Case C-252/21 *Meta Platforms and Others* (*supra* Chapter VII. note 128), para. 109; Joined Cases C-26/22 and C-64/22 *SCHUFA Holding* (*supra* Chapter IV. note 335), para. 78.

[312] WP217 (*supra* Chapter VII. note 309), p. 24.

[313] Ibid, p. 25.

[314] Case C-13/16 *Rīgas satiksme* (*supra* Chapter VII. note 301), para. 29.

[315] See also regarding the DPD, Case C-13/16 *Rīgas satiksme* (*supra* Chapter VII. note 301), para. 29.

[316] See Recital 47 GDPR.

include, for example, employee data or data from suppliers or competitors.[317] Thus, any ideal or economic interest of the controller or a third party is to be understood as legitimate interest.[318] Whether the use of personal data as an economic asset by companies is necessary, however, is another story.

Data processing is unlawful even if it is necessary, if the interests or fundamental rights and freedoms of the data subjects are overriding.[319] The data subject can therefore put three concerns on the balance: interests, fundamental rights and fundamental freedoms.[320] The scope of protection for data subjects is thus more broadly defined than the scope of legitimate interests of the data controller or a third party.[321] The fundamental rights enshrined in Article 7 and 8 of the Charter in particular have to be taken into account when balancing the legitimate interests of the controller or the third party with the interests and fundamental rights and freedoms of the data subject.[322] Furthermore, other fundamental rights, such as the freedom to conduct a business laid down in Article 16 of the Charter, also come into consideration, insofar as their exercise would also be impaired by the data processing.[323] When assessing the interests or fundamental rights of the data subjects, the expectations of the data subjects at the time of data collection must be taken into account.[324] The expectations of the data subject are expressed in the principle of fairness as described above.[325] The interests and fundamental rights of the data subject could override the interest of the data controller where personal data are processed in contexts where data subjects do not reasonably expect processing.[326] Data processing for profiling, possibly with the help of data bro-

---

[317] P. Reimer, 'Artikel 6 Rechtmäßigkeit der Verarbeitung' (*supra* Chapter VII. note 176), para. 56.

[318] E.M. Frenzel, 'DS-GVO Art. 6 Rechtmäßigkeit der Verarbeitung' (*supra* Chapter VII. note 299), para. 28; P. Reimer, 'Artikel 6 Rechtmäßigkeit der Verarbeitung' (*supra* Chapter VII. note 176), para. 54.

[319] E.M. Frenzel, 'DS-GVO Art. 6 Rechtmäßigkeit der Verarbeitung' (*supra* Chapter VII. note 299), para. 28.

[320] P. Reimer, 'Artikel 6 Rechtmäßigkeit der Verarbeitung' (*supra* Chapter VII. note 176), para. 60.

[321] D. Jahnel, 'Art 6 Rechtmäßigkeit der Verarbeitung' (*supra* Chapter VII. note 124), para. 77.

[322] H. Heberlein 'DS-GVO Art. 6 Rechtmäßigkeit der Verarbeitung' (*supra* Chapter VII. note 301), para. 28 with reference to Case C-468/10 *ASNEF* (*supra* Chapter VI. note 174), para. 40 and Case C-131/12 *Google Spain and Google* (*supra* Chapter IV. note 283), para. 74.

[323] F. Zuiderveen Borgesius, 'Legal basis for behavioural targeting' (*supra* Chapter VII. note 76), p. 167; P. Reimer, 'Artikel 6 Rechtmäßigkeit der Verarbeitung' (*supra* Chapter VII. note 176), para. 60.

[324] See Recital 47 GDPR.

[325] H. Heberlein 'DS-GVO Art. 6 Rechtmäßigkeit der Verarbeitung' (*supra* Chapter VII. note 301), para. 28.

[326] See Recital 47 GDPR; H. Heberlein 'DS-GVO Art. 6 Rechtmäßigkeit der Verarbeitung' (*supra* Chapter VII. note 301), para. 28; P. Reimer, 'Artikel 6 Rechtmäßigkeit der Verarbeitung' (*supra* Chapter VII. note 176), para. 61; Case C-252/21 *Meta Platforms and Others* (*supra* Chapter VII. note 128), para. 112; Joined Cases C-26/22 and C-64/22 *SCHUFA Holding* (*supra* Chapter IV. note 335), para. 80.

kers and personal data from different sources, which was not predictable for the data subjects, constitutes an interference with their right to data protection and thus the legitimate interest of the data controller in the economic use of personal data is overridden by the right to data protection.[327] Furthermore, the relationship between the data subject and the data controller can be decisive, e.g. whether the data controller has a position of authority or whether there is an imbalance of power.[328]

In its WP217, the WP29 uses three scenarios to illustrate plausibly how the balancing of interests can occur and how the balancing can tilt in one direction. Therefore, these scenarios are outlined below in order to provide subsequent considerations on the balancing test. In the first scenario, a person orders pizza via an app on their mobile phone, where address and credit card details are stored and the person receives advertisements for a special offer from the pizzeria in their mailbox a few days later.[329] The pizzeria clearly has an economic interest in this case. Due to the relatively innocuous nature of the personal data and the context, the limited data processing and additional safeguards, the interests and rights of the data subject do not override the legitimate interests of the pizzeria in this scenario.[330]

In the second scenario, the context is the same, but in addition, the purchase history, the browsing history and the location data of the person's mobile phone are stored and processed.[331] This data is processed and analysed to run targeted advertisements off- and on-line for the same special offer as in scenario one.[332] The data processed and the context are relatively harmless in this scenario as well.[333] However, the larger scale of the data collection and the data procession techniques have to be taken into account when applying the balancing test.[334] In addition, there is no transparency and clarity for the data subject as to whether the data processing does not lead to price discrimination.[335] Consequently, according to the WP29, in this scenario the interests and rights of the data subject override the legitimate interest of the pizzeria and the latter would have to obtain consent for the data processing.[336]

In scenario three, the consumption behaviour, time and type of order are shared with an insurance company, which adjusts the health insurance premiums

---

[327] WP217 (*supra* Chapter VII. note 309), p. 26.

[328] H. Heberlein 'DS-GVO Art. 6 Rechtmäßigkeit der Verarbeitung' (*supra* Chapter VII. note 301), para. 28.

[329] WP217 (*supra* Chapter VII. note 309), p. 31.

[330] Ibid.

[331] Ibid, p. 32.

[332] Ibid.

[333] Ibid.

[334] Ibid.

[335] Ibid.

[336] Ibid.

based on these information.[337] In this scenario, an insurance company, a third party, has a legitimate interest in knowing about possible health risks and adjusting premiums accordingly.[338] However, the data subject cannot expect that, because he or she orders a pizza, the insurance premium will potentially be adjusted.[339] In addition to this rampant data processing and profiling, the sensitive nature of the personal data must be taken into account.[340] Consequently, in this scenario, the interests and rights of the data subject outweigh the legitimate interest of the insurance company and the data processing would require consent.[341]

When balancing the interests, the legitimate interest of the data controller or a third party must be assessed.[342] The data controller must carry out this balancing test him- or herself.[343] In principle, EU data protection law allows for a balancing of the conflicting rights and interests in a specific case and must not categorically and generally exclude the processing of certain categories of personal data.[344] The data controller may exercise a fundamental right, such as the right to freedom to conduct a business under Article 16 of the Charter, which must be proportionate and necessary.[345] Whether the use of personal data as an economic asset is proportionate and necessary in the context of digital products or services is questionable.[346] The interests in data processing can be given increased weight in the balancing process by reference to fundamental rights and freedoms.[347] In addition, the data controller may also have other legitimate interests, which, the more compelling they are, may also argue for a balancing test in favour of the data controller.[348] The CJEU has held in this regard that the protection of property, health and life of the data controller and his family may constitute a legitimate interest.[349] Moreover, the purpose of ensuring the general operability of an online media service may be subject to a balancing test with the interests or fundamental rights and freedoms of the users.[350] However, the legitimate interest must be

[337] Ibid, p. 33.
[338] Ibid.
[339] Ibid.
[340] Ibid.
[341] Ibid.
[342] Ibid, p. 34.
[343] D. Jahnel, 'Art 6 Rechtmäßigkeit der Verarbeitung' (*supra* Chapter VII. note 124), para. 68.
[344] Case C–582/14 *Breyer* (*supra* Chapter II. note 136), para. 62.
[345] WP217 (*supra* Chapter VII. note 309), p. 34.
[346] See also F. Zuiderveen Borgesius, 'Legal basis for behavioural targeting' (*supra* Chapter VII. note 76), p. 168.
[347] WP217 (*supra* Chapter VII. note 309), p. 34.
[348] Ibid, p. 35; D. Jahnel, 'Art 6 Rechtmäßigkeit der Verarbeitung' (*supra* Chapter VII. note 124), para. 78.
[349] Case C–212 *Ryneš*, para. 34; Case C-708/18 *Asociatia de Proprietari bloc M5A-ScaraA* (*supra* Chapter VI. note 174), para. 60.
[350] Case C-582/14 *Breyer* (*supra* Chapter II. note 136), para. 63.

interpreted restrictively.[351] Thus, the economic interest in processing personal data for unexpected purposes cannot be considered a legitimate interest that could legitimise the use or disclosure of personal data.[352]

Furthermore, the impact on the data subject must be considered.[353] The nature of the personal data must be taken into account, whereby the more sensitive the personal data is, the greater the impact on the data subject is.[354] The fundamental rights of the data subject may be impacted to different degrees by the data processing, depending on whether the personal data in question are already publicly accessible or not.[355] In addition, the way in which the personal data is processed must be factored in, including the origin of the personal data, the scale of the data processing and the combination of the personal data for profiling for economic purposes.[356] Furthermore, the expectations of the data subject regarding the use and disclosure of the personal data must be taken into account.[357]

Finally, the position of the data controller and the data subject in relation to each other, in particular a possible imbalance of power and the belonging of the data subject to a vulnerable group, e.g. a child, must be assessed.[358] In principle, the age of the data subjects must be taken into account when balancing the respective rights and interests.[359] However, this does not imply that, when processing personal data of a child, the data controller or a third party can never rely on their legitimate interest.[360] Rather, the interests, fundamental rights and freedoms of children are to be given particular importance when applying the balancing test.[361]

Additional safeguards may also be considered when applying the balancing test.[362] These include anonymisation techniques where possible, data minimisation, technical and organisational measures to ensure that personal data are not used for unexpected purposes, privacy by design, data protection impact assessment, transparency and data portability to empower data subjects.[363] The WP29

---

[351] E.M. Frenzel, 'DS-GVO Art. 6 Rechtmäßigkeit der Verarbeitung' (*supra* Chapter VII. note 299), para. 28.

[352] Ibid.

[353] WP217 (*supra* Chapter VII. note 309), p. 36.

[354] Ibid, p. 39.

[355] H. Heberlein 'DS-GVO Art. 6 Rechtmäßigkeit der Verarbeitung' (*supra* Chapter VII. note 301), para. 29.

[356] WP217 (*supra* Chapter VII. note 309), p. 39.

[357] Ibid, p. 40; D. Jahnel, 'Art 6 Rechtmäßigkeit der Verarbeitung' (*supra* Chapter VII. note 124), para. 79.

[358] WP217 (*supra* Chapter VII. note 309), p. 41; P. Reimer, 'Artikel 6 Rechtmäßigkeit der Verarbeitung' (*supra* Chapter VII. note 176), para. 64; D. Jahnel, 'Art 6 Rechtmäßigkeit der Verarbeitung' (*supra* Chapter VII. note 124), para. 66.

[359] Case C-13/16 *Rīgas satiksme* (*supra* Chapter VII. note 301), para. 33.

[360] P. Reimer, 'Artikel 6 Rechtmäßigkeit der Verarbeitung' (*supra* Chapter VII. note 176), para. 64.

[361] Ibid.

[362] WP217 (*supra* Chapter VII. note 309), p. 42.

[363] Ibid.

highlights that data portability in particular enables data subjects to derive greater benefit from digital services, promotes more competitive market conditions and is thus beneficial for data protection as well as for competition and consumer protection.[364]

Among these additional safeguards that play a role in the assessment of the balance is the obligation to inform the data subject. The GDPR obliges the data controller to inform the data subject about the legitimate interest.[365] Information on the legitimate interests involved in the processing of their personal data is in particular prerequisite for enabling the data subject to exercise his or her right to object to the processing of personal data relating to him or her.[366] The right to object allows the data subject to object to data processing, including profiling, based on legitimate interest, where there are grounds for such an objection in the particular situation.[367] In this case, the data subject must provide the relevant grounds.[368] This must then lead to a reassessment of the balance, taking into account the particular arguments put forward by the data subject.[369] Nevertheless, the data controller could offer a more comprehensive 'opt-out option' that would not require additional proof of legitimate grounds by the data subject.[370]

In the case of data processing based on legitimate interest for direct marketing, the data subject may object to such processing at any time.[371] From this point on, the personal data may no longer be used for direct marketing.[372] This right to object to direct marketing is not bound to any grounds and is also neither rebuttable by providing compelling legitimate grounds that override the interests, rights and freedoms of the data subjects nor the assertion, exercise or defence of legal claims by the data controller.[373] The right to object to direct marketing is therefore not subject to any conditions.[374] This is reasonable, especially as direct marketing has evolved and advertising now appears on smartphones, tablets and computers based on behavioural targeting, is personalised and serves the goal to learn as much as possible about customers through online and offline tracking and monitoring of activities, as described in Chapter III. 2.[375] This change in

[364] Ibid, p. 48.
[365] See Articles 13 (1) (d) and 14 (2) (b) GDPR.
[366] H. Heberlein 'DS-GVO Art. 6 Rechtmäßigkeit der Verarbeitung' (*supra* Chapter VII. note 301), para. 34.
[367] See Article 21 (1) GDPR.
[368] WP217 (*supra* Chapter VII. note 309), p. 45; H. Heberlein 'DS-GVO Art. 6 Rechtmäßigkeit der Verarbeitung' (*supra* Chapter VII. note 301), para. 34.
[369] WP217 (*supra* Chapter VII. note 309), p. 45.
[370] Ibid.
[371] See Article 21 (2) GDPR.
[372] See Articel 21 (3) GDPR.
[373] H. Heberlein 'DS-GVO Art. 6 Rechtmäßigkeit der Verarbeitung' (*supra* Chapter VII. note 301), para. 34.
[374] WP217 (*supra* Chapter VII. note 309), p. 45.
[375] Ibid, p. 46.

prevailing business models and the increasing value of personal data as an asset for companies explains the simplified right to object to direct marketing.[376]

The question remains whether data controllers or third parties can rely on their legitimate interest to use personal data as an economic asset. The above explanations and especially the necessary balancing test indicate that this question cannot be answered categorically. As the CJEU ruled, the balancing of the conflicting rights and interests depends on the circumstances of the individual case.[377] Therefore, the assessment of whether the interest in the economic use of personal data can outweigh the interests and fundamental rights of the data subjects must be carried out on a case-by-case basis, too. If one looks at the practices described in Chapter III. 2., they are probably most comparable to scenario 2 above (data is stored, processed and analysed to run targeted advertisements). In such constellations, the WP29 opposes legitimate interest as a legitimate ground for processing. Thus, the use of personal data as an economic asset would not qualify as legitimate interest and would violate Article 8 of the Charter due to a lack of a legitimate basis.

The CJEU held that the operator of a website on which a social plugin is embedded and the provider of this social plugin must each have a legitimate interest, thus justifying the data processing.[378] The Court held that both the operator of the website and the provider of the social plugin have an economic interest in the data processing.[379] Whether this economic interest is sufficient for the balancing test in the specific case was unfortunately not answered. The CJEU dealt with the economic interest in more detail in *Google Spain and Google.*

In *Google Spain and Google*, the CJEU held that the processing of personal data carried out by a search engine operator may substantially affect the fundamental right to the protection of personal data, since the search engine executes a search on the basis of a natural person's name, enabling any internet user to obtain information about the data subject potentially relating to numerous aspects of his or her private life, and thus to build up a more or less detailed profile of the person.[380] Moreover, the CJEU emphasised that the effect of the interference with the fundamental rights of the data subject is further increased by the significant role of the internet and search engines in modern society, which give ubiquity to the information contained in a list of results.[381] The CJEU therefore considered that because of its potential seriousness, such interference could not be justified solely on the basis of the search engine operator's economic interest in

[376] Ibid, p. 46.

[377] Case C-468/10 *ASNEF* (*supra* Chapter VI. note 174), para. 40; Case C-13/16 *Rīgas satiksme* (*supra* Chapter VII. note 301), para. 31.

[378] Case C-40/17 *Fashion ID* (*supra* Chapter VII. note 56), para. 97.

[379] Ibid, para. 80.

[380] Case C-131/12 *Google Spain and Google* (*supra* Chapter IV. note 283), para. 80; see also Case C-460/20 *Google* (*supra* Chapter VI. note 174), para. 52

[381] Case C-131/12 *Google Spain and Google* (*supra* Chapter IV. note 283), para. 80.

processing the personal data.[382] The CJEU concluded that the fundamental rights to privacy and data protection of the data subject, as laid down in Articles 7 and 8 of the Charter, in principle outweigh the economic interest of a search engine operator.[383]

The question of whether a company such as Facebook can justify collecting personal data on the grounds that it pursues legitimate interests, i.e. personalised advertising, under Article 6 (1) (f) GDPR was referred to the CJEU. The CJEU held that the data processing in question can principally be deemed necessary for the legitimate interests pursued by Facebook or a third party, provided that (i) Facebook has informed the users from whom the personal data is collected about a legitimate interest associated with the processing.[384] (ii) Such processing must be conducted strictly within the confines necessary for the specified legitimate interest.[385] (iii) Considering all pertinent circumstances, the interests or fundamental freedoms and rights of the users must not take precedence over the legitimate interest pursued by Facebook.[386] The CJEU concludes, among other considerations, that in the absence of user consent, the interests and fundamental rights of users supersede Facebook's interest in personalised advertising through which it finances its operations.[387]

In line with the above considerations, in order to affirm legitimate interest in the economic use of personal data by the data controller, the CJEU established (i) that there has to be a legitimate interest of the controller or a third party, (ii) that the processing has to be necessary for the purposes of the legitimate interests, and (iii) that the interest or fundamental rights and freedoms of the data subject which require the protection of personal data do not override those legitimate interests. In light of the above, the Court rightfully rejected legitimate interest for the economic use of personal data in this case.

c) Other possible legitimate bases laid down by law

There are also other legitimate bases on which the economic use of personal data could be justified. For example, data processing may be lawful if it is 'necessary for compliance with a legal obligation to which the controller is subject'.[388] The data processing activities must be required of the data controller by Union or Member State law.[389] The relevant legal basis laying down obligations for the

[382] Ibid, para. 81.
[383] Ibid, para. 97.
[384] Case C-252/21 *Meta Platforms and Others* (*supra* Chapter VII. note 128), paras. 115–118.
[385] Ibid.
[386] Ibid.
[387] Ibid.
[388] See Article 6 (1) (c) GDPR.
[389] See Article 6 (3) GDPR.

data controller must be sufficiently clear, precise, foreseeable and specify the purposes of the processing.[390] A legal obligation that was not established by a legal provision but by a contract is not covered by this legitimate basis.[391] The data processing must pursue an objective in the public interest, i.e. the data controller must not process data to fulfil a contractual obligation in the individual interest and rely on this ground of processing.[392] The WP29 stresses that for the monitoring of users to combat illegal downloading, without a clear and specific legal obligation to do so, this basis is not appropriate.[393] Rather, this basis covers situations such as employers having to report the salary data or working time of their employees to the authorities[394] or financial institution being obliged to report transactions to the authorities for anti-money laundering purposes.[395] Consequently, this basis cannot be sufficient to use personal data as an economic asset. It is primarily individual interests that are pursued through the economic use of personal data. Furthermore, there is no obligation under Member State or Union law to use personal data as an economic asset, i.e. to profile users, share data and provide targeted advertising, as described in Chapter III. 2.

Besides this legitimate basis, Article 6 (1) (d) GDPR provides for a legitimate basis where 'processing is necessary in order to protect the vital interests of the data subject or of another natural person'. Vital interests are primarily the protection of life and physical integrity.[396] According to the WP29, vital interests are a question of life and death.[397] In such instances, data protection gives way to the protection of life.[398] This is a subordinate ground for lawful processing.[399] In addition, the scope of application is very narrow, which leads to a marginal practical significance.[400] Existential business interests of individual companies are

---

[390] See Recital 41 GDPR.

[391] H. Heberlein 'DS-GVO Art. 6 Rechtmäßigkeit der Verarbeitung' (*supra* Chapter VII. note 301), para. 16; M. Kastelitz, W. Hötzendorfer and C. Tschohl, 'Art 6 DSGVO. Rechtmäßigkeit der Verarbeitung' (*supra* Chapter VII. note 301), para. 39; WP217 (*supra* Chapter VII. note 309), p. 19.

[392] H. Heberlein 'DS-GVO Art. 6 Rechtmäßigkeit der Verarbeitung' (*supra* Chapter VII. note 301), para. 16.

[393] WP217 (*supra* Chapter VII. note 309), p. 19.

[394] See Case C-342/12 *Worten* (*supra* Chapter II. note 56).

[395] Ibid.

[396] H. Heberlein 'DS-GVO Art. 6 Rechtmäßigkeit der Verarbeitung' (*supra* Chapter VII. note 301), para. 18; WP217 (*supra* Chapter VII. note 309), p. 20; M. Kastelitz, W. Hötzendorfer and C. Tschohl, 'Art 6 DSGVO. Rechtmäßigkeit der Verarbeitung' (*supra* Chapter VII. note 301), para. 39.

[397] WP217 (*supra* Chapter VII. note 309), p. 20.

[398] P. Reimer, 'Artikel 6 Rechtmäßigkeit der Verarbeitung' (*supra* Chapter VII. note 176), para. 31.

[399] See Recital 46 GDPR; H. Heberlein 'DS-GVO Art. 6 Rechtmäßigkeit der Verarbeitung' (*supra* Chapter VII. note 301), para. 19; M. Kastelitz, W. Hötzendorfer and C. Tschohl, 'Art 6 DSGVO. Rechtmäßigkeit der Verarbeitung' (*supra* Chapter VII. note 301), para. 44.

[400] WP217 (*supra* Chapter VII. note 309), p. 20; M. Kastelitz, W. Hötzendorfer and C.

not sufficient to rely on this basis for processing.[401] The use of personal data as an economic asset will in most cases not be a matter of life and death and therefore this ground for processing is not applicable.

Another legal ground requires that the processing is necessary for a task entrusted to the data controller and that this task is either in the public interest or in the exercise of official authority.[402] The condition of necessity requires, in accordance with the purpose of the GDPR, that the processing of personal data be limited to what is absolutely necessary.[403] The processing activities must therefore be necessary for the performance of tasks in the public interests as well as in the exercise of official authority, allowing the data controller to fulfil this task efficiently.[404] As examples, the WP29 mentions electronic monitoring of e-mail traffic, processing activities in the transport or health sector (e.g. epidemiological studies, research) and combating illegal content on the Internet.[405] This legal basis has a potentially very wide scope, which requires a strict interpretation and a clear identification of the public interest at stake and the authority justifying the processing on a case-by-case basis.[406] As explained above, generally, the economic use of personal data pursues individual and economic interests and is therefore not covered by this legal basis.

6. Right of access to and right to rectify personal data as an economic asset

Article 8 (2) second sentence of the Charter contains the right of the data subject to obtain access to data collected concerning him or her and, where required, to obtain rectification.[407] The right of access is an essential core element of the fundamental right to data protection.[408] Only individuals who can determine by whom their personal data is being processed and for what purpose can assess

---

Tschohl, 'Art 6 DSGVO. Rechtmäßigkeit der Verarbeitung' (*supra* Chapter VII. note 301), para. 44; D. Jahnel, 'Art 6 Rechtmäßigkeit der Verarbeitung' (*supra* Chapter VII. note 124), para. 52.

[401] P. Reimer, 'Artikel 6 Rechtmäßigkeit der Verarbeitung' (*supra* Chapter VII. note 176), para. 33.

[402] See Article 6 (1) (e) GDPR.

[403] H. Heberlein 'DS-GVO Art. 6 Rechtmäßigkeit der Verarbeitung' (*supra* Chapter VII. note 301), para. 22.

[404] Ibid.

[405] WP217 (*supra* Chapter VII. note 309), p. 22.

[406] Ibid.

[407] H. Johlen, 'Art. 8 Schutz personenbezogener Daten' (*supra* Chapter VII. note 1), para. 57.

[408] T. Riesz, 'Art 8 GRC. Schutz personenbezogener Daten' (*supra* Chapter VI. note 27), para. 72; H. Johlen, 'Art. 8 Schutz personenbezogener Daten' (*supra* Chapter VII. note 1), para. 58.

whether the personal data is accurate and is being processed in accordance with the Charter and, if necessary, avert an infringement of the fundamental right to data protection.[409] Both the right of access and the right of rectification are integral parts of the right to informational self-determination.[410] Like the right to data protection as such, the right of access and right to rectify are not absolute and can be limited according to Article 52 (1) of the Charter.[411] However, this is only possible in case of substantial and valid justifications.[412] For the scope and details of the right of access and the right of rectification, please refer to the discussion in Chapters IV. 3. b) and c).

The question arises as to whether the other rights of data subjects described in Chapter IV. 2. are covered by Article 8 (2) of the Charter, although they are not explicitly mentioned. Contrary to the wording of Article 8 of the Charter, there are several reasons in favour of such an interpretation. *Kranenborg* points out that the CJEU includes the right to be actively informed under Article 8 of the Charter.[413] He notes that the CJEU stated that an active notification to the data subject is necessary to ensure correct and lawful data processing and to guarantee the protection of the right to data protection.[414] *Riesz* argues that the continued storage of personal data beyond the specified, fair purpose leads to an unlawful interference with the right to data protection and that the right to erasure thus serves to 'rectify' the infringement and accrues to the data subjects despite the fact that it is not explicitly listed in Article 8 (2) of the Charter.[415] He also refers to the *Google Spain and Google* case, in which the CJEU recognised that data subjects can demand under Article 8 of the Charter that personal data be stored by a search engine operator for no longer than is necessary and thus the right to erasure or 'to be forgotten' is also covered by Article 8 of the Charter.[416] Consequently, Article 8 (2) of the Charter is not an exhaustive list of data subjects' rights that must be safeguarded in order to be compatible with the fundamental

[409] T. Riesz, 'Art 8 GRC. Schutz personenbezogener Daten' (*supra* Chapter VI. note 27), para. 72.

[410] H. Johlen, 'Art. 8 Schutz personenbezogener Daten' (*supra* Chapter VII. note 1), para. 61.

[411] H.D. Jarass, 'Art. 8 Schutz personenbezogener Daten' (*supra* Chapter VI. note 64), para. 21; T. Riesz, 'Art 8 GRC. Schutz personenbezogener Daten' (*supra* Chapter VI. note 27), para. 74.

[412] H.D. Jarass, 'Art. 8 Schutz personenbezogener Daten' (*supra* Chapter VI. note 64), para. 21.

[413] H. Kranenborg, 'Art 8 Protection of Personal Data' (*supra* Chapter VII. note 14), para. 162.

[414] Ibid, with reference to Case C-203/15 *Tele2 Sverige* (*supra* Chapter VI. note 174), para. 293.

[415] T. Riesz, 'Art 8 GRC. Schutz personenbezogener Daten' (*supra* Chapter VI. note 27), para. 76.

[416] Ibid, para. 76, with reference to Case C-131/12 *Google Spain and Google* (*supra* Chapter IV. note 283), para. 79.

right to data protection.[417] Thus, the other rights described in Chapter IV. 2. must also be protected to ensure that data processing activities are compatible with Article 8 of the Charter.

What do these conclusions mean for the use of personal data as an economic asset? Firstly, this means that all data subjects' rights must be respected to ensure that the economic use of personal data is compatible with the Charter. Furthermore, these rights strengthen the data subject's informational self-determination. Thus, the argumentation of Chapter IV. 2., that personal data as an economic asset should be allocated to the data subjects, is appropriate, as it strengthens the data subjects both in their control over their personal data and in their protection of their fundamental right. This does not mean that companies or third parties are not allowed to use personal data of data subjects as an economic asset. However, they must always guarantee data subjects' rights, otherwise the use of personal data as an economic asset is not compatible with Article 8 of the Charter.

7. Conclusion: Personal data as an economic asset can be compatible with Article 8 of the Charter

In the case of the use of personal data as an economic asset, which always involves data processing in the background, the scope of Article 8 of the Charter is triggered if there is an establishment in the EU, even if personal data is not processed by the establishment but in the context of its activities, or if there is no establishment in the EU but products or services are offered in a targeted manner to EU citizens. Furthermore, data controllers and processors and their commercial use of and economic interest in personal data may be decisive in triggering the application of data protection rules.

In principle, the economic use of personal data is not per se incompatible with Article 8 of the Charter. However, certain conditions must be met. One of these conditions is that personal data must be processed fairly. The use of personal data as an economic asset, in order to comply with the explicit principle of fairness of Article 8 (2) of the Charter, must fulfil two conditions: First, the economic use of personal data must be clear, transparent and comprehensible to data subjects. Second, data subjects must be fully informed about the economic use of personal data in all its forms. This includes information about the risks involved in the commercial use of personal data, about the sharing with third parties and about the rights of data subjects. In most instances this is not the case, as data subjects are unaware of the use of personal data as an economic asset. Furthermore, all data subjects' rights must be respected to ensure that the economic use of personal data is compatible with the Charter.

---

[417] T. Riesz, 'Art 8 GRC. Schutz personenbezogener Daten' (*supra* Chapter VI. note 27), para. 77.

Moreover, according to Article 8 (2) of the Charter, data processing may only be carried out for specified purposes. For personal data to be used as an economic asset, the purpose of the data processing (i.e. economic exploitation) must be explicitly disclosed before the personal data is collected, must be limited to the purpose and it must be limited in time. It must be legitimate, proportionate and necessary. This purpose limitation and data minimisation allows data subjects to retain control over their personal data and anticipate interference with their fundamental right to data protection. It is a balancing act to meet these requirements in practice when using personal data for economic purposes, as the specified purpose must not be too vague, but at the same time not too detailed and incomprehensible.

If personal data as an economic asset are processed fairly and for a specified purpose and, in addition, the consent of the data subject has been obtained, the requirements of Article 8 (2) of the Charter are met. Consequently, valid consent to the use of personal data as an economic asset precludes interference with the fundamental right to data protection.

Consent must be 'freely' given, i.e. data subjects have genuine freedom and power over it. Particular consideration must be given to power asymmetries and 'take it or leave it' constellations, as consent is not given freely here. One solution to this could be a fee-based alternative in which personal data are not processed and exploited economically. Furthermore, consent must be 'specific' and 'informed'. In many cases, consent is not an expression of a self-determined and informed decision about the economic use of personal data because they are not aware of the use of personal data by companies. Moreover, consent must be given by a 'clear, affirmative act'. This means that data subjects must actively consent to the economic exploitation of their personal data and data controllers must be able to prove that consent has been given. Lastly, consent must be withdrawable at any time.

If data subjects themselves decide to use their personal data as an economic asset in return for 'free' services or products, they are expressing their self-determination and private autonomy. Data subjects are free to decide whether to consent to the use of personal data as an economic asset, unless the processing of their personal data is unfair, unspecified and/or they lose control over their personal data as a result of consent.

There are strict and additional requirements placed on both the consent to data processing and the economic use of children's personal data. One of these is that a parent or legal guardian must consent to the processing of personal data of the child. Likewise, when processing sensitive personal data, consent must be explicit in addition to the above requirements. Sensitive personal data and personal data concerning vulnerable people are of higher value to companies and it therefore makes sense to set higher requirements for their exploitation.

Another legitimate basis for data processing is the necessity for the performance of a contract. It follows from the wording 'necessary' that this ground of justification cannot be invoked if the data processing is useful but not necessary

for the performance of a contract. In practice, however, the economic use of personal data is useful and not necessary.

The legitimate interest in the economic use of personal data could be another legitimate basis for data processing. Whether data controllers or third parties can rely on their legitimate interest to use personal data as an economic asset, cannot be answered categorically. As a balancing test must always be applied, it boils down to a case-by-case decision. If one follows the opinions of data protection advocates, data controllers and third parties cannot invoke their legitimate interest to use personal data as an economic asset. Similarly, they cannot invoke the fulfilment of a legal obligation or the protection of vital interests of data subjects when using personal data economically.

All in all, personal data as an economic asset can be compatible with Article 8 of the Charter. Consent is of central importance. It is the only clear, legitimate basis for the economic use of personal data. This is reasonable, as data subjects themselves should be the ones to decide on the economic use of their personal data.

VIII. Personal data as an economic asset in the light of Article 52 of the Charter

Article 52 of the Charter aims to define the scope of the rights and principles of the Charter and rules for their interpretation. Article 6 TEU, as mentioned above, states that the general provisions of Title VII are to be taken into account for the interpretation of the Charter. This therefore also includes Article 52 of the Charter. In order to discuss the limitations on the use of personal data as an economic asset, the following aspects are discussed below. Firstly, Section 1 deals with limitations on the exercise of rights and freedoms of the Charter. It examines if and when the economic use of personal data can be compatible with Article 52 (1) of the Charter. Section 2 analyses the rights and interests that interact with the right to data protection and need to be balanced when personal data is used as an economic asset. Section 3 then provides a short overview of the relationship between the rights enshrined in the Charter and the rights provided for in the Treaties. Finally, Section 4 discusses the extent to which the ECHR can be used to address the economic use of personal data.

1. Limitations on the exercise of rights and freedoms

Article 52 (1) of the Charter concerns the essence of EU law and deals with core issues of fundamental rights.[1] In fact, it concerns the fundamental question of when restrictions violate fundamental rights and when they do not. Generally, fundamental rights do not offer absolute protection, but they can be restricted.[2] Only absolute rights such as human dignity, which is set out in Article 1 of the Charter, or the prohibition of slavery and forced labour, which is laid down in

[1] S. Peers and S. Prechal, 'Art 52 Scope and Interpretation of Rights and Principles' in S. Peers et al. (eds.), *The EU Charter of Fundamental Rights*, para. 07; O. Scarcello, 'Preserving the "Essence" of Fundamental Rights under Article 52(1) of the Charter: A Sisyphean Task?', 16 *European Constitutional Law Review* (2020), p. 667.

[2] A. Schwerdtfeger, 'Artikel 52 Tragweite und Auslegung der Rechte und Grundsätze' in J. Meyer and S. Hölscheidt (eds.), *Charta der Grundrechte der Europäischen Union*, para. 27.

Article 5 of the Charter, cannot be restricted.[3] They can be defined as unlimited fundamental rights.[4]

As mentioned above, the right to the protection of personal data is not an unlimited right and must be viewed in terms of its function in society.[5] It is therefore possible that the right to the protection of personal data is subject to limitations.

If there is no consent, it is necessary to examine whether the economic use of personal data represents a justified limitation of the right to data protection. Generally, Article 52 (1) of the Charter applies to any limitation, as the wording already suggests.[6] An exception is the fundamental right to data protection, the limitation clause of which is specifically enshrined in Article 8 (2) of the Charter. The interplay of these two provisions has still not been clarified by the CJEU or legal scholars and was criticised early on.[7] Many authors assume that the requirements of Article 52 (1) of the Charter have to be considered alongside the requirements of Article 8 (2) of the Charter.[8] Therefore, Article 52 (1) of the Charter will be discussed below. A detailed analysis of this provision would go beyond the scope of this paper. Therefore, its contours that are needed to interpret the phenomenon of personal data as an economic asset will be outlined.

a) Article 52 (1) as a general limitation clause

Firstly, it must be clarified whether in constellations between two private parties, as is usually the case with the use of personal data as an economic asset, the

---

[3] S. Peers and S. Prechal, 'Art 52 Scope and Interpretation of Rights and Principles' (*supra* Chapter VIII. note 1), para. 34; A. Schwerdtfeger, 'Artikel 52 Tragweite und Auslegung der Rechte und Grundsätze' (*supra* Chapter VIII. note 2), para. 27.

[4] H.D. Jarass, 'Art. 52 Tragweite und Auslegung der Rechte und Grundsätze' in H.D. Jarass (ed.), *Charta der Grundrechte der Europäischen Union*, para. 22.

[5] Case C-154/21 *Österreichische Post* (*supra* Chapter IV. note 234), para. 47; Joined Cases C-37/20 and C-601/20 *Luxembourg Business Registers*, EU:C:2022:912, para. 45; Case C-817/19 *Ligue des droits humains*, EU:C:2022:491, para. 112. Case C-92/09 *Volker und Markus Schecke und Eifert* (*supra* Chapter II. note 184), para. 48; T. Riesz, 'Art 8 GRC. Schutz personenbezogener Daten' (*supra* Chapter VI. note 27), para. 60; M. Tzanou, 'Data protection as a fundamental right next to privacy? "Reconstructing" a not so new right' (*supra* Chapter IV. note 187), p. 98.

[6] A. Schwerdtfeger, 'Artikel 52 Tragweite und Auslegung der Rechte und Grundsätze' (*supra* Chapter VIII. note 2), para. 28; H.D. Jarass, 'Art. 52 Tragweite und Auslegung der Rechte und Grundsätze' (*supra* Chapter VIII. note 4), para. 20.

[7] G. González Fuster and R. Gellert, 'The fundamental right to data protection in the European Union: in search of an uncharted right', 26 *International Review of Law, Computers & Technology* (2012), p. 70.

[8] A. Schwerdtfeger, 'Artikel 52 Tragweite und Auslegung der Rechte und Grundsätze' (*supra* Chapter VIII. note 2), para. 28; H.D. Jarass, 'Art. 52 Tragweite und Auslegung der Rechte und Grundsätze' (*supra* Chapter VIII. note 4), para. 22; H. Johlen, 'Art. 8 Schutz personenbezogener Daten' (*supra* Chapter VII. note 1), para. 40.

general limitation clause of Article 52 (1) of the Charter applies, which is not self-evident.[9] In *McDonagh*, the CJEU applied Article 52 (1) of the Charter in a dispute between private parties.[10] The provision thus allows that rights of the Charter may be restricted in order to promote the protection of other rights enshrined in the Charter.[11] Another argument in favour of the application of Article 52 (1) of the Charter in disputes between private individuals is that the balance between the conflicting fundamental rights involves the protection of the essence of fundamental rights, which is explicitly stated in Article 52 (1) of the Charter.[12] Moreover, the balancing test that must be applied in the case of conflicting fundamental rights also fits the principle of proportionality of Article 52 (1) of the Charter.[13]

Article 52 (1) of the Charter imposes several conditions on limitations of rights enshrined therein, as can be gathered from its wording, which reads

> 'Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.'[14]

A general limitation clause is thus introduced, which is very reminiscent of limitations of the ECHR.[15] The European Convention that drafted the Charter included the essence of fundamental rights, which did not entail much discussion, as the focus was rather on proportionality and its articulation.[16]

b) Limitation provided for by law

Any limitation of a fundamental right enshrined in the Charter must be provided for by law, according to Article 52 (1) of the Charter. This includes a limitation provided for by a law itself as well as the authorisation for a limitation provided for by a law.[17] Should the limitation serve to promote the fundamental rights of

---

[9] H.D. Jarass, 'Die Bedeutung der Unionsgrundrechte unter Privaten' (*supra* Chapter VI. note 76), p. 326.

[10] Case C-12/11 *McDonagh*, EU:C:2013:43, para. 61; H.D. Jarass, 'Die Bedeutung der Unionsgrundrechte unter Privaten' (*supra* Chapter VI. note 76), p. 327.

[11] H.D. Jarass, 'Die Bedeutung der Unionsgrundrechte unter Privaten' (*supra* Chapter VI. note 76), p. 327

[12] Ibid.

[13] Ibid.

[14] See Article 52 (1) Charter.

[15] S. Peers and S. Prechal, 'Art 52 Scope and Interpretation of Rights and Principles' (*supra* Chapter VIII. note 1), para. 15; A. Schwerdtfeger, 'Artikel 52 Tragweite und Auslegung der Rechte und Grundsätze' (*supra* Chapter VIII. note 2), para. 10; H. Krämer, 'Art. 52 Tragweite und Auslegung der Rechte und Grundsätze' (*supra* Chapter VII. note 60), para. 31.

[16] A. Schwerdtfeger, 'Artikel 52 Tragweite und Auslegung der Rechte und Grundsätze' (*supra* Chapter VIII. note 2), para. 10.

[17] A. Schwerdtfeger, 'Artikel 52 Tragweite und Auslegung der Rechte und Grundsätze' (*supra* Chapter VIII. note 2), para. 30.

other persons, it also requires a legal basis.[18] The legal basis for any limitation must be sufficiently clear and precise.[19] Furthermore, the legislation in question must impose 'minimum safeguards so that the persons […] have sufficient guarantees' that their rights are protected.[20] A limitation is to be deemed provided for by law within the meaning of Article 52 (1) of the Charter if it is based on a provision adopted by the Union legislature.[21] It is also sufficient if the limitation is provided for by national legislature.[22] The legislation which permits the interference with a fundamental right must itself define the scope of the limitation,

> '[…] bearing in mind, that the [CJEU] may, where appropriate, specify, by means of interpretation, the actual scope of the limitation in the light of the very wording of the EU legislation in question as well as its general scheme and the objectives it pursues, as interpreted in view of the fundamental rights guaranteed by the Charter.'[23]

The GDPR meets these requirements. The CJEU itself held that the GDPR 'respects all the fundamental rights […] recognised by the Charter […]'.[24] It was introduced by the Union legislator and introduces numerous obligations for data controllers and rights for data subjects, as described in Chapter IV. 3. The use of personal data as an economic asset involves in most cases data processing operations, as set out in Chapter III. 2. Data processing may limit the exercise of fundamental rights of data subjects but is explicitly allowed by the GDPR under certain conditions.[25] In principle, the limitation of the exercise of fundamental rights using personal data as an economic asset is thus provided for by law, at least as far as data processing is concerned.

---

[18] H.D. Jarass, 'Art. 52 Tragweite und Auslegung der Rechte und Grundsätze' (*supra* Chapter VIII. note 4), para. 23.

[19] See Case C-293/12 *Digital Rights Ireland* (*supra* Chapter II. note 130), para. 54; Case C-419/14 *WebMindLicenses* (*supra* Chapter II. note 185), para. 81.

[20] See Case C-293/12 *Digital Rights Ireland* (*supra* Chapter II. note 130), para. 54.

[21] See Case C-547/14 *Philip Morris Brands*, EU:C:2016:325, para. 150; H.D. Jarass, 'Art. 52 Tragweite und Auslegung der Rechte und Grundsätze' (*supra* Chapter VIII. note 4), para. 24.

[22] See Case C-540/16 *Spika*, EU:C:2018:565, para. 44; S. Peers and S. Prechal, 'Art 52 Scope and Interpretation of Rights and Principles' (*supra* Chapter VIII. note 1), para. 39; A. Schwerdtfeger, 'Artikel 52 Tragweite und Auslegung der Rechte und Grundsätze' (*supra* Chapter VIII. note 2), para. 33; H.D. Jarass, 'Art. 52 Tragweite und Auslegung der Rechte und Grundsätze' (*supra* Chapter VIII. note 4), para. 26.

[23] Joined Cases C-37/20 and C-601/20 *Luxembourg Business Registers* (*supra* Chapter VIII. note 5), para. 47; Case C-817/19 *Ligue des droits humains* (*supra* Chapter VIII. note 5), para. 114.

[24] Case C-307/22 *FT* (*supra* Chapter IV. note 234), para. 59;

[25] See A. Roßnagel, 'Kein "Verbotsprinzip" und kein "Verbot mit Erlaubnisvorbehalt" im Datenschutzrecht' (*supra* Chapter VI. note 198), p. 4.

c) Essence of right to protection of personal data

Furthermore, any limitation of a right enshrined in the Charter must respect the essence of the rights and freedoms recognised by the Charter, according to Article 52 (1) of the Charter. Where an EU measure or national measure implementing EU law violates the essence of a fundamental right, that measure is invalid.[26]

Lenaerts speaks of a 'nucleus' that is absolute and left free of any limitations.[27] *Brkan* uses the image of peeling an onion: the outermost layer is the fundamental right as such, without interference of any form, the innermost layer is that of the core or 'essence', which must not be interfered with or restricted.[28]

The Explanations on Article 1 of the Charter state that human dignity is part of the essence of all Charter rights.[29] The Explanations suggest that the concept of essence of a fundamental right is inspired by the jurisprudence of the CJEU on fundamental rights.[30] This may be true at a European level, but neither the CJEU nor the Charter introduced a new concept, as the essence of a fundamental right is deeply rooted in some constitutional traditions of the Member States.[31] The question of the essence of a fundamental right cannot be answered on the basis of the wording of the Charter, but rather requires a contextual, case-by-case analysis.[32]

Under established case law of the CJEU, the obligation to respect the essential content of fundamental rights 'does not call into question that right as such'.[33] With regard to the essence of fundamental rights, the *Schrems* judgment is to be highlighted as a milestone, as it contours the structure of fundamental rights, in particular Article 52 (1) of the Charter.[34] The CJEU pointed out that legislation

---

[26] K. Lenaerts, 'Limits on Limitations: The Essence of Fundamental Rights in the EU', 20 *German Law Journal* (2019), p. 780.

[27] Ibid, p. 781.

[28] M. Brkan, 'The Concept of Essence of Fundamental Rights in the EU Legal Order: Peeling the Onion to its Core', 14 *European Constitutional Law Review* (2018), p. 333.

[29] Explanations relating to the Charter of Fundamental Rights [2007] OJ C303/17.

[30] K. Lenaerts, 'Limits on Limitations: The Essence of Fundamental Rights in the EU' (*supra* Chapter VIII. note 26), p. 780.

[31] Ibid; M. Brkan, 'The Concept of Essence of Fundamental Rights in the EU Legal Order: Peeling the Onion to its Core' (*supra* Chapter VIII. note 28), p. 338.

[32] T. Ojanen, 'Making the Essence of Fundamental Rights Real: The Court of Justice of the European Union Clarifies the Structure of Fundamental Rights under the Charter' 12 *European Constitutional Law Review* (2016), p. 326; M. Brkan, 'The Concept of Essence of Fundamental Rights in the EU Legal Order: Peeling the Onion to its Core' (*supra* Chapter VIII. note 28), p. 350.

[33] See for example, Case C–73/16 *Puškár* (*supra* Chapter VII. note 115), para. 64; also A. Schwerdtfeger, 'Artikel 52 Tragweite und Auslegung der Rechte und Grundsätze' (*supra* Chapter VIII. note 2), para. 34 and the case law cited; M. Brkan, 'The Concept of Essence of Fundamental Rights in the EU Legal Order: Peeling the Onion to its Core' (*supra* Chapter VIII. note 28), p. 363.

[34] T. Ojanen, 'Making the Essence of Fundamental Rights Real: The Court of Justice of the European Union Clarifies the Structure of Fundamental Rights under the Charter' (*supra* Chapter VIII. note 32), p. 320.

allowing the authorities to access the content of electronic communications in a blanket manner violates the essence of the fundamental right to respect for private life.[35] Furthermore, the CJEU stated that legislation which does not provide for the possibility for citizens to obtain access to their personal data concerning them or to obtain their rectification or erasure by means of a judicial remedy violates the essence of the fundamental right to effective judicial protection.[36] Since the CJEU did not examine the content of the legislation in question, it can be concluded that the fundamental rights enshrined in the Charter have an inviolable core which may not be limited or balanced.[37]

In the case law since *Schrems*, the CJEU has not yet developed an elaborate method for determining the essence of a fundamental right.[38] For example, the *Bauer* judgment could also be understood as protecting the essence of the fundamental right to an annual period of paid leave enshrined in Article 31 (2) of the Charter, as the CJEU referred to the 'very substance of that right'.[39] To establish whether a measure violates the essence of a fundamental right, the intensity and also the extent of the interference must be taken into account.[40] A measure that violates certain aspects of a fundamental right, but does not affect others, may respect the essence of the right.[41] The CJEU has so far been cautious in finding a violation of the concept of the essence of a fundamental right.[42] An overly broad conception of the essence of a fundamental right should be treated with caution, as otherwise all Charter rights could become absolute rights and this would be

[35] Case C-362/14 *Schrems* (*supra* Chapter VI. note 64), para. 94.

[36] Ibid, para. 95.

[37] T. Ojanen, 'Making the Essence of Fundamental Rights Real: The Court of Justice of the European Union Clarifies the Structure of Fundamental Rights under the Charter' (*supra* Chapter VIII. note 32), p. 325.

[38] See O. Scarcello, 'Preserving the "Essence" of Fundamental Rights under Article 52(1) of the Charter: A Sisyphean Task?' (*supra* Chapter VIII. note 1), pp. 662–667, who gives a detailed list of CJEU cases on Article 52 (1) of the Charter based on sophisticated criteria; see also M. Brkan, 'The Concept of Essence of Fundamental Rights in the EU Legal Order: Peeling the Onion to its Core'(*supra* Chapter VIII. note 28), p. 337; M. Dawson, O. Lynskey and E. Muir, 'What is the Added Value of the Concept of the "Essence" of EU Fundamental Rights?', 20 *German Law Journal* (2019), p. 768.

[39] E. Muir, 'The Horizontal Effects of Charter Rights Given Expression to in EU Legislation, from Mangold to Bauer' (*supra* Chapter VI. note 112), p. 209; See Case C-569/16 *Bauer* (*supra* Chapter VI. note 87), para. 49.

[40] K. Lenaerts, 'Limits on Limitations: The Essence of Fundamental Rights in the EU' (*supra* Chapter VIII. note 26), p. 785.

[41] Ibid.

[42] S. Peers and S. Prechal, 'Art 52 Scope and Interpretation of Rights and Principles' (*supra* Chapter VIII. note 1), para. 66; see also M. Brkan, 'The Essence of the Fundamental Rights to Privacy and Data Protection: Finding the Way Through the Maze of the CJEU's Constitutional Reasoning', 20 *German Law Journal* (2019), p. 869; M. Brkan, 'The Concept of Essence of Fundamental Rights in the EU Legal Order: Peeling the Onion to its Core' (*supra* Chapter VIII. note 28), p. 337.

detrimental to the democratic system and the constant balancing of interests in the EU.[43] It is essential that the essence of a fundamental right remains the core and does not include the shell.[44]

What is the essence of the fundamental right to data protection that must be respected when using personal data as an economic asset? It will be argued that companies could use personal data as an economic asset and do not adversely affect the essence of the fundamental right to data protection as long as data subjects have control over it.

The CJEU has so far been vague in its case law on the essence of the fundamental right to data protection.[45] In *Digital Rights Ireland*, the CJEU held that the retention of personal data in question did not 'adversely affect the essence of the fundamental right to the protection of personal data' because certain principles of data protection and data security were respected.[46]

The Court specified that these principles include technical and organisational measures to avoid 'accidental or unlawful destruction, accidental loss or alteration of the data'.[47] In *Ligue des droits humains*, the CJEU also argued that interferences did not 'adversely affect' the essence of the fundamental rights enshrined in Articles 7 and 8 of the Charter because rules were laid down governing the transfer, processing and retention of personal data as well as rules intended to ensure the security, confidentiality and integrity of personal data and to protect them against unlawful access and processing.[48] The CJU also held that an interference did not undermine the essence of the fundamental rights enshrined in Articles 7 and 8 of the Charter because it 'must fully meet the requirements arising from the GDPR'.[49] Moreover, 'the requirement that processing of sensitive data be "strictly necessary" entails particularly strict checking as to whether the principle of data minimization is observed'.[50]

From this reasoning, one could infer that the essence of the fundamental right to data protection is data security and that certain technical and organisational measures exclude an interference with its essence. Thus, the economic exploitation of personal data described in Chapter III. 2. could respect the essence of the

---

[43] K. Lenaerts, 'Limits on Limitations: The Essence of Fundamental Rights in the EU' (*supra* Chapter VIII. note 26), p. 793.

[44] See also M. Brkan, 'The Concept of Essence of Fundamental Rights in the EU Legal Order: Peeling the Onion to its Core' (*supra* Chapter VIII. note 28), p. 368.

[45] M. Brkan, 'The Essence of the Fundamental Rights to Privacy and Data Protection: Finding the Way Through the Maze of the CJEU's Constitutional Reasoning' (*supra* Chapter VIII. note 42), p. 878.

[46] Case C-293/12 *Digital Rights Ireland* (*supra* Chapter II. note 130), para. 40.

[47] Ibid.

[48] Case C-817/19 *Ligue des droits humains* (*supra* Chapter VIII. note 5), para. 120.

[49] Joined Cases C-37/20 and C-601/20 *Luxembourg Business Registers* (*supra* Chapter VIII. note 5), para. 53.

[50] Case C-205/21 *Ministerstvo na vatreshnite raboti* (*supra* Chapter VII. note 116), para. 125.

fundamental right to data protection if a certain level of data security is ensured. Such an interpretation of the essence of the fundamental right to data protection would be misguided, as it would reduce the essence to a minimum standard and the hurdle to respect the essence would be too low.[51] Moreover, if the essence of the fundamental right to data protection were reduced to a minimum standard, its purpose and role would be undermined in the constitutional landscape.[52]

The question of whether any interference with the elements set out in Article 8 (2) of the Charter, i.e. purpose limitation, fairness, right of access and right to rectification (see in detail, Chapter VII above), constitutes an interference with the essence of the fundamental right to data protection can also be answered in the negative.[53] As *Brkan* rightly argues, interference with the essence requires that the right can no longer be exercised or is undermined as such.[54] Below this threshold, interference with the elements laid down in Article 8 (2) of the Charter is an ordinary interference with the right to data protection, but not with its essence.[55] This means that unfair economic exploitation of personal data, such as described in Chapter VII 3., can be an unjust interference with the fundamental right to data protection, but is not necessarily a violation of the essence of that fundamental right.

Control is the essence of the right to data protection.[56] Control is to be interpreted broadly in this context and is intended to give data subjects autonomy and disposition power over their personal data.[57] This concept of control pursues a liberal worldview in which data subjects can actively decide whether to grant and even participate in the use of their personal data or to restrict or prohibit the processing of their personal data.[58] Control as the essence of the right to data protection is supported by the fact that Article 8 of the Charter aims to balance power asymmetries, which is clear from its structure, i.e. rights for data subjects and obligations for data controllers.[59] As shown in Chapter III. 2., a few com-

---

[51] M. Brkan, 'The Essence of the Fundamental Rights to Privacy and Data Protection: Finding the Way Through the Maze of the CJEU's Constitutional Reasoning' (*supra* Chapter VIII. note 42), p. 879.

[52] Ibid.

[53] Ibid, p. 881.

[54] Ibid.

[55] Ibid.

[56] See also D. Clifford and J. Ausloos, 'Data Protection and the Role of Fairness', (*supra* Chapter VII. note 77), p. 144.

[57] Ibid, p. 145.

[58] C. Lazaro and D. Le Métayer, 'Control over Personal Data: True Remedy or Fairy Tale?' (*supra* Chapter I. note 15), p. 9.

[59] D. Clifford and J. Ausloos, 'Data Protection and the Role of Fairness' (*supra* Chapter VII. note 77), p. 144; see also C. Lazaro and D. Le Métayer, 'Control over Personal Data: True Remedy or Fairy Tale?' (*supra* Chapter I. note 15), p. 10; Lynskey describes data protection as 'a positive right to reduce information and power asymmetries', see O. Lynskey, 'Deconstructing Data Protection: The "Added-Value" Of A Right To Data Protection in the EU Legal Order' (*supra* Chapter IV. note 190), p. 592; O. Lynskey, 'Delivering Data Protection: The Next Chapter'(*supra* Chapter VII. note 14), p. 82.

panies have stored vast amounts of personal data, generate knowledge and money, and get more power. By granting data subjects control over their personal data, these companies cannot handle personal data as they please and a balance is sought. Furthermore, control over personal data allows data subjects to control the persona they portray in society, free from inappropriate or unwarranted distortion or misrepresentation.[60] As *Ferretti* states, control is also a fundamental value for data subjects to preserve and develop their persona in such a way that they can participate fully in society.[61] Moreover, the fundamental right to data protection aims to strengthen trust in data processing, and as more and more personal data is processed and also used economically, trust can be strengthened if the data is under the control of the data subjects.[62] In addition, the numerous EU policy documents that explicitly highlight control over personal data also support the notion of control as the essence of the right to data protection enshrined in Article 8 of the Charter.[63]

Control, just like the fundamental right to data protection as such, is not guaranteed without limits.[64] To refer back to the judgment of the German Federal Constitutional Court: individuals do not have a right in the sense of absolute, unrestricted control over 'their' personal data, but rather it must be considered in its function and interaction in society.[65] Consequently, companies can use personal data as an economic asset and do not adversely affect the essence of the fundamental right to data protection as long as data subjects have control over it. As argued in Chapter IV. 3., data subjects have control over their personal data to the extent that their data rights are respected.

In order to respect and strengthen the essence of the fundamental right to data protection, some authors suggest that individuals should collaborate, as this puts them in a stronger position to decide and control the provision of their personal data.[66] Data cooperatives are proposed in this context, empowering individuals by collectively using their personal data.[67] It is hoped that this will not only lead to synergy effects in the collective use of knowledge, but also to a stronger negotiating position in order to obtain better services and conditions from companies for the members of the data cooperatives.[68] The current situation, in which per-

---

[60] F. Ferretti, 'Data protection and the legitimate interest of data controllers: Much ado about nothing or the winter of rights?' 51 *Common Market Law Review* (2014), p. 850.

[61] Ibid.

[62] Ibid.

[63] C. Lazaro and D. Le Métayer, 'Control over Personal Data: True Remedy or Fairy Tale?' (*supra* Chapter I. note 15), p. 16.

[64] D. Clifford and J. Ausloos, 'Data Protection and the Role of Fairness' (*supra* Chapter VII. note 77), p. 145.

[65] See BVerfG, I BvR 209/83 (*supra* Chapter IV. note 187), para. 148.

[66] C. Lazaro and D. Le Métayer, 'Control over Personal Data: True Remedy or Fairy Tale?' (*supra* Chapter I. note 15), p. 27.

[67] A. Pentland, A. Lipton and T. Hardjono, *Building The New Economy – Data as Capital* (MIT Press, 2021), p. 21.

[68] Ibid, p. 31.

sonal data of individuals is used as an economic asset without giving enough value back to them, can be compared to the situation of workers in the late 1800s and early 1900s, as a result of which trade unions were formed.[69] Thus, data subjects themselves could also use personal data as an economic asset and act as data brokers themselves, provided that they retain control over the personal data. Data subject rights, privacy-friendly technologies and collaboration among data subjects are essential to ensure that an individual's control over personal data does not remain a mere fantasy.[70]

d) Objectives of general interest or protection of the rights and freedoms of others

Limitations to Charter rights must also 'meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others'.[71] The objectives of general interest include those of Article 3 TEU (i.e. peace, freedom, equality etc.) as well as other interests protected by primary law.[72] For example, the CJEU held that the processing and storage of fingerprints to prevent passport falsification and illegal entry into the EU,[73] data retention to prevent, detect, investigate and prosecute terrorist offences and serious crime,[74] or the general public's access to information in order to prevent money laundering and terrorist financing are all objectives serving the general interest that are capable of justifying even serious interferences with the fundamental right enshrined in Article 8 of the Charter.[75] Nevertheless, there must be an appropriate balancing of the general interest objective and the fundamental right in question.[76] Whether the current use of personal data as an economic asset contributes

---

[69] Ibid, p. 81.

[70] C. Lazaro and D. Le Métayer, 'Control over Personal Data: True Remedy or Fairy Tale?' (*supra* Chapter I. note 15), p. 34.

[71] See Article 52 (1) of the Charter.

[72] Explanations relating to the Charter of Fundamental Rights [2007] OJ C303/32; S. Peers and S. Prechal, 'Art 52 Scope and Interpretation of Rights and Principles' (*supra* Chapter VIII. note 1), para. 48; A. Schwerdtfeger, 'Artikel 52 Tragweite und Auslegung der Rechte und Grundsätze' (*supra* Chapter VIII. note 2), para. 35.

[73] Case C-291/12 *Schwarz* (*supra* Chapter II. note 131), paras. 36–38.

[74] Case C-817/19 *Ligue des droits humains* (*supra* Chapter VIII. note 5), para. 122.

[75] Joined Cases C-37/20 and C-601/20 *Luxembourg Business Registers* (*supra* Chapter VIII. note 5), para. 59.

[76] Joined Cases C-37/20 and C-601/20 *Luxembourg Business Registers* (*supra* Chapter VIII. note 5), para. 64; Case C-817/19 *Ligue des droits humains* (*supra* Chapter VIII. note 5), para. 115; Case C-184/20 *Vyriausioji tarnybinės etikos komisija* (*supra* Chapter IV. note 295), para. 98; Case C-140/20 *Commissioner of An Garda Síochána*, EU:C:2022:258, para. 52; Joined Cases C-511/18, C-512/18 and C-520/18 *La Quadrature du Net and Others* (*supra* Chapter VI. note 174), para. 130; Case C-293/12 *Digital Rights Ireland* (*supra* Chapter II. note 130), para. 52; Case C-92/09 *Volker und Markus Schecke und Eifert* (*supra* Chapter II. note 184), paras. 76, 77 and 86; Case C-73/07 *Satakunnan Markkinapörssi und Satamedia* (*supra* Chapter II. note 44), para. 56.

to the objective of economic growth or technological progress of Article 3 TEU is debatable. However, the proposed data cooperatives could contribute to economic growth, as data could be used by the community and its individuals for neighbourhood planning and making neighbourhoods more appealing.[77] More attractive neighbourhoods attract more people, which leads to diverse amenities and economic growth.[78]

In addition, the rights and freedoms of others must be protected, which covers collisions of fundamental rights.[79] Thus, if necessary, the fundamental rights of one can justify a limitation of a fundamental right of the other.[80] Consequently, there are numerous possibilities in which restrictions are legitimate.[81] The balancing of different interests and fundamental rights when using personal data as an economic asset will be discussed in Chapter VIII. 2. below.

e) Proportionality

In addition, limitations must always be proportionate.[82] The principle of proportionality is one of the general principles of Union law.[83] It serves to strike a fair balance between colliding fundamental rights or interests.[84] The principle of proportionality indicates some intersections with the essence of a fundamental right, but there are constellations in which the essence of a fundamental right is respected but the measure is not proportionate.[85] Likewise, *Brkan* argues for a conceptual distinction between proportionality and essence, since in the case of proportionality a justificatory argument exists, but the interference might be disproportionate, whereas in the case of interference with the essence there is never a justificatory argument.[86] Subsequently, she advocates a distinction be-

---

[77] A. Pentland, A. Lipton and T. Hardjono, *Building The New Economy – Data as Capital* (*supra* Chapter VIII. note 67), p. 23.

[78] Ibid, p. 25.

[79] A. Schwerdtfeger, 'Artikel 52 Tragweite und Auslegung der Rechte und Grundsätze' (*supra* Chapter VIII. note 2), para. 36; H. Krämer, 'Art. 52 Tragweite und Auslegung der Rechte und Grundsätze' (*supra* Chapter VII. note 60), para. 47.

[80] A. Schwerdtfeger, 'Artikel 52 Tragweite und Auslegung der Rechte und Grundsätze' (*supra* Chapter VIII. note 2), para. 36.

[81] S. Peers and S. Prechal, 'Art 52 Scope and Interpretation of Rights and Principles' (*supra* Chapter VIII. note 1), para. 50.

[82] See Article 52 (1) of the Charter.

[83] Case C-384/17 *Link Logistik N&N*, EU:C:2018:810, para. 40; A. Schwerdtfeger, 'Artikel 52 Tragweite und Auslegung der Rechte und Grundsätze' (*supra* Chapter VIII. note 2), para. 37; C. G. H. Riedel, *Die Grundrechtsprüfung durch den EuGH* (Mohr Siebeck, 2020), p. 141.

[84] A. Schwerdtfeger, 'Artikel 52 Tragweite und Auslegung der Rechte und Grundsätze' (*supra* Chapter VIII. note 2), para. 38.

[85] K. Lenaerts, 'Limits on Limitations: The Essence of Fundamental Rights in the EU' (*supra* Chapter VIII. note 26), p. 786.

[86] M. Brkan, 'The Concept of Essence of Fundamental Rights in the EU Legal Order: Peeling the Onion to its Core' (*supra* Chapter VIII. note 28), p. 360.

tween interference with the essence of a fundamental right and a 'serious' or 'particularly serious interference' with this right.[87]

The CJEU has repeatedly held that the principle of proportionality requires 'that the measures adopted do not exceed the limits of what is appropriate and necessary in order to attain the legitimate objectives pursued […]'.[88] Proportionality also requires that 'no less onerous method than that obligation […] itself [is] capable of realising those objectives as efficiently'.[89] This is reminiscent of the requirement of necessity in the German-speaking legal area.[90] In many cases, it is debatable whether the use of personal data as an economic asset is actually necessary or proportionate. The practices relating to behavioural advertising described in Chapter III. 2. b) are certainly not the least intrusive means of advertising.[91] Moreover, the large-scale economic use of personal data also is disproportionate, as targeted advertising would be possible without it.[92]

2. Balancing fundamental rights when using personal data as an economic asset

It is not unknown to the law that aspects of personality, e.g. the right to one's own image, can be sold or commercialised, as described in Chapter IV. Furthermore, the right to the protection of personal data is not an absolute right and must be viewed in terms of its function in society.[93] It is therefore possible that the right to the protection of personal data is subject to restrictions and interferences. Consequently, not only the data subject but also third parties (i.e. companies or individuals of the data economy) are in principle not prevented from using personal data as an economic asset.[94] Rather, it is power and information asym-

[87] Ibid; see also C. G. H. Riedel, *Die Grundrechtsprüfung durch den EuGH* (*supra* Chapter VIII. note 83), p. 341, who comes to the conclusion that the CJEU differentiates between proportionality and essence.

[88] Case C–473/16 F, EU:C:2018:36, para. 56; See also Joined Cases C–37/20 and C–601/20 Luxembourg Business Registers (*supra* Chapter VIII. note 5), para. 65; Case C–817/19 Ligue des droits humains (*supra* Chapter VIII. note 5), para. 117.

[89] Case C–73/16 *Puškár* (*supra* Chapter VII. note 115), para. 68.

[90] A. Schwerdtfeger, 'Artikel 52 Tragweite und Auslegung der Rechte und Grundsätze' (*supra* Chapter VIII. note 2), para. 39.

[91] F. Zuiderveen Borgesius, 'Legal basis for behavioural targeting' (*supra* Chapter VII. note 76), p. 168.

[92] Ibid.

[93] Case C-92/09 *Volker und Markus Schecke und Eifert* (*supra* Chapter II. note 184), para. 48; T. Riesz, 'Art 8 GRC. Schutz personenbezogener Daten' (*supra* Chapter VI. note 27), para. 60; M. Tzanou, 'Data protection as a fundamental right next to privacy? "Reconstructing" a not so new right' (*supra* Chapter IV. note 187), p. 98.

[94] Datenethikkommission, *Gutachten der Datenethikkommission*, p. 104; González Fuster and Gellert describe data protection law as 'enabler of personal data processing', see G. González Fuster and R. Gellert, 'The fundamental right to data protection in the European Union: in search of an uncharted right' (*supra* Chapter VIII. note 7), p. 78.

metries that must be prevented by data protection law.[95] The right to protection of personal data may be limited if necessary to protect the rights and interests of others.

If conflicting fundamental rights are at issue, the CJEU held that a fair balance must be struck between differing rights enshrined in the Charter.[96] When the right to data protection comes into interplay with other fundamental rights and interests, a balancing test for the interpretation and application of Article 8 of the Charter is required.[97] Data controllers can invoke their fundamental rights, such as freedom of expression (Article 11 of the Charter) and freedom to conduct a business (Article 16 of the Charter), for the economic use of personal data.[98] In balancing these conflicting fundamental rights, it is not a matter of enforcing one fundamental rights at the expense of another, but rather of practical concordance to ensure that all fundamental rights can be exercised.[99] In this respect *Brkan* warns that a predominance of data protection within the EU could upset the balance of fundamental rights protection and therefore urges for an appropriate balance between data protection and other fundamental rights.[100] Balancing between fundamental rights has been described as 'a difficult task'.[101] Some of the rights and interests that individuals might pursue when using personal data as an economic asset and with which the right to data protection interacts are outlined hereafter. The structure follows the Fundamental Rights Agency's concise overview.[102]

---

[95] O. Lynskey, 'Delivering Data Protection: The Next Chapter' (*supra* Chapter VII. note 14), p. 82; M. von Grafenstein, 'Refining the Concept of the Right to Data Protection in Article 8 ECFR – Part II' (*supra* Chapter VII. note 31), p. 194.

[96] Case C-70/10 *Scarlet* (*supra* Chapter II. note 130), para. 45; Case C-275/06 *Promusicae* (*supra* Chapter II. note 135), para. 68; Case C-580/13 *Coty Germany* (*supra* Chapter VI. note 85), para. 34; H.D. Jarass, 'Die Bedeutung der Unionsgrundrechte unter Privaten' (*supra* Chapter VI. note 76), p. 324.

[97] European Union Agency for Fundamental Rights and Council of Europe (eds.), *Handbook on European data protection law* (*supra* Chapter II. note 26), p. 53; Case C-275/06 *Promusicae* (*supra* Chapter II. note 135), para. 68.

[98] A. Roßnagel, 'Kein "Verbotsprinzip" und kein "Verbot mit Erlaubnisvorbehalt" im Datenschutzrecht' (*supra* Chapter VI. note 198), p. 3.

[99] Ibid.

[100] M. Brkan, 'The Unstoppable Expansion of the EU Fundamental Right to Data Protection: Little Shop of Horrors?' (*supra* Chapter VII. note 40), p. 841.

[101] M. Tzanou, 'Balancing Fundamental Rights: United in Diversity? Some Reflections on the Recent Case Law of the European Court of Justice on Data Protection', 6 *Croatian Yearbook of European Law & Policy* (2010), p. 63.

[102] See Explanations relating to the Charter of Fundamental Rights [2007] OJ C303/21.

a) Interaction with the right to freedom of expression and information

The right to data protection frequently interacts with the right to freedom of expression and information, which is laid down in Article 11 of the Charter. Individuals and companies could claim that they use personal data as an economic asset to hold an opinion and/or to receive and impart information and ideas. On the other hand, individuals might invoke their right to data protection, for example to have their personal data deleted. Article 85 GDPR addresses this interaction and states that the right to protection of personal data should be reconciled with the right to freedom of expression and information. The ECHR can also be used for interpretation pursuant to Article 52 (3) of the Charter, as Article 11 of the Charter corresponds to Article 10 of the ECHR.[103] A number of judgments of the European courts can be used as a guideline for balancing the right to data protection and the right to freedom of expression.[104]

In *Satakunnan Markkinapörssi und Satamedia*, the CJEU addressed the relationship between the right to protection of personal data (then still under the guise of the right to privacy) and the right to freedom of expression. In this case, a company had disseminated information on 1.2 million people via text message service.[105] Users were charged € 2 for this service.[106] The information comprised surname, given name, earned and unearned income and tax data.[107] The company argued that this service was solely for journalistic purposes and was therefore covered by the freedom of expression and information.[108] The CJEU first emphasised that in a democratic society, the right to freedom of expression and the related concept of journalism must be interpreted broadly.[109] In order to create a balance between the right to freedom of expression and the right to privacy, limitations in relation to the protection of personal data must be strictly necessary.[110] The CJEU held that the data processing activities concerned 'may be classified as "journalistic activities" if their object is the disclosure to the public of information, opinions or ideas, irrespective of the medium which is used to transmit them'.[111] Furthermore, remarkably, the CJEU stated that these journalistic

---

[103] European Union Agency for Fundamental Rights and Council of Europe (eds.), *Handbook on European data protection law* (*supra* Chapter II. note 26), p. 54.

[104] C. Docksey, 'Four fundamental rights: finding the balance' (*supra* Chapter VII. note 3), p. 207.

[105] Case C-73/07 *Satakunnan Markkinapörssi und Satamedia* (*supra* Chapter II. note 44), para. 26.

[106] Ibid, para. 29.

[107] Ibid, para. 26.

[108] European Union Agency for Fundamental Rights and Council of Europe (eds.), *Handbook on European data protection law* (*supra* Chapter II. note 26), p. 55.

[109] Case C-73/07 *Satakunnan Markkinapörssi und Satamedia* (*supra* Chapter II. note 44), para. 56.

[110] Ibid.

[111] Ibid, para. 61.

activities 'are not limited to media undertakings and may be undertaken for profit-making purposes'.[112]

Following this line of argument, companies could sell personal data to the public. A large amount of personal data could be traded. Thereby, personal data would be used as an economic asset under the guise of freedom of expression and journalism. This approach is not convincing.[113] Consequently, and rightfully so, the ECtHR in the same case rejected the dissemination of the personal data, as the mass distribution of the raw data did not serve the public interest and did not fall under the privilege of journalistic activities.[114] Thus, the right to protection of the data subjects' personal data outweighed the right to freedom of expression of the company.

In *Google Spain and Google*, the CJEU argued that an interference with the fundamental right to data protection could be justified by the public's interest in having access to the personal data or information.[115] When balancing the data subjects' rights against the interests of internet users, the position of the data subject in public life must be taken into account.[116] Information on persons in the public eye may be in the public interest and hence the position of the data subject as a public figure could justify the interference with the right to protection of personal data enshrined in Article 8 of the Charter.[117] In contrast, sensitive data can lead to the right to protection of personal data outweighing the public's interest in access to information.[118] In the specific case, the balancing test was applied in favour of the data subject, as the right to data protection outweighed both the economic interests of the search engine operator and the right of access to information of the public.[119] Thus, the personal data concerned could not be economically exploited by Google in this case.

This judgment illustrates that several factors must be considered when balancing fundamental rights. The fact that the status of a data subject as a public figure may be decisive for the right to freedom of expression to override the right to protection of personal data has been decided by the ECtHR on several occasions. In one case, the publication of an article about the arrest of an actor was covered

---

[112] Ibid.

[113] See also M. Tzanou, 'Balancing Fundamental Rights: United in Diversity? Some Reflections on the Recent Case Law of the European Court of Justice on Data Protection' (*supra* Chapter VIII. note 101), p. 67.

[114] ECtHR, *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland*, Judgment of 27 June 2017, Application No. 931/13, paras. 167–178.

[115] Case C-131/12 *Google Spain and Google* (*supra* Chapter IV. note 283), para. 97.

[116] Ibid.

[117] European Union Agency for Fundamental Rights and Council of Europe (eds.), *Handbook on European data protection law* (*supra* Chapter II. note 26), p. 57.

[118] Case C-460/20 *Google* (*supra* Chapter VI. note 174), para. 62; Case C-131/12 *Google Spain and Google* (*supra* Chapter IV. note 283), para. 81; see, by analogy, Case C-184/20 *Vyriausioji tarnybinės etikos komisija* (*supra* Chapter IV. note 295), para. 111.

[119] Case C-131/12 *Google Spain and Google* (*supra* Chapter IV. note 283), para. 99.

by Article 10 of the ECHR, as the event were in the public interest, the actor was a well-known public figure and the information was accurate.[120] An article about an alleged child of Prince Albert of Monaco was also an exercise of the right to freedom of expression, as Prince Albert is a public figure and a possible heir to the throne is in the public interest.[121] In another case, a German singer and producer had to accept a humorous advertising campaign using his first name without his consent, as the campaign referred to him, a public figure, and events in the public interest.[122] These judgments illustrate that personal data can be used commercially and as an economic asset, provided that the data subject is a public figure and there is a public interest in it. In these constellations, personal data can be used as an economic asset because the right to freedom of expression overrides the right to data protection.

There are also constellations, in which the right to freedom of expression and the right to data protection do not oppose, but support each other.[123] In *Digital Rights Ireland*, the CJEU held that the general retention of communication data does not respect the right to data protection because, the Court argued among other reasons, individuals may feel that their lives are under constant surveillance.[124] Furthermore, the retention of data could have an impact on the use of electronic communications and thus on the exercise of the right to freedom of expression under Article 11 of the Charter.[125] Thus, by preventing limitless data retention and surveillance, data protection law ensures the exercise of the right to freedom of expression.[126]

Surveillance has long ceased to take place at the state level, as was the case in *Digital Rights Ireland*. As shown in Chapter III. 2., companies have started to collect, analyse and economically exploit user data via internet usage, social media usage and smart homes. The user data collected goes beyond what governments typically can collect. Since the collection of personal data is targeted and

---

[120] European Union Agency for Fundamental Rights and Council of Europe (eds.), *Handbook on European data protection law* (*supra* Chapter II. note 26), p. 58, referring to ECtHR, *Axel Springer AG v. Germany*, Judgment of 7 February 2012, Application No. 39954/08.

[121] European Union Agency for Fundamental Rights and Council of Europe (eds.), *Handbook on European data protection law* (*supra* Chapter II. note 26), p. 57, referring to ECtHR, *Coudec and Hachette Filipacchi Associés v. France*, Judgment of 10 November 2015, Application No. 40454/07.

[122] European Union Agency for Fundamental Rights and Council of Europe (eds.), *Handbook on European data protection law* (*supra* Chapter II. note 26), p. 57, referring to ECtHR, *Bohlen v. Germany*, Judgment of 19 February 2015, Application No. 53495/09.

[123] C. Docksey, 'Four fundamental rights: finding the balance' (*supra* Chapter VII. note 3), p. 207; European Union Agency for Fundamental Rights and Council of Europe (eds.), *Handbook on European data protection law* (*supra* Chapter II. note 26), p. 61.

[124] Case C-293/12 *Digital Rights Ireland* (*supra* Chapter II. note 130), para. 37.

[125] Ibid, para. 28.

[126] C. Docksey, 'Four fundamental rights: finding the balance' (*supra* Chapter VII. note 3), p. 207; European Union Agency for Fundamental Rights and Council of Europe (eds.), *Handbook on European data protection law* (*supra* Chapter II. note 26), p. 62.

systematic, it is akin to surveillance for the market capitalisation of user data, which is why *Zuboff* chooses the term 'surveillance capitalism'.[127] Given the similarities of 'surveillance capitalism' to data retention in *Digital Rights Ireland*, it can be concluded that data subjects could assert both their right to data protection and their right to freedom of expression.

b) Interaction with the right to property

In *Scarlet* and *Sabam*, the CJEU dealt with the balance between the freedom to conduct a business and the right to intellectual property.[128] The protection of one fundamental right must be balanced against the protection of the other fundamental right.[129] The essence of the fundamental rights involved must not be violated under any circumstances.[130] Thus, in the *Alemo-Herron* judgment of the CJEU, it was decisive to respect the essence of the rights concerned.[131]

Furthermore, the appropriate balance between the conflicting fundamental rights depends not only on the fundamental rights of the two parties to a dispute, but also on the fundamental rights of third parties.[132] This was pointed out by the CJEU in its *SABAM* judgment, in which a management company invoked their right to property laid down in Article 17 of the Charter and a hosting service provider invoked the protection of the freedom to conduct a business according to Article 16 of the Charter.[133] The management company (SABAM) argued that the hosting service provider made use of works in SABAM's repertoire without their consent and requested that the hosting service provider be ordered to cease unlawfully making available works from SABAM's repertoire.[134]

In the context of the necessary balance, the fundamental rights of internet users, such as the protection of personal data enshrined in Article 8 of the Charter

---

[127] See S. Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (*supra* Chapter I. note 3).

[128] Case C-70/10 *Scarlet* (*supra* Chapter II. note 130), para. 46; Case C-360/10 *SABAM* (*supra* Chapter VI. note 85), para. 44; H.D. Jarass, 'Die Bedeutung der Unionsgrundrechte unter Privaten' (*supra* Chapter VI. note 76), p. 324.

[129] Case C-360/10 *SABAM* (*supra* Chapter VI. note 85), para. 42; Case C-580/13 *Coty Germany* (*supra* Chapter VI. note 85), para. 34; H.D. Jarass, 'Die Bedeutung der Unionsgrundrechte unter Privaten' (*supra* Chapter VI. note 76), p. 324.

[130] Case C-70/10 *Scarlet* (*supra* Chapter II. note 130), paras. 48 and 49; Case C-360/10 *SABAM* (*supra* Chapter VI. note 85), paras. 46 and 47; Case C-580/13 *Coty Germany* (*supra* Chapter VI. note 85), para. 35; H.D. Jarass, 'Die Bedeutung der Unionsgrundrechte unter Privaten' (*supra* Chapter VI. note 76), p. 325.

[131] Case C-426/11 *Alemo-Herron* (*supra* Chapter VI. note 85), para. 35; H.D. Jarass, 'Die Bedeutung der Unionsgrundrechte unter Privaten' (*supra* Chapter VI. note 76), p. 325.

[132] H.D. Jarass, 'Die Bedeutung der Unionsgrundrechte unter Privaten' (*supra* Chapter VI. note 76), p. 325.

[133] Case C-360/10 *SABAM* (*supra* Chapter VI. note 85), para. 44; H.D. Jarass, 'Die Bedeutung der Unionsgrundrechte unter Privaten' (*supra* Chapter VI. note 76), p. 325.

[134] Case C-360/10 *SABAM* (*supra* Chapter VI. note 85), paras. 18 and 20.

and the freedom of information enshrined in Article 11 of the Charter, must also be taken into account, as the CJEU held.[135] The CJEU stated that an injunction made against a hosting service provider which requires it to install the contested filtering system 'would involve the identification, systematic analysis and processing of information connected with the profiles created on the social network by its users'.[136] Based on the balancing of fundamental rights, the injunction was rejected.[137]

Likewise, the CJEU held in *Promusicae* that the right to intellectual property must be reconciled with the right to data protection.[138] *Promusicae* requested that *Telefónica*, a company that provides Internet access, disclose the names and addresses of certain persons who allegedly exchanged music files for which the copyright and licensing rights were held by *Promusicae*.[139] The CJEU emphasised that the principle of proportionality in particular must be considered when balancing the different fundamental rights.[140]

However, companies and individuals will most likely not be able to establish intellectual property rights to personal data of data subjects that are commercially exploited. The remarks of Chapter IV. 2. c) can be used again for this argument. One difference between works protected by intellectual property and personal data is that these works require creative input and financial as well as time investment, while personal data is often a by-product.[141] Moreover, personal data will rarely be an original, individual creation.[142] In order to use personal data as an economic asset, companies do not create original, novel creations, but aggregate them into quantitative data sets. In addition, one reason for protecting intellectual property is that it can still be commercially released to the public, while personal data usually has an internal and not an external purpose.[143] Furthermore, traditional value chains have changed in the age of digitisation and

---

[135] Ibid, para. 48; H.D. Jarass, 'Die Bedeutung der Unionsgrundrechte unter Privaten' (*supra* Chapter VI. note 76), p. 325.

[136] Case C-360/10 *SABAM* (*supra* Chapter VI. note 85), para. 49.

[137] Ibid, para. 52.

[138] Case C-275/06 *Promusicae* (*supra* Chapter II. note 135), para. 63.

[139] Ibid, para. 30.

[140] Ibid, para. 68.

[141] I. Stepanov, 'Introducing a property right over data in the EU: the data producer's right – an evaluation' (*supra* Chapter IV. note 49), p. 78; A. Schmid, K.-J. Schmidt and H. Zech, 'Rechte an Daten zum Stand der Diskussion' (*supra* Chapter IV. note 3), p. 630; M. Grützmacher, 'Dateneigentum – ein Flickenteppich' (*supra* Chapter IV. note 8), p. 488; H. Zech, 'Daten als Wirtschaftsgut – Überlegungen zu einem Recht des Datenerzeugers' (*supra* Chapter IV. note 4), p. 141.

[142] C. Peschel and S. Rockstroh, 'Big Data in der Industrie – Chancen und Risiken neuer datenbasierter Dienste' (*supra* Chapter IV. note 16), p. 572; F. Schuster and S. Hunzinger, 'Vor- und nachvertragliche Pflichten beim IT-Vertrag – Teil II: Nachvertragliche Pflichten' (*supra* Chapter IV. note 18), p. 279.

[143] I. Stepanov, 'Introducing a property right over data in the EU: the data producer's right – an evaluation' (*supra* Chapter IV. note 49), p. 78.

the purpose of copyright is not necessarily applicable to the personal data economy.[144] Similarly, Chapters IV. 1. a) and b) indicated that there are currently no property rights in personal data and proposals to create property rights in personal data are not convincing. For these reasons, the right to (intellectual) property of personal data as an economic asset is unlikely to ever outweigh the right to data protection of data subjects.

c) Interaction with economic interests

Chapter III. described in detail how companies use, share and derive value from personal data. The Fundamental Rights Agency rightly points out that, as a result from these practices, companies might perceive data protection rules as burdensome and restrictive of their economic interests.[145] Therefore, data protection law interacts with economic interests and the question arises whether economic interests, i.e. the right to freedom to conduct a business set out in Article 16 of the Charter, can restrict the fundamental right to data protection.[146]

Some authors argue that Article 9 (1) GDPR should be interpreted restrictively in the case of 'incidentally' processed sensitive data in order to ensure an appropriate balance between the right to freedom to conduct a business and the right to data protection.[147] They state that more and more areas of life are becoming the subject of data processing activities and thus sensitive data are coincidentally being processed as well, but in which data controllers have no interest and therefore do not exploit them.[148] They claim that the prohibition of data processing in these cases should only exist to the extent that data controllers exploit the sensitive information of the special categories of personal data.[149] This position is not to be supported. The example of Chapters III. 3. and VII. 4. b) show that sensitive data are indeed processed and used deliberately and not just coincidentally, as they are among the most valuable personal data. Furthermore, the focus should be on the data processing per se and not on whether the sensitive content of personal data is actually exploited. This would lead to legal uncertainty, as in most cases the actual use of personal data is not transparent for data subjects in the digital economy. It is even less transparent which personal data are indeed exploited and which are not. The mere intention to process personal data should trigger the application of data protection provisions.[150]

---

[144] A. Duisberg, 'Datenhoheit und Recht des Datenbankherstellers – Recht am Einzeldatum vs. Rechte an Datensammlungen' (*supra* Chapter IV. note 16), p. 18.

[145] European Union Agency for Fundamental Rights and Council of Europe (eds.), *Handbook on European data protection law* (*supra* Chapter II. note 26), p. 68

[146] Ibid.

[147] T. Britz, M. Indenhuck and T. Langerhans, 'Die Verarbeitung "zufällig" sensibler Daten', 11 *ZD – Zeitschrift für Datenschutz* (2021), p. 563.

[148] Ibid, p. 561.

[149] Ibid, p. 563.

[150] M. von Grafenstein, 'Refining the Concept of the Right to Data Protection in Article 8 ECFR – Part III' (*supra* Chapter VI. note 192), p. 384.

With that in mind, one of the core principles of EU data protection law, as described multiple times in this work, is to ensure data subjects' control over their personal data and that its aim is to address the imbalance between companies that process vast amounts of personal data and individuals, who do not have an oversight of the data processing activities.[151] The CJEU has stated that a fair balance must be struck when balancing economic interests and the fundamental right to data protection enshrined in Article 8 of the Charter.[152] The Court held, as already mentioned in Chapter VII. 5. b) in relation to legitimate interest, that in principle the economic interests in data processing do not override the fundamental right to data protection and that an interference with the fundamental right to data protection cannot be justified by mere economic interests of a search engine operator.[153]

In *Manni*, Mr. Manni requested that his personal data be deleted from a public commercial register.[154] In view of the importance of the legitimate aim pursued by the register, the CJEU held that Mr. Manni was not entitled to have his personal data deleted, that economic interests of third parties in public and private limited liability companies were worth protecting, that the personal data were necessary for the establishment and intensification of business relations and that entry into the register would ensure legal certainty and fair trading.[155] These economic interests thus outweighed Mr. Manni's rights under data protection law.[156] Considering these two judgments, a case-by-case decision must be made when balancing economic interests and the fundamental right to data protection.[157]

3. Relationship to rights provided for in the Treaties

Article 52 (2) of the Charter stipulates that 'rights recognised by this Charter for which provision is made in the Treaties shall be exercised under the conditions and within the limits defined by those Treaties'. This provision was intended to ensure the identity of the corresponding rights and to preserve the *acquis*.[158] Within the scope of application of Article 52 (2) of the Charter, the CJEU rules, in principle, solely on the basis of the provisions of the Treaties.[159]

---

[151] European Union Agency for Fundamental Rights and Council of Europe (eds.), *Handbook on European data protection law* (*supra* Chapter II. note 26), p. 79.

[152] Case C-131/12 *Google Spain and Google* (*supra* Chapter IV. note 283),, para. 81.

[153] Ibid, paras. 81 and 97.

[154] Case C-398/15 *Manni* (*supra* Chapter VI. note 174), para. 26.

[155] Ibid, paras. 50–60.

[156] European Union Agency for Fundamental Rights and Council of Europe (eds.), *Handbook on European data protection law* (*supra* Chapter II. note 26), p. 80.

[157] Ibid, p. 79.

[158] A. Schwerdtfeger, 'Artikel 52 Tragweite und Auslegung der Rechte und Grundsätze' (*supra* Chapter VIII. note 2), para. 15.

[159] Ibid, para. 46.

Article 16 TFEU repeats both literally and chronologically the right to data protection enshrined in Article 8 (1) of the Charter.[160] This additional mention of the right to data protection raises questions, especially since Article 16 (1) TFEU does not provide for any limits and could become a right without limits when read together with Article 52 (2) of the Charter.[161] Accordingly, whether the right to data protection is subject to the limitation clause of Article 52 (1) or Article 52 (2) of the Charter is disputed in the literature.[162]

There are several reasons against an unlimited right to data protection and the application of Article 52 (2) of the Charter, i.e. that the right to data protection should be exercised under the conditions defined by Article 16 TFEU.[163] Firstly, it is not indicated in the text or the legislative history that Article 16 TFEU goes beyond the limits of Article 8 of the Charter and supersedes it.[164] Moreover, when it comes to the right to data protection, the CJEU does not refer to Article 16 TFEU, but applies Articles 7 and 8 of the Charter, presumably because of the distinct limitation of Article 8 thereof.[165] Furthermore, Article 52 (2) of the Charter is only intended to ensure that rights that were already provided for in the treaties before the Charter entered into force are not rendered meaningless by the Charter.[166] Article 16 was introduced chronologically after Article 8 of the Charter, as mentioned above, which is why this reason also falls short. Accordingly, the CJEU also correctly applies Article 52 (1) of the Charter to questions on the interpretation of the right to data protection.[167] Ultimately, Article 16 TFEU is an affirmation of Article 8 of the Charter.[168] On the question of which fundamen-

---

[160] T. Riesz, 'Art 8 GRC. Schutz personenbezogener Daten' (*supra* Chapter VI. note 27), para. 11.

[161] Ibid.

[162] See N. Bernsdorff, 'Artikel 8 Schutz personenbezogener Daten' (*supra* Chapter VII. note 1), para. 24; T. Kingreen, 'Art. 8 GRCh' (*supra* Chapter VII. note 28), para. 4; T. Riesz, 'Art 8 GRC. Schutz personenbezogener Daten' (*supra* Chapter VI. note 27), para. 92; H. Johlen, 'Art. 8 Schutz personenbezogener Daten'(*supra* Chapter VII. note 1), para. 38; I. Spiecker gen. Döhmann and M. Eisenbarth, 'Kommt das "Volkszählungsurteil" nun durch den EuGH? – Der Europäische Datenschutz nach Inkrafttreten des Vertrags von Lissabon', 66 *JZ – Juristen Zeitung* (2011), p. 172.

[163] See also T. Riesz, 'Art 8 GRC. Schutz personenbezogener Daten' (*supra* Chapter VI. note 27), para. 92.

[164] Ibid, para. 11.

[165] A. Schwerdtfeger, 'Artikel 52 Tragweite und Auslegung der Rechte und Grundsätze' (*supra* Chapter VIII. note 2), para. 48; T. Riesz, 'Art 8 GRC. Schutz personenbezogener Daten' (*supra* Chapter VI. note 27), para. 11.

[166] T. Kingreen, 'Art. 8 GRCh'(*supra* Chapter VII. note 28), para. 4.

[167] See Case C-746/18 *Prokuratuur* (*supra* Chapter VI. note 174); Case C-511/18 *La Quadrature du Net and others* (*supra* Chapter VI. note 174); Case C-623/17 *Privacy International* (*supra* Chapter VI. note 174); Case C-203/15 *Tele2 Sverige* (*supra* Chapter VI. note 174); Case C-291/12 *Schwarz* (*supra* Chapter II. note 131).

[168] T. Riesz, 'Art 8 GRC. Schutz personenbezogener Daten' (*supra* Chapter VI. note 27), para. 11.

tal rights requirements the use of personal data as an economic asset must respect, reference must thus be made to Articles 52 (1) and 8 of the Charter and not to Article 52 (2) of the Charter and Article 16 TFEU.[169]

4. Relationship to rights provided for by the ECHR

This chapter discusses the extent to which the ECHR can be used to address and interpret the economic use of personal data. Article 52 (3) of the Charter states that

'In so far as this Charter contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the meaning and scope of those rights shall be the same as those laid down by the said Convention. This provision shall not prevent Union law providing more extensive protection.'

The provision is central to the interpretation and application of the Charter.[170] The relationship between Article 52 (3) and Article 52 (1) of the Charter is to be decided in favour of Article 52 (1) of the Charter, whereby Article 52 (3) of the Charter may, if necessary, be used as an aid to interpretation.[171] The CJEU often applies Article 52 (1) of the Charter instead of Article 52 (3) of the Charter.[172] Furthermore, the justification for limitations of fundamental rights covered by Article 52 (3) of the Charter is also based on Article 52 (1) of the Charter.[173] Nevertheless, Article 52 (3) is an important aid to interpretation.

The reference to the ECHR reflects the fact that it was one of the main influences on the Charter.[174] The CJEU has ruled that this provision establishes a minimum standard of fundamental rights protection.[175] It is also indicated in the

---

[169] See Chapter VII. (Article 8 of the Charter) and VIII. (Article 52 (1) of the Charter) respectively.

[170] H. Krämer, 'Art. 52 Tragweite und Auslegung der Rechte und Grundsätze' (*supra* Chapter VII. note 60), para. 69.

[171] A. Schwerdtfeger, 'Artikel 52 Tragweite und Auslegung der Rechte und Grundsätze' (*supra* Chapter VIII. note 2), para. 67; H. Krämer, 'Art. 52 Tragweite und Auslegung der Rechte und Grundsätze' (*supra* Chapter VII. note 60), para. 78; by contrast, see S. Peers and S. Prechal, 'Art 52 Scope and Interpretation of Rights and Principles' (*supra* Chapter VIII. note 1), para. 213.

[172] See Case C-92/09 *Volker und Markus Schecke und Eifert* (*supra* Chapter II. note 184); Case C-291/12 *Schwarz* (*supra* Chapter II. note 131); Case C-468/10 *ASNEF* (*supra* Chapter VI. note 174); S. Peers and S. Prechal, 'Art 52 Scope and Interpretation of Rights and Principles' (*supra* Chapter VIII. note 1), para. 128; H.D. Jarass, 'Art. 52 Tragweite und Auslegung der Rechte und Grundsätze' (*supra* Chapter VIII. note 4), para. 6.

[173] Ibid.

[174] H. Krämer, 'Art. 52 Tragweite und Auslegung der Rechte und Grundsätze' (*supra* Chapter VII. note 60), para. 65.

[175] Case C-235/17 *Commission v Hungary*, EU:C:2019:432, para. 72; Case C-528/15 *Al Chodor*, EU:C:2017:213, para. 37; Case C-258/14 *Florescu*, EU:C:2017:448, para. 49; Case

Explanations to the Charter that the protection of fundamental rights enshrined in the Charter should not undermine the level of protection granted by the ECHR.[176] Moreover, the cross-reference to the ECHR includes both the Convention and the Protocols.[177] This is noteworthy as not all protocols have been ratified by all Member States.[178] In addition, the Explanations underline that ECHR rights are to be interpreted not only on the basis of the text of the Convention and the Protocols, but also on the basis of the ECtHR case-law.[179] Again, this should be understood to allow a higher standard to be set than that of the ECHR and also to allow the CJEU to interpret the ECHR in the absence of relevant case-law from the ECtHR.[180] The ECHR and the case-law of the ECtHR are of high relevance for fundamental rights laid down in the Charter.[181] The provision can be used for interpretation when the Charter serves to interpret a norm of secondary law in a vertically conforming manner, for example.[182]

According to the Explanations to the Charter, some provisions of the Charter have the same scope and meaning as the corresponding Articles of the ECHR, e.g. Article 7 corresponds to Article 8 of the ECHR, Article 10 (1) corresponds to Article 9 of the ECHR, Article 11 corresponds to Article 10 of the ECHR and Article 17 corresponds to Article 1 of the Protocol to the ECHR.[183] In the case law on Article 52 (3) of the Charter, the CJEU has established that Article 7 of the Charter is to be given the same meaning and scope as Article 8 (1) ECHR as interpreted by the ECtHR.[184]

However, Article 8 of the Charter is a structurally independent fundamental right that also covers cases that have no connection to private life.[185] As Article 8

C-492/18 PPU *TC*, EU:C:2019:108, para. 57; A. Ward, 'Art 51 – Field of Application' (*supra* Chapter VI. note 42), para. 20.

[176] Explanations relating to the Charter of Fundamental Rights [2007] OJ C303/33.

[177] Ibid.

[178] S. Peers and S. Prechal, 'Art 52 Scope and Interpretation of Rights and Principles' (*supra* Chapter VIII. note 1), para. 105.

[179] Explanations relating to the Charter of Fundamental Rights [2007] OJ C303/33.

[180] S. Peers and S. Prechal, 'Art 52 Scope and Interpretation of Rights and Principles' (*supra* Chapter VIII. note 1), para. 123.

[181] H.D. Jarass, 'Art. 52 Tragweite und Auslegung der Rechte und Grundsätze' (*supra* Chapter VIII. note 4), para. 65.

[182] H. Krämer, 'Art. 52 Tragweite und Auslegung der Rechte und Grundsätze' (*supra* Chapter VII. note 60), para. 70.

[183] Explanations relating to the Charter of Fundamental Rights [2007] OJ C303/33.

[184] Case C-400/10 PPU *McB*, EU:C:2010:582, para. 53; Case C-256/11 *Dereci and Others,* EU:C:2011:734, para. 50*;* Joined Cases C-356/11 and C-357/11 *O and S*, EU:C:2012:776, para. 76; Case C-673/16 *Coman*, EU:C:2018:385, para. 49; Case C-345/17 *Buivids* (*supra* Chapter II. note 34), para. 65; Case-419/14 *WebMindLicenses*, para. 70; Case C-129/18 *SM*, EU:C:2019:248, para. 65; Case C-78/18 *European Commission v Hungary*, EU:C:2020:476, para. 122; S. Peers and S. Prechal, 'Art 52 Scope and Interpretation of Rights and Principles' (*supra* Chapter VIII. note 1), para. 110.

[185] T. Riesz, 'Art 8 GRC. Schutz personenbezogener Daten' (*supra* Chapter VI. note 27), para. 8.

of the Charter constitutes a separate fundamental right, there is no equivalent in the ECHR and yet the case law of the ECtHR can be taken into account.[186] Firstly, the Explanations to the Charter state that Article 8 of the Charter is also based on Article 8 ECHR, which indicates the close link between the two systems.[187] Furthermore, the CJEU held that the limitations which may lawfully be imposed on the right to the protection of personal data correspond to those set out in Article 8 ECHR.[188] Accordingly, the CJEU found a substantive proximity between Articles 7 and 8 of the Charter[189] and referred to the case law of the ECtHR.[190] Generally, the CJEU reads Articles 7 and 8 of the Charter together.[191] This approach makes a clear distinction between the two fundamental rights difficult and a distinct case law on Article 8 of the Charter is essentially lacking.[192] Although this could be amended, this means that the case law of the ECtHR on Article 8 of the ECHR can also be used to interpret Article 8 of the Charter, since Articles 7 and 8 of the Charter are read together and the former corresponds to Article 8 of the ECHR. Moreover, taking into account the legislative history and the Explanations of Article 8 of the Charter, the values and contents of Article 8 ECHR are significant, even though Article 8 of the Charter is a fundamental right of its own.[193] This significance when balancing fundamental rights was illustrated in Chapter VIII. 2 above.

The ECtHR has established in its case law that the right to data protection is an essential element of the right to respect for private and family life enshrined in

---

[186] H.D. Jarass, 'Art. 8 Schutz personenbezogener Daten' (*supra* Chapter VI. note 64), para. 13.

[187] Explanations relating to the Charter of Fundamental Rights [2007] OJ C303/20; T. Riesz, 'Art 8 GRC. Schutz personenbezogener Daten' (*supra* Chapter VI. note 27), para. 8.

[188] Case C-92/09 *Volker und Markus Schecke und Eifert* (*supra* Chapter II. note 184), para. 52.

[189] Ibid, para. 47; Case C-468/10 *ASNEF* (*supra* Chapter VI. note 174), para. 41.

[190] Case C-92/09 *Volker und Markus Schecke und Eifert* (*supra* Chapter II. note 184), para. 52.

[191] Case C-291/12 *Schwarz* (*supra* Chapter II. note 131); Case C-293/12 *Digital Rights Ireland* (*supra* Chapter II. note 130); Case C-131/12 *Google Spain and Google* (*supra* Chapter IV. note 283); Case C-446/12 *Willems and Others* (*supra* Chapter VI. note 174); Case C-362/14 *Schrems* (*supra* Chapter VI. note 64); Case C-203/15 *Tele2 Sverige* (*supra* Chapter VI. note 174); Case C-207/16 *Ministerio Fiscal* (*supra* Chapter VI. note 174); Case C-136/17 *GC and Others* (*supra* Chapter IV. note 295); Case C-708/18 *Asociatia de Proprietari bloc M5A-ScaraA* (*supra* Chapter VI. note 174); Case C-311/18 *Facebook Ireland and Schrems* (*supra* Chapter IV. note 295); Case C-623/17 *Privacy International* (*supra* Chapter VI. note 174); Joined Cases C-511/18, C-512/18 and C-520/18 *La Quadrature du Net and Others* (*supra* Chapter VI. note 174); Case C-746/18 *Prokuratuur* (*supra* Chapter VI. note 174); by contrast, see Case C-141/12 *Y.S.* (*supra* Chapter II. note 65)*;* more recently Case C-645/19 *Facebook Ireland and Others* (*supra* Chapter VI. note 174), para. 67.

[192] H. Kranenborg, 'Art 8 Protection of Personal Data' (*supra* Chapter VII. note 14), para. 46.

[193] T. Riesz, 'Art 8 GRC. Schutz personenbezogener Daten' (*supra* Chapter VI. note 27), para. 9.

Article 8 of the ECHR.[194] Moreover, *van der Sloot* argues that Article 8 of the ECHR has been transformed to a personality right thus giving individuals control over their personal information.[195] Furthermore, the ECtHR has emphasised that this right gives the data subject a form of informational self-determination.[196] In the context of informational self-determination, data subjects should be able to determine for themselves how their personal is used. Thus, data subjects should also be able to decide for themselves whether their personal data will be used as an economic asset. Should they consent to this use, Article 8 of the ECHR does not prevent it, provided that its conditions are met.

5. Conclusion: Limitations on the use of personal data as an economic asset

Most fundamental rights, including the right to data protection, do not offer absolute protection, but can be restricted. Article 52 (1) of the Charter sets out conditions under which interference with fundamental rights is allowed: a legal basis, respecting the essence of the fundamental right, meeting an objective of general interest or needing to protect the rights and freedoms of others and adhering to the principle of proportionality. Thus, data processing and the related economic use of personal data may be justified if these circumstances are fulfilled.

Data processing and the use of personal data as an economic asset may limit the exercise of fundamental rights of data subjects but are explicitly allowed by the GDPR under certain conditions and thus provided for by law.

The essence of a fundamental right is an inviolable core. A violation of this core always constitutes an unlawful violation of a fundamental right. It was argued above that the essence of the right to data protection is control. Control by data subjects is not limitless but means that they can exercise their data rights and that these are respected. Consequently, the essence of the fundamental right to data protection does not prevent companies or data subjects themselves from using personal data as an economic asset, as long as the data subjects retain control over their personal data.

It is more difficult to assess whether the current use of personal data as an economic asset contributes to the objective of economic growth or technological progress and therefore meets objectives of general interest. Data cooperatives could contribute to economic growth.

---

[194] See ECtHR, *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland* (*supra* Chapter VIII. note 114), para. 136 and the case law cited.

[195] B. van der Sloot, 'Privacy as Personality Right: Why the ECtHR's Focus on Ulterior Interests Might Prove Indispensable in the Age of "Big Data"', 31 *Utrecht Journal of International and European Law* (2015), p. 44.

[196] ECtHR, *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland* (*supra* Chapter VIII. note 114), para. 137.

The use of personal data as an economic asset must also be proportionate and necessary. The practices relating to behavioural advertising described in Chapter III. 2. a) must therefore be the least intrusive means of advertising. It is not possible to make a blanket statement that all types of behavioural advertising are not proportionate, as it depends on the specific circumstances of the data processing operations.

Furthermore, if conflicting fundamental rights are at issue, a fair balance must be struck between differing rights enshrined in the Charter. Here too, the balancing test boils down to a case-by-case balancing exercise. Decisive factors may be the publicity of the data subject concerned or the use for journalistic activities. Article 8 of the ECHR can be used as aid to interpretation.

All in all, the use of personal data as an economic asset must fulfil all the requirements of Article 52 (1) of the Charter to constitute a justified interference with the right do data protection. The right to data protection can also be limited by rights and interests of others. Thus, personal data as an economic asset can be a justified interference according to the Charter.

IX. Conclusion

This work primarily aimed to address the question of whether and to what extent the use of personal data as an economic asset can be compatible with the Charter. Based on a doctrinal analysis, which sought to systematise and rationalise the EU's primary law, secondary law and supplementary sources of EU law and the case law of the CJEU, it can be concluded that personal data as an economic asset can be compatible with the Charter.

Firstly, this work focused on a comprehensive exploration of the concept of personal data, revealing its nuanced and multifaceted nature within the legal framework. The analysis delved into key legislative documents such as the GPDR and examined pivotal case law form the CJEU to unravel the intricacies of personal data. It underscored the EU legislator's intention to provide a broad definition of personal data, aligning with the perspectives of both the WP29 and the CJEU. The contextual approach taken by both the WP29 and the CJEU, considering the four elements of 'any information', 'relating to', 'identified or identifiable', 'natural person', prevents an overly restrictive or expansive definition.

The first building block, 'any information', is broadly interpreted without regard to subjectivity or objectivity, content or format. The CJEU's *Nowak* case reinforces this stance. The second building block, 'relating to', allows for a nuanced understanding, incorporating elements such as 'content', 'purpose' and 'result', as seen in the *Nowak* case, surpassing the narrower interpretation in the *YS* judgment. The third building block, 'identified or identifiable', focuses on means likely to be used to identify individuals directly or indirectly. The CJEU emphasises the legality of means, necessitating a case-by-case evaluation. While pseudonymous data falls under identifiability, anonymous data do not. The fourth element, 'natural person', generally includes living beings but can extend to deceased individuals, unborn children and legal persons. Which data is personal and which is not, is a case-by-case decision that also depends on the context. Further CJEU case law will bring more clarity in the future.

The term 'economic asset' suggested that data is ascribed a certain material value. Using Facebook as an example, it was analysed how companies use personal data as an economic asset, particularly through profiling. Profiling involves merging and analysing personal data to create comprehensive personality profiles, aiming to predict individual behaviour. These detailed profiles are especially valuable for advertising companies, enabling them to target specific audiences with personalised advertisements, a strategy proven to be highly lucrative.

The monetisation of personal data is epitomised by data sharing, both within companies and with external entities. It was highlighted that data brokers specialise in collecting vast datasets about individuals and trading them as economic assets to third parties. By examining the prices at which data brokers sell personal data, one can calculate the market value, with the quantity of personal data being one of the key determinants of profitability.

The discussion also delved into the consequences of data breaches during data sharing and processing, exploring how fines imposed due to breaches can influence the overall value calculation. The presence of personal data on the dark web was examined as an additional factor in determining the value of such breaches.

Various surveys and experiments on individuals' willingness to reveal their personal data for monetary compensation were presented. While there are criticism of the concept of willingness to pay for privacy, these studies provide valuable insights into individuals' perspectives on the value of their personal data. The analysis indicated the difference between the minimum amount to sell personal data and the maximum price to protect personal data.

Summarising the methods presented, it was concluded that while a concrete fixed value for personal data is elusive, it undeniably holds value that is context-dependent and variable. Sensitive data consistently emerged as the most valuable data and the awareness of data 'ownership' further increased its value.

Additionally, it was sought to examine how and by whom personal data can be used as an economic asset. It was elucidated that, within German-speaking national legal systems and EU law, personal data lacks traditional ownership status in the private law sense. The discussion explored the normative desirability of constructing an allocation of rights based on the storage medium, recognising the evolving landscape of cloud services that challenges this conventional approach.

Giving the acknowledged absence of personal data ownership in the current legal frameworks, both within German-speaking nations and the EU, an enduring debate has emerged regarding the introduction of an *erga omnes* property right to personal data. Advocates for this approach emphasise the potential for enhanced legal certainty and secure data access. However, the discussion highlighted the existence of legal uncertainties arising from multipersonality inherent in personal data, casting doubt on the practicality of such an approach. In addition, proposals in the areas of investment protection, trade secrets, copyright and patent law were examined and found to be inadequate, either due to explicit exclusions or inherent limitations in their applicability to personal data. Moreover, it was underscored that while contractual agreements might confer exclusive rights to personal data, the nature of contracts inherently limits their scope to the parties involved, falling short of the *erga omnes* principle.

Following this examination, the substantial rights granted to data subjects under EU data protection law were highlighted. While not unlimited or *erga omnes*, these rights empower data subjects with significant control and disposition over their personal data, forming a robust legal foundation. It was argued

that part of this control and disposition should involve data subjects participating in the value derived from their personal data. Advocating for the autonomy of data subjects, it was postulated that individuals should have the freedom to decide whether to make their personal data available in exchange for digital products or services. The commercialisation of personal data, an undeniable phenomenon, should be a decision within the purview of data subjects, as they possess the right to use their personal data as an economic asset.

The EU's response to the challenges and opportunities presented by the digital age, particularly in recognising the economic value of (personal) data, were examined. The strategic initiatives, including the drive towards a Digital Single Market, underscore the EU's commitment to adapting to the evolving landscape.

Legislative actions such as the Data Governance Act and the Data Act, mark significant milestones by explicitly addressing the rights associated with data and striving to enhance its usability and fair allocation of value. The DCD, a further notable development, extends contract law to situations involving the exchange of personal data for digital content or services, thereby granting consumers substantial rights in the digital realm.

However, as with any transformative shift, challenges and critiques have emerged, particularly concerning the commercialisation of fundamental rights and the potential pitfalls. This work has delved into these complexities, acknowledging the need for a balanced approach that safeguards individual rights while recognising the economic potential of personal data. In navigating this nuanced landscape, the EU has demonstrated a proactive stance, balancing the imperative for economic growth with the protection of fundamental rights. While significant strides have been made, continual adaption and evaluation are crucial to ensure that the legal framework remains robust and reflective of the evolving digital reality. The recognition of personal data as a valuable economic asset opens new avenues for future research, emphasising the importance of a dynamic legal framework that can adeptly respond to the ever-changing digital landscape.

Fundamental rights aspects of the economic exploitation of personal data have not been sufficiently considered in the scientific literature so far. The application of the Charter to the economic exploitation of personal data was explored. The comprehensive analysis demonstrated that the Charter is not confided by the nature of EU actions but extends its reach to encompass diverse scenarios involving personal data.

The Charter's applicability to Member States, particularly when implementing EU law related to the economic use of personal data, is underscored by the abundance of relevant secondary law, including the GDPR. The examination of CJEU case law illuminates a broad interpretation of the Charter, emphasising the horizontal effect of its provisions, especially those deemed unconditional and mandatory. Notably, Article 8 of the Charter, enshrining the fundamental right to data protection, is argued to possess these essential characteristics.

From a normative standpoint, recognising the fundamental right to data protection as applicable not only to state authorities but also to private individuals

and companies is imperative. This recognition is grounded in the acknowledgment that these entities wield substantial economic and informational power through the accumulation of personal data. Extending the Charter's safeguards to private actors becomes crucial in fostering truly effective data protection and rectifying power imbalances in the evolving digital landscape.

Therefore, the use of personal data as an economic asset must meet the requirements of Article 8 of the Charter. One of these requirements is that personal data must be processed fairly. Thus, the economic use of personal data must be clear, transparent and comprehensible to data subjects. Furthermore, data subjects must be fully informed about the economic use of personal data in all its forms. This includes information about the risks involved in the commercial use of personal data, about the sharing with third parties and about the rights of data subjects. As some practical examples have revealed, in most instances this is not the case, as data subjects are not aware of the use of their personal data as an economic asset and thus personal data is not processed fairly.

Moreover, for personal data to be used as an economic asset, the purpose of the data processing (i.e. economic exploitation) must be explicitly disclosed before the personal data is collected, must be limited to the purpose and it must be limited in time. It must be legitimate, proportionate and necessary. It is therefore hardly surprising that personal data used as an economic asset on the black market is not compatible with Article 8 of the Charter.

Furthermore, consent is of central importance. Valid consent to the use of personal data as an economic asset precludes interference with Article 8 of the Charter as long as the above criteria are met. There are strict and additional requirements placed on both the consent to data processing and the economic use of children's personal data. Valid consent allows data subjects themselves to decide on the economic use of their personal data. If data subjects themselves decide to use their personal data as an economic asset in return for 'free' services or products, they are expressing their self-determination and private autonomy.

Other legitimate bases for data processing enshrined in Article 8 (2) of the Charter and specified in the GDPR, such as the necessity for the performance of a contract, the fulfilment of a legal obligation or the protection of vital interests of data subjects, cannot be invoked when using personal data as an economic asset. Whether data controllers or third parties can rely on their legitimate interest to use personal data as an economic asset, cannot be answered categorically, as it boils down to a case-by-case decision.

In conclusion, personal data as an economic asset can align with Article 8 of the Charter, with consent emerging as a pivotal and clear legitimate basis. Empowering data subjects to decide on the economic use of their personal data is underscored as a cornerstone principle, highlighting the centrality of individual autonomy and self-determination in data-driven economies.

In summary, fundamental rights, including the right to data protection, are not absolute and can be subject to restrictions. Article 52 (1) of the Charter provides the conditions under which interference with fundamental rights is al-

lowed, including the presence of a legal basis, respect for the essence of the fundamental right, pursuit of an objective of general interest, protection of the rights and freedoms of others and adherence to the principle of proportionality. Therefore, data processing and the economic use of personal data may be justified if these conditions are met.

The GDPR explicitly allows data processing and the economic use of personal data under certain conditions, thereby establishing a legal framework for such activities. The essence of the right to data protection was identified as control, and as long as data subjects retain control over their personal data, the economic use of personal data is not inherently precluded.

The evaluation of whether the economic use of personal data contributes to general interest objectives, such as economic growth or technological progress, requires careful consideration. Data cooperatives are recognised as a potential avenue contributing to economic growth, suggesting a nuanced perspective on the societal impact of such practices.

The principle of proportionality and necessity plays a central role in assessing the practices related to the economic use of personal data, particularly in areas like behavioural advertising. Each case must be evaluated individually to ensure that these practices are the least intrusive means possible. Moreover, conflicts between fundamental rights necessitate a balanced approach, with a fair consideration of various factors, such as the publicity of the data subject or the context of journalistic activities. Reference to Article 8 of the ECHR aids in this interpretative process.

All in all, this work has unraveled the intricate legal landscape surrounding the economic use of personal data in the EU, navigating the delicate balance between fundamental rights, particularly the right to data protection, and the imperatives of a data-driven economy. The extensive exploration of legal principles, such as those enshrined in the Charter and the GDPR, underscores that the use of personal data as an economic asset can indeed align with these frameworks under specific conditions. However, the extent to which individuals, beyond large corporations, will actively engage in leveraging their personal data as an economic asset hinges on multifaceted legal and societal factors. The evolving landscape prompts a vital question: Can we strike a harmonious equilibrium between the economic potential of personal data and the imperative to safeguard individual autonomy? The answer lies not only in legal frameworks but in the collective consciousness of a society navigating the uncharted territories of a data-driven era.

Bibliography

Acemoglu, Daron et al., 'Too Much Data: Prices and Inefficiencies in Data Markets', 14 *American Economic Journal: Microeconomics* (2022), pp. 218–256.

Acquisti, Alessandro et al., 'What is Privacy Worth?', 42 *The Journal of Legal Studies* (2013), pp. 249–274.

Ada, Sila et al., 'Context information can increase revenue in online display advertising auctions: Evidence from a policy change', 59 *Journal of Marketing Research* (2022), pp. 1040–1058.

Ahmadi, Iman et al., 'Overwhelming targeting options: Selecting audience segments for online advertising', *International Journal of Research in Marketing*, forthcoming.

Albers, Marion, *Informationelle Selbstbestimmung* (Baden-Baden: Nomos Verlag, 2005).

Albrecht, Jan Philipp, 'How the GDPR Will Change the World', 2 *European Data Protection Law Review* (2016), pp. 287–289.

Alonso García, Ricardo, 'The General Provision of the Charter of Fundamental Rights of the European Union', 8 *European Law Journal* (2002), pp. 492–514.

Bamberger, Kenneth A. et al., 'Can You Pay for Privacy? Consumer Expectations and the Behavior of Free and Paid Apps', 35 *Berkeley Technology Law Journal* (2020), pp. 327–366.

Barak, Omer et al., 'The price is right?: economic value of location sharing', *Proceedings of the 2013 ACM conference on Pervasive and ubiquitous computing adjunct publication* (2013), pp. 891–899.

Bartsch, Michael, 'Computerviren und Produkthaftung', 16 *CR – Computer und Recht* (2000), pp. 721–725.

– 'Software als Rechtsgut', 26 *CR – Computer und Recht* (2010), pp. 553–559.

Bauer, Christine, Korunovska, Jana and Spiekermann, Sarah, 'On the Value of Information – What Facebook Users are Willing to Pay', *Proceedings of the 20th European Conference on Information Systems* (2012), pp. 1–12.

Beales, Howard, 'The Value of Behavioral Targeting', *Network Advertising Initiative* (2010), pp. 1–24.

Becerril, Anahiby, 'The value of our personal data in the Big Data and the Internet of all Things Era', 7 *Advances in Distributed Computing and Artificial Intelligence Journal* (2018), pp. 71–80.

Benndorf, Volker and Normann, Hans-Theo, 'The Willingness to Sell Personal Data', 120 *The Scandinavian Journal of Economics* (2018), pp. 1260–1278.

Berger, Daniel, 'Facebook beendet Zusammenarbeit mit Datenhändlern', *Heise Online* (2018), https://www.heise.de/newsticker/meldung/Facebook-beendet-Zusammenarbeit-mit-Datenhaendlern-4008444.html (accessed 31 January 2024).

Birckan, Guilherme et al., 'Personal Data Protection and Its Reflexes on the Data Broker Industry' in Rogério Mugnaini (ed.), *Data and Information in Online Environments* (Florianópolis: Springer Publishing, 2020), pp. 103–117.

Birnbaum, Emily, 'D.C. attorney general sues Mark Zuckerberg over Cambridge Analytica', *Politico* (2022), https://www.politico.com/news/2022/05/23/attorney-general-sues-mark-zuckerberg-cambridge-analytica-00034368 (accessed 31 January 2024).

Blasi Casagran, Cristina and Vermeulen, Mathias, 'Reflections on the murky legal practices of political micro-targeting from a GDPR perspective', 11 *International Data Privacy Law* (2021), pp. 348–359.

Boehme-Neßler, Volker, 'Das Recht auf Vergessenwerden – Ein neues Internet-Grundrecht im Europäischen Recht', 33 *NVwZ – Neue Zeitschrift für Verwaltungsrecht* (2014), pp. 825–830.

Boerding, Andreas et al., 'Data Ownership – A Property Rights Approach from a European Perspective', 11 *Journal of Civil Law Studies* (2018), pp. 323–370.

Bolsinger, Harald, 'Wo bleibt die digitale Dividende für Europas Konsumenten?', 40 *DuD – Datenschutz und Datensicherheit* (2016), pp. 382–385.

Bottis, Maria and Bouchagiar, George, 'Personal Data v. Big Data: Challenges of Commodification of Personal Data', 8 *Open Journal of Philosophy* (2018), pp. 206–215.

Bradshaw, Simon, Millard, Christopher and Walden, Ian, 'Contracts for clouds: comparison and analysis of the Terms and Conditions of cloud computing services', 19 *International Journal of Law and Information Technology* (2011), pp. 187–223.

Bräutigam, Peter, 'Das Nutzungsverhältnis bei sozialen Netzwerken – Zivilrechtlicher Austausch von IT-Leistung gegen personenbezogene Daten', 15 *MMR – Zeitschrift für IT-Recht und Recht der Digitalisierung* (2012), pp. 635–641.

Britz, Thomas, Indenhuck, Moritz and Langerhans, Tom, 'Die Verarbeitung "zufällig" sensibler Daten', 11 *ZD – Zeitschrift für Datenschutz* (2021), pp. 559–564.

Brkan, Maja, 'The Unstoppable Expansion of the EU Fundamental Right to Data Protection: Little Shop of Horrors?', 23 *Maastricht Journal of European and Comparative Law* (2016), pp. 812–841.

– 'The Concept of Essence of Fundamental Rights in the EU Legal Order: Peeling the Onion to its Core', 14 *European Constitutional Law Review* (2018), pp. 332–368.

– 'The Essence of the Fundamental Rights to Privacy and Data Protection: Finding the Way Through the Maze of the CJEU's Constitutional Reasoning', 20 *German Law Journal* (2019), pp. 864–883.

Buchner, Benedikt, 'Wissen ist Macht?', 32 *DuD – Datenschutz und Datensicherheit* (2008), pp. 724–728.

– 'Die Einwilligung im Datenschutzrecht – vom Rechtfertigungsgrund zum Kommerzialisierungsinstrument', 34 *DuD – Datenschutz und Datensicherheit* (2010), pp. 39–43.

Burgess, Lucie et al., 'The Value of Personal Data in Iot: Industry Perspectives on Consumer Conceptions of Value', *Living in the Internet of Things* (2019), pp. 1–11.

Bygrave, Lee A., 'Information Concepts in Law: Generic Dreams and Definitional Daylight', 35 *Oxford Journal of Legal Studies* (2015), pp. 91–120.

Cadwalladr, Carole and Graham-Harrison, Emma, 'Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach', *The Guardian* (2018), https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election (accessed 31 January 2024).

Cahillane, Laura Schweppe, Jennifer (eds.)*, Legal Research Methods: Principles and Practicalities* (Dublin: Clarus Press, 2016).

Calliess, Christian and Ruffert, Matthias (eds.), *EUV/AEUV* (6th edition, Munich: C.H.Beck, 2022).

Carrascal, Juan Pablo et al., 'Your browsing behavior for a Big Mac: Economics of personal information online', *Proceedings of the 22nd International Conference on World Wide Web* (2011), pp. 189–200.

Ceci, Laura, 'Hours of video uploaded to Youtube every minute as of February 2022', *Statista* (2023), https://www.statista.com/statistics/259477/hours-of-video-uploaded-to-youtube-every-minute/ (accessed 31 January 2024).

Cheong, Hyongmook et al., 'A Data Valuation Model to Estimate the Investment Value of Platform Companies: Based on Discounted Cash Flow', 16 *Journal of Risk and Financial Management* (2023), pp. 1–17.

Chirita, Anca D., 'The Rise of Big Data and The Loss of Privacy', 28 *MPI Studies on Intellectual Property and Competition Law* (2018), pp. 153–189.

Clifford, Damian and Ausloos, Jef, 'Data Protection and the Role of Fairness', 37 *Yearbook of European Law* (2018), pp. 130–187.

Cohen, Julie E., 'The Inverse Relationship between Secrecy and Privacy', 77 *Social Research* (2010), pp. 883–898.

– 'What Privacy Is For', 126 *Harvard Law Review* (2013), pp. 1904–1933.

– 'Affording Fundamental Rights: A Provocation Inspired by Mireille Hildebrandt, 4 *Critical Analysis of Law* (2017), pp. 78–90.

– 'Examined Lives: Informational Privacy and the Subject as Object', 52 *Stanford Law Review* (2020), pp. 1373–1438.

Collins, Keith and Dance, Gabriel, 'How Researchers Learned to Use Facebook "Likes" to Sway Your Thinking', *The New York Times* (2018), https://www.nytimes.com/2018/03/20/technology/facebook-cambridge-behavior-model.html (accessed 31 January 2024).

Comandé, Giovanni and Schneider, Giulia, 'It's time: Leveraging the GDPR to shift the balance towards research-friendly EU data spaces', 59 *Common Market Law Review* (2022), pp. 739–776.

Confessore, Nicholas, LaForgia, Michael and Dance, Gabriel, 'Facebook's Data Sharing and Privacy Rules: 5 Takeaways From Our Investigations', *The New York Times* (2018), https://www.nytimes.com/2018/12/18/us/politics/facebook-data-sharing-deals.html (accessed 31 January 2024).

Costa-Cabral, Francisco and Lynskey, Orla, 'The Internal and External Constraints of Data Protection on Competition Law in the EU', *LSE Law, Society and Economy Working Papers* (2015), pp. 1–39.

– 'Family ties: The intersection between data protection and competition in EU law', 54 *Common Market Law Review* (2017), pp. 11–50.

Cox, Joseph, 'Leaked Documents Expose the Secretive Market for Your Web Browsing Data', *Vice* (2020), https://www.vice.com/en/article/qjdkq7/avast-antivirus-sells-user-browsing-data-investigation (accessed 31 January 2024).

– 'Data Broker Is Selling Location Data of People Who Visit Abortion Clinics', *Vice* (2022), https://www.vice.com/en/article/m7vzjb/location-data-abortion-clinics-safegraph-planned-parenthood (accessed 31 January 2024).

Coyle, Diane and Manley, Annabel, 'What is the Value of Data? A review of empirical methods', *The Bennett Institute for Public Policy* (2022), pp. 1–30.

Coyle, Diane et al., 'The value of data summary report', *The Bennett Institute for Public Policy* (2020), pp. 1–17.

Custers, Bart and Malgieri, Gianclaudio, 'Priceless data: why the EU fundamental right to data protection is at odds with trade in personal data', 45 *Computer Law & Security Review* (2022), pp. 1–11.

Curry, Edward, 'The Big Data Value Chain: Definitions, Concepts, and Theoretical Approaches' in José Cavanillas et al. (eds.) *New Horizons for a Data-Driven Economy* (Berlin: Springer Verlag, 2016), pp. 29–37.

Cvrcek, Dan et al., 'A study on the value of location privacy', *Proceedings of the 2006 ACM Workshop on Privacy in the Electronic Society* (2006), pp. 1–10.

Czajkowski, Nico and Müller-ter Jung, Marco, 'Datenfinanzierte Premiumdienste und Fernabsatzrecht', 34 *CR – Computer und Recht* (2018), pp. 157–166.

Dance, Gabriel, LaForgia, Michael and Confessore, Nicholas, 'As Facebook Raised a Privacy Wall, It Carved an Opening for Tech Giants', *The New York Times* (2018), https://www.nytimes.com/2018/12/18/technology/facebook-privacy.html (accessed 31 January 2024).

Datenethikkommission, *Gutachten der Datenethikkommission*, 23 October 2019.

Dawson, Mark, Lynskey, Orla and Muir, Elise, 'What is the Added Value of the Concept of the "Essence" of EU Fundamental Rights?', 20 *German Law Journal* (2019), pp. 763–778.

De Filippi, Primavera and Maurel, Lionel, 'The paradoxes of open data and how to get rid of it? Analysing the interplay between open data and sui-generis rights on databases', 23 *International Journal of Law and Information Technology* (2015), pp. 1–22.

De Franceschi, Alberto and Lehmann, Michael, 'Data as Tradeable Commodity and New Measures for their Protection', 1 *The Italian Law Journal* (2015), pp. 51–72.

De Gregorio, Giovanni, *Digital Constitutionalism in Europe – Reframing Rights and Powers in the Algorithmic Society* (Cambridge: Cambridge University Press, 2022).

– 'The rise of digital constitutionalism in the European Union', 19 *International Journal of Constitutional Law* (2021), pp. 41–70.

De Hert, Paul, 'Data protection's future without democratic bright line rules. Co-existing with Technologies in Europe after Breyer', 3 *European Data Protection Law Review* (2017), pp. 20–35.

Delacroix, Sylvie and Lawrence, Neil D., 'Bottom-up data Trusts: disturbing the "one size fits all" approach to data governance', 9 *International Data Privacy Law* (2019), pp. 236–252.

Dixon, Stacy, 'Facebook: advertising revenue worldwide 2009–2022', *Statista* (2023), https://www.statista.com/statistics/271258/facebooks-advertising-revenue-worldwide/ (accessed 31 January 2024).

Docksey, Christopher, 'Four fundamental rights: finding the balance', 6 *International Data Privacy Law* (2016), pp. 195–209.

Dorner, Michael, 'Big Data und Dateneigentum', 30 *CR – Computer und Recht* (2014), pp. 617–628.

Dougan, Michael, 'Judicial review of Member State action under the general principles and the Charter: Defining the "scope of Union law"', 52 *Common Market Law Review* (2015), pp. 1201–1245.

Douilhet, Emile and Karanasiou, Argyro P. 'Legal Responses to the Commodification of Personal Data in the Era of Big Data: The Paradigm Shift From Data Protection Towards Data Ownership' in Information Resources Management Association (ed.), *Web Services: Concepts, Methodologies, Tools, and Applications* (Hershey: IGI Global, 2019), pp. 2076–2085.

Drexl, Josef, 'Designing Competitive Markets for Industrial Data – Between Propertisation and Access', 8 *JIPITEC – Journal of Intellectual Property, Information Technology and E-Commerce Law* (2017), pp. 257–292.

Duch-Brown, Nestor et al., 'The economics of ownership, access and trade in digital era', *JRC Digital Economy Working Paper* (2017), pp. 1–55.

Duisberg, Alexander, 'Datenhoheit und Recht des Datenbankherstellers – Recht am Einzeldatum vs. Rechte an Datensammlungen' in Oliver Raabe and Manuela Wagner

(eds.), *Daten als Wirtschaftsgut – Europäische Datenökonomie oder Rechte an Daten?* (Berlin: Smart Data, 2017), pp. 16–28.

Durovic, Mateja and Montanaro, Marco, 'Data Protection and Data Commerce: Friends or Foes?', 17 *European Review of Contract Law* (2021), pp. 1–36.

Dwoskin, Elizabeth, 'Data Broker Removes Rape-Victims List After Journal Inquiry', *The Wall Street Journal* (2013), https://www.wsj.com/articles/BL-DGB-31536 (accessed 31 January 2024).

Eckhardt, Jens, 'Anmerkung zu EuGH, Urteil vom 19. Oktober 2016 – C-582/14', 60 *ZUM – Zeitschrift für Urheber- und Medienrecht* (2016), pp. 1029–1030.

– 'Anwendungsbereich des Datenschutzrechts – Geklärt durch den EuGH?', 32 *CR – Computer und Recht* (2016), pp. 786–790.

Eeckhout, Piet, 'The EU Charter of Fundamental Rights and the Federal Question', 39 *Common Market Law Review* (2002), pp. 945–994.

Efroni, Zohar, 'Gaps and opportunities: The rudimentary protection for "data-paying consumers" under new EU consumer protection law', 57 *Common Market Law Review* (2020), pp. 799–830.

Ehmann, Eugen and Selmayr, Martin (eds.), *DS-GVO Datenschutz-Grundverordnung* (2nd edition, Munich: C.H. Beck, 2018).

Ehrenberg, Billy, 'How much is your personal data worth?', *The Guardian* (2014), https://www.theguardian.com/news/datablog/2014/apr/22/how-much-is-personal-data-worth (accessed 31 January 2024).

Elliott, Deni, 'Data Protection Is More Than Privacy', 5 *European Data Protection Law Review* (2019), pp. 13–16.

El Khoury, Alessandro, 'Dynamic IP Addresses Can be Personal Data, Sometimes. A story of Binary Relations and Schrödinger's cat', 8 *European Journal of Risk Regulation* (2017), pp. 191–197.

Elvy, Stacy-Ann, 'Paying for Privacy and the Personal Data Economy', 117 *Columbia Law Review* (2017), pp. 1369–1459.

ENISA – European Network and Information Security Agency, *Study on monetizing privacy – An economic model for pricing personal information*, 28 February 2021.

Ensthaler, Jürgen, 'Industrie 4.0 und die Berechtigung an Daten', 69 *NJW – Neue Juristische Wochenschrift* (2016), pp. 3473–3478.

European Union Agency for Fundamental Rights and Council of Europe, *Handbook on European data protection law*, (Luxembourg: Publications Office of the European Union, 2018).

– *Your rights matter: Data protection and privacy – Fundamental Rights Survey* (Luxembourg: Publications Office of the European Union, 2020).

Fabiano, Nicola, 'The value of personal data is the Data Protection and Privacy preliminary condition: synthetic human profiles on the web and ethics', *3rd International Conference on Applications of Intelligent Systems* (2020), pp. 1–5.

Farahat, Ayman and Bailey, Michael C., 'How Effective is Targeted Advertising', *Proceedings of the 21st International Conference on World Wide Web* (2012), pp. 111–120.

Federal Trade Commission, *A Look At What ISPs Know About You: Examining the Privacy Practices of Six Major Internet Service Providers*, 21 October 2021.

Feiler, Lukas and Forgó, Nikolaus, *EU-DSGVO* (Vienna: Verlag Österreich, 2016).

Ferretti, Federico, 'Data protection and the legitimate interest of data controllers: Much ado about nothing or the winter of rights?' 51 *Common Market Law Review* (2014), pp. 843–868.

Finck, Michèle and Pallas, Frank, 'They who must not be identified — distinguishing personal from non-personal data under the GDPR', 10 *International Data Privacy Law* (2020), pp. 11–36.

Forgó, Nikolaus, 'Daten als Gegenstand von sachenrechtlichen, datenschutz- und urheberrechtlichen Regelungen' in Nikolaus Forgó and Brigitta Zöchling-Jud (eds.), *Das Vertragsrecht des ABGB auf dem Prüfstand: Überlegungen im digitalen Zeitalter* (Vienna: Manz Verlag, 2018), pp. 351–394.

Fouche, Gwladys, 'Facebook owner Meta faces EU ban on targeted advertising', *Reuters* (2023), https://www.reuters.com/technology/facebook-owner-faces-eu-ban-targeted-advertising-norway-says-2023-11-01/#:~:text=%22On%2027%20October%2C%20the%20EDPB,Economic%20Area%2C%22%20it%20said. (accessed 31 January 2024).

Fowler, Geoffrey A., 'I tried to read all my app privacy policies. It was 1 million words.', *The Washington Post* (2022), https://www.washingtonpost.com/technology/2022/05/31/abolish-privacy-policies/ (accessed 31 January 2024).

Frantziou, Eleni, 'The Horizontal Effect of the Charter of Fundamental Rights of the EU: Rediscovering the Reasons for Horizontality', 21 *European Law Journal* (2015), pp. 657–679.

– '(Most of) the Charter of Fundamental Rights is Horizontally Applicable', 15 *European Constitutional Law Review* (2019), pp. 306–323.

– 'The Binding Charter Ten Years on: More than a "Mere Entrety"?', 38 *Yearbook of European Law* (2019), pp. 73–118.

– 'The Horizontal Effect of the Charter: Towards an Understanding of Horizontality as a Strucutral Constitutional Principle', *22* Cambridge Yearbook of European Legal Studies (2020), pp. 208–232.

Froese, Julia and Straub, Sebastian, 'Wem gehören die Daten? – Rechtliche Aspekte der digitalen Souveränität in der Wirtschaft' in Ernst Hartmann (ed.), *Digitalisierung souverän gestalten – Innovative Impulse im Maschinenbau* (Berlin: Springer Verlag, 2021), pp. 86–97.

Garben, Sacha, 'Balancing social and economic fundamental rights in the EU legal order', 11 *European Labour Law Journal* (2020), pp. 364–390.

Gärtner, Anette and Brimsted, Kate, 'Let's Talk about Data Ownership', 39 *European Intellectual Property Review* (2017), pp. 461–466.

Goldfarb, Avi and Tucker, Catherine, 'Shifts in Privacy Concerns', 102 *American Economic Review* (2012), pp. 349–353.

González Fuster, Gloria and Gellert, Raphaël, 'The fundamental right to data protection in the European Union: in search of an uncharted right', 26 *International Review of Law, Computers & Technology* (2012), pp. 73–82.

Graef, Inge, Husovec, Martin and Purtova, Nadezhda, 'Data Portability and Data Control: Lessons for an Emerging Concept in EU law', 19 *German Law Journal* (2018), pp. 1359–1398.

Granville, Kevin, 'Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens', *The New York Times* (2018), https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html (accessed 31 January 2024).

Grossklags, Jens and Acquisti, Alessandro, 'When 25 Cents is too much: An Experiment on Willingness-To-Sell and Willingness-To-Protect Personal Information', *Proceedings of the Workshop on the Economics of Information Security* (2007), pp. 1–22.

Grützmacher, Malte, 'Dateneigentum – ein Flickenteppich', 32 *CR – Computer und* Recht (2016), pp. 485–495.

Hamilton, Isobel Asher, 'Mark Zuckerberg's former mentor has invested in privacy app Jumbo, which helps you mass delete old social media posts', *Business Insider* (2020), https://www.businessinsider.com/privacy-app-jumbo-raises-8-million-series-a-2020-6 (accessed 31 January 2024).

Hancox, Emily, 'The meaning of "implementing" EU law under Article 51(1) of the Charter: Åkerberg Fransson', 50 *Common Market Law Review* (2013), pp. 1411–1431.

– 'The Relationship Between the Charter and General Principles: Looking back and Looking Forward', 22 *Cambridge Yearbook of European Legal Studies* (2020), pp. 233–257.

Hann, Il-Horn et al., 'Overcoming Online Information Privacy Concerns: An Information-Processing Theory Approach', 24 *Journal of Management Information Systems* (2007), pp. 13–42.

Häglund, Emil and Björklund, Johanna, 'AI-Driven Contextual Advertising: A Technology Report and Implication Analysis', *arXiv:2205.00911* (2022), pp. 1–19.

Härting, Niko, 'Digital Goods und Datenschutz – Daten sparen oder monetarisieren?', 32 CR – Computer und Recht (2016), pp. 735–740.

Hansen, Hauke and Struwe, Dario, 'Speicherung von IP-Adressen zur Abwehr von Cyberattacken zulässig', 8 *GRUR-Prax – Praxis im Immaterialgüter- und Wettbewerbsrecht* (2016), pp. 503–503.

Heinzke, Philippe and Engel, Lennart, 'Datenverarbeitung zur Vertragserfüllung – Anforderungen und Grenzen', 10 *ZD – Zeitschrift für Datenschutz* (2020), pp. 189–194.

Helberger, Natali, Zuiderveen Borgesius, Frederik and Reyna, Agustin, 'The perfect match? A closer look at the relationship between EU consumer law and data protection law', 54 *Common Market Law Review* (2018), pp. 142—1466.

Hennemann, Moritz and Steinrötter, Björn, 'Data Act – Fundament des neuen EU-Datenwirtschaftsrechts?', 75 *NJW – Neue Juristische Wochenschrift* (2022), pp. 1481–1486.

Hern, Alex, 'Cambridge Analytica: how did it turn clicks into votes?', *The Guardian* (2018), https://www.theguardian.com/news/2018/may/06/cambridge-analytica-how-turn-clicks-into-votes-christopher-wylie (accessed 31 January 2024).

Heun, Sven-Erik and Assion, Simon, 'Internet(recht) der Dinge – Zum Aufeinandertreffen von Sachen- und Informationsrecht', 31 *CR – Computer und Recht* (2015), pp. 812–818.

Heymann, Thomas, 'Der Schutz von Daten bei der Cloud Verarbeitung', 31 *CR – Computer und Recht* (2015), pp. 807–811.

– 'Rechte an Daten – Warum Daten keiner eigentumsrechtlichen Logik folgen', 32 *CR – Computer und Recht* (2016), pp. 650–657.

Hoeren, Thomas, 'Dateneigentum – Versuch einer Anwendung von § 303a StGB im Zivilrecht', 16 *MMR – Zeitschrift für IT-Recht und Recht der Digitalisierung* (2013), pp. 486–491.

– 'Datenbesitz statt Dateneigentum', 22 *MMR – Zeitschrift für IT-Recht und Recht der Digitalisierung* (2019), pp. 5–8.

Hoeren, Thomas and Pinelli, Stefan, 'Daten im Rechtsverkehr – Überlegungen für ein allgemeines Datenvertragsrecht', 75 *JZ – Juristen Zeitung* (2020), pp. 879–884.

Holoubek, Michael and Lienbacher, Georg (eds.), *GRC-Kommentar* (2nd edition, Vienna: Manz, 2019).

Hornung, Gerrit, 'Ökonomische Verwertung und informationelle Selbstbestimmung' in Alexander Roßnagel and Gerrit Hornung (eds.), *Grundrechtschutz im Smart Car* (Springer Verlag, 2019), pp. 109–126.

Hornung, Gerrit and Goeble, Thilo, 'Data Ownership im vernetzten Automobil', 31 *CR – Computer und Recht* (2015), pp. 265–273.

Hoy, Mariea Grubbs and Milne, George, 'Gender Differences in Privacy-Related Measures for Young Adult Facebook Users', 10 *Journal of Interactive Advertising* (2010), pp. 28–45.

Huberman, Bernardo A., Adar, Eytan and Fine, Leslie R., 'Valuating Privacy', 3 *IEEE Security and Privacy Magazine* (2005), pp. 22–25.

Ingram, David, 'Privacy is a right, but it may not be free. How does $3 a month sound?', *NBCNews* (2020), https://www.nbcnews.com/tech/security/privacy-right-it-may-not-be-free-how-does-3-n1184291 (accessed 31 January 2024).

IPSOS, 'IAB State of Data 2021 Quantitative Analysis Assessing Perceived vs. Actual Preparedness for the Post Third-Party Cookie and Identifier Tracking and Ecosystem', *International Advertising Bureau* (2021), https://www.iab.com/wp-content/uploads/2021/03/IAB_Ipsos_State_Of_Data_2021-03.pdf (accessed 31 January 2024).

Isaac, Mike and Frenkel, Sheera, 'Facebook Security Breach Exposes Accounts of 50 Million Users', *The New York Times* (2018), https://www.nytimes.com/2018/09/28/technology/facebook-hack-data-breach.html?action=click&module=RelatedCoverage&pgtype=Article&region=Footer (accessed 31 January 2024).

Jahnel, Dietmar (ed.), *DSGVO Datenschutz-Grundverordnung* (Vienna: Jan Sramek Verlag, 2021).

Jahnel, Dietmar and Bergauer, Christian (eds.), *Teil-Kommentar zur DS-GVO* (Vienna: Jan Sramek Verlag, 2018).

Janeček, Václav, 'Ownership of personal data in the Internet of Things', 34 *Computer Law & Security Review* (2018), pp. 1039–1052.

Jarass, Hans D. (ed.), *Charta der Grundrechte der Europäischen Union* (4th edition, Munich: C.H. Beck, 2021).

– 'Die Bedeutung der Unionsgrundrechte unter Privaten', 25 *ZEuP – Zeitschrift für Europäisches Privatrecht* (2017), pp. 310–334.

Jones, Charles I. and Tonetti, Christopher, 'Nonrivalry and the Economics of Data', 110 *American Economic Review* (2020), pp. 2819–2858.

Kalle, Ansgar, 'Herausgabe von Daten in der Insolvenz', 13 *BRJ – Bonner Rechtsjournal* (2020), pp. 38–45.

Kang, Cecilia, 'F.T.C. Hits Musical.ly With Record Fine for Child Privacy Violation', *The New York Times* (2019), https://www.nytimes.com/2019/02/27/technology/ftc-tiktok-child-privacy-fine.html?module=inline (accessed 31 January 2024).

Kang, Cecilia and Frenkel, Sheera, 'Facebook Says Cambridge Analytica Harvested Data of Up to 87 Million Users', *The New York Times* (2018), https://www.nytimes.com/2018/04/04/technology/mark-zuckerberg-testify-congress.html (accessed 31 January 2024).

Karanasiou, Argyro P. and Douilhet, Emile, 'Never Mind the Data: The Legal Quest over Control of Information & the Networked Self', *IEEE International Conference on Cloud Engineering Workshop (IC2EW)* (2016), pp. 100–105.

Kemp, Simon, 'Digital 2022: Global Overview Report', *Datareportal* (2022), https://datareportal.com/reports/digital-2022-global-overview-report (accessed 31 January 2024).

Keppeler, Lutz M., '"Objektive Theorie" des Personenbezugs und "berechtigtes Interesse" als Untergang der Rechtssicherheit?', 32 *CR – Computer und Recht* (2016), pp. 360–367.

Kilian, Wolfgang, 'Strukturwandel der Privatheit' in Hansjürgen Garstka and Wolfgang Coy (eds.), *Gedächtnisschrift für Wilhelm Steinmüller* (2014), pp. 195–224.

Klink-Straub, Judith and Straub, Tobias, 'Data Act als Rahmen für gemeinsame Datennutzung', 12 *ZDAktuell* (2022), p. 01076.

Knyrim, Rainer (ed.), *Datenschutz-Grundverordnung* (Vienna: Manz, 2016).

– (ed.), *Der DatKomm* (Vienna: Manz, 2022).
Kokott, Juliane and Sobotta, Christoph, 'The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR', 3 *International Data Privacy Law* (2013), pp. 222–228.
Koops, Bert-Jaap, 'The trouble with European data protection law', 4 *International Data Privacy Law* (2014), pp. 250–261.
Krasnova, Hanna et al., 'Investigating the Value of Privacy in Online Social Networks: Conjoint Analysis', *Proceedings of the 30th International Conference on Information Systems* (2009), pp. 1–19.
Krause, Rüdiger, 'Horizontal Effect of the EU Charter of Fundamental Rights: *Bauer and Willmeroth, MPG*', 58 *Common Market Law Review* (2021), pp. 1173–1206.
Kühling, Jürgen, 'Rückkehr des Rechts: Verpflichtung von Google & Co. zu Datenschutz', 14 *EuZW – Europäische Zeitschrift für Wirtschaftsrecht* (2014), pp. 527–532.
Kühling, Jürgen and Klar, Manuel, 'EuGH: Speicherung von IP-Adressen beim Besuch einer Internetseite', 7 *ZD – Zeitschrift für Datenschutz* (2017), pp. 24–29.
Langhanke, Carmen, *Daten als Leistung – Eine rechtsvergleichende Untersuchung zu Deutschland, Österreich und der Schweiz* (Tübingen: Mohr Siebeck, 2018).
Langhanke, Carmen and Schmidt-Kessel, Martin, 'Consumer Data as Consideration', 4 *Journal of European Consumer and Market Law* (2015), pp. 218–223.
Lazaro, Christophe and Le Métayer, Daniel, 'Control over Personal Data: True Remedy or Fairy Tale?', 12 *SCRIPTed* (2015), pp. 4–34.
Lazarus, David, 'Column: Shadowy data brokers make the most of their invisibility cloak', *Los Angeles Times* (2019), https://www.latimes.com/business/story/2019-11-05/column-data-brokers (accessed 31 January 2024).
Lazzerini, Nicole, '(Some of) the fundamental rights granted by the Charter may be a source of obligations for private parties: *AMS*', 51 *Common Market Law Review* (2014), pp. 907–933.
Leczykiewicz, Dorota, 'The Judgment in *Bauer* and the Effect of the EU Charter of Fundamental Rights in Horizontal Situations', 16 *European Review of Contract Law* (2020), pp. 323–333.
Lenaerts, Koen, 'Exploring the Limits of the EU Charter of Fundamental Rights', 8 *European Constitutional Law Review* (2012), pp. 375–403.
– 'Limits on Limitations: The Essence of Fundamental Rights in the EU', 20 *German Law Journal* (2019), pp. 77—793.
Li, Xiao-Bai et al, 'Valuing Personal Data with Privacy Consideration', 52 *Decision Sciences* (2021), pp. 393–426.
Lim, Chiehyeon et al., 'From data to value: A nine-factor framework for data-based value creation in information-intensive services', 39 *International Journal of Information Management* (2018), pp. 121–135.
Lynskey, Orla, 'Deconstructing Data Protection: The "Added-Value" Of A Right To Data Protection in the EU Legal Order', 63 *International & Comparative Law Quarterly* (2014), pp. 569–597.
– 'Control over Personal Data in a Digital Age: *Google Spain v AEPD and Mario Costeja Gonzalez*', 78 *The Modern Law Review* (2015), pp. 52—534.
– 'Delivering Data Protection: The Next Chapter', 21 *German Law Journal* (2020), pp. 80–84.
Malgieri, Gianclaudio and Custers, Bart, 'Pricing privacy – the right to know the value of your personal data', 34 *Computer Law & Security Review* (2018), pp. 289–303.

Manjoo, Farhad, 'Why You Shouldn't Use Facebook to Log In to Other Sites', *The New York Times* (2018), https://www.nytimes.com/2018/10/02/technology/personaltech/facebook-log-in-hack.html (accessed 31 January 2024).

Mantz, Reto and Spittka, Jan, 'EuGH: Speicherung von IP-Adressen beim Besuch einer Website', 69 *NJW – Neue Juristische Wochenschrift* (2016), pp. 3579–3583.

Markendorf, Merih, 'Recht an Daten in der deutschen Rechtsordnung', 9 *ZD – Zeitschrift für Datenschutz* (2018), pp. 409–413.

McDermott, Yvonne, 'Conceptualising the right to data protection in an era of Big Data', 4 *Big Data & Society* (2017), pp. 1–7.

Metzger, Axel, 'Dienst gegen Daten: Ein synallagmatischer Vertrag', 216 *Archiv für civilistische Praxis* (2016), pp. 817–865.

– 'Data as Counter-Performance: What Rights and Duties do Parties Have?', 8 *JIPITEC* (2017), pp. 2–8.

Metzger, Axel et al., 'Data-Related Aspects of the Digital Content Directive', 9 *JIPITEC* (2018), pp. 90–109.

Meyer, Jürgen and Hölscheidt, Sven (eds.), *Charta der Grundrechte der Europäischen Union* (5th edition, Berlin: Nomos Verlag, 2019).

Michl, Fabian, 'Datenbesitz – ein grundrechtliches Schutzgut?', 72 *NJW – Neue Juristische Wochenschrift* (2019), pp. 2729–2733.

Mitchell, Gareth, 'How much data is on the internet?', *Science Focus* (2021), https://www.sciencefocus.com/future-technology/how-much-data-is-on-the-internet/ (accessed 31 January 2024).

Moos, Flemming and Rothkegel, Tobias, 'EuGH: Speicherung von IP-Adressen beim Besuch einer Internetseite', 19 *MMR – Zeitschrift für IT-Recht und Recht der Digitalisierung* (2016), pp. 842–847.

Morey, Timothy et al., 'Customer Data: Designing for Transparency and Trust', 93 *Harvard business review* (2015), pp. 96–107.

Mostert, Menno et al., 'From Privacy to Data Protection in the EU: Implications for Big Data Health Research', 25 *European Journal of Health and Law* (2018), pp. 43–55.

Mourby, Miranda et al., 'Are "pseudonymised" data always personal data? Implications of the GDPR for administrative data research in the UK', 34 *Computer Law & Security Report* (2018), pp. 222–233.

Muir, Elise, 'The fundamental rights implications of EU legislation: Some constitutional challenges', 51 *Common Market Law Review* (2014), pp. 219–245.

– 'The Horizontal Effects of Charter Rights Given Expression to in EU Legislation, from Mangold to Bauer',12 *Review of European Administrative Law* (2019), pp. 185–215.

Müller-Christmann, Bernd, 'Haftung für Zerstörung von Computerdaten', 49 *NJW – Neue Juristische Wochenschrift* (1996), pp. 200–202.

Newman, Lily, 'WhatsApp Has Shared Your Data with Facebook for Years, Actually', *Wired* (2021), https://www.wired.com/story/whatsapp-facebook-data-share-notification/ (accessed 31 January 2024).

Nolte, Norbert, 'Das Recht auf Vergessenwerden – mehr als nur ein Hype?', 31 *NJW – Neue Juristische Wochenzeitschrift* (2014), pp. 2238–2242.

Noshad, Morteza et al., 'A data value metric for quantifying information content and utility', 8:82 *Journal of Big Data (*2021), pp. 1–23.

Nguyen, David and Paczos, Marta, 'Measuring the economic value of data and cross-border data flows – A business perspective', 297 *OECD Digital Economy Papers* (2020), pp. 1–47.

Ojanen, Tumas, 'Making the Essence of Fundamental Rights Real: The Court of Justice of the European Union Clarifies the Structure of Fundamental Rights under the Charter', 12 *European Constitutional Law Review* (2016), pp. 318–329.

Ovide, Shira, 'The Truth About your Whatsapp Data', *The New York Times* (2021), https://www.nytimes.com/2021/01/13/technology/whatsapp-data.html (accessed 31 January 2024).

Paal, Boris and Pauly, Daniel (eds.), *DS-GVO BDSG* (3rd edition, Munich: CH-Beck, 2021).

Park, Yong Jin, 'Do men and women differ in privacy? Gendered privacy and (in)equality in the Internet', 50 *Computers in Human Behavior* (2015), pp. 252–258.

Peers, Steve et al. (eds.), *The EU Charter of Fundamental Rights* (2nd edition, Oxford: Hart Publishing, 2021).

Pentland, Alex, Lipton, Alexander and Hardjono, Thomas, *Building The New Economy – Data as Capital* (Cambridge: MIT Press, 2021).

Peschel, Christopher and Rockstroh, Sebastian, 'Big Data in der Industrie – Chancen und Risiken neuer datenbasierter Dienste', 17 *MMR – Zeitschrift für IT-Recht und Recht der Digitalisierung* (2014), pp. 571–576.

Petrosyan, Ani, 'Worldwide digital population 2023', *Statista* (2023), https://www.statista.com/statistics/617136/digital-population-worldwide/ (accessed 31 January 2024).

Picht, Peter Georg and Richter, Heiko, 'EU Digital Regulation 2022: Data Desiderata', 71 *GRUR International Journal of European and International IP Law* (2022), pp. 395–402.

Poulou, Anastasia, 'Financial assistance conditionality and human rights protection: What is the role of the EU Charter of Fundamental Rights?', 54 *Common Market Law Review* (2017), pp. 991–1025.

Preibusch, Sören, 'The Value of Web Search Privacy', 13 *IEEE Security & Privacy* (2015), pp. 24–32.

Preibusch, Sören, Kübler, Dorothea and Beresford, Alistair R., 'Price versus privacy: an experiment into the competitive advantage of collecting less personal information', 13 *Electronic Commerce Research* (2013), pp. 423–455.

Prince, Christine, 'Do consumers want to control their personal data? Empirical evidence', 110 *International Journal of Human-Computer Studies* (2018), pp. 21–32.

Prins, Corien, 'Property and Privacy: European Perspectives and the Commodification of our Identity' in Lucie Guibault and P. Bernt Hugenholtz (eds.), *The Future of the Public Domain, Identifying the Commons in Information Law* (Alphen aan den Rijn: Kluwer Law International, 2006), pp. 223–257.

Purtova, Nadezhda, 'The illusion of personal data as no one's property', 7 *Law, Innovation and Technology* (2015), pp. 83–111.

– 'The law of everything. Broad concept of personal data and future of EU data protection law', 10 *Law, Innovation and Technology* (2018), pp. 40–81.

Rafieian, Omid and Yoganarasimhan, Hema, 'Targeting and Privacy in Mobile Advertising', 40 *Marketing Science* (2021), pp. 193–218.

Redeker, Helmut, 'Information als eigenständiges Rechtsgut', 27 *CR – Computer und Recht* (2011), pp. 634–639.

Reding, Viviane, 'The European data protection framework for the twenty-first century', 2 *International Data Privacy Law* (2012), pp. 119–129.

Rees, Christopher, 'Who owns our data?', 30 *Computer Law & Security Review* (2014), pp. 75–79.

Reid, Alan S., 'The European Court of Justice case of Breyer', 2 *Journal of Information Rights, Policy and Practice* (2017), pp. 1–7.

Reiners, Wilfried, 'Datenschutz in der Personal Data Economy – Eine Chance für Europa', 5 *ZD – Zeitschrift für Datenschutz* (2015), pp. 51–55.

Richter, Heiko, 'EuGH: Datenschutzrecht: Speicherung von IP-Adressen beim Besuch einer Website', 27 *EuZW – Europäische Zeitschrift für Wirtschaftsrecht* (2016), pp. 909–914.

Riedel, Christian, G.H., *Die Grundrechtsprüfung durch den EuGH* (Tübingen: Mohr Siebeck, 2020).

Roeber, Bjoern et al., 'Personal data: how context shapes consumer's data sharing with organizations from various sectors', 25 *Electronic Markets* (2015), pp. 95–108.

Rose, Ellen, 'Data Users versus Data Subjects: Are Consumers Willing to Pay for Property Rights to Personal Information?', *Proceedings of the 38th Annual Hawaii International Conference on System Sciences* (2005), pp. 1–10.

Rosenberg, Matthew, Confessore, Nicholas and Cadwalladr, Carole, 'How Trump Consultants Exploited the Facebook Data of Millions', *The New York Times* (2018), https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html (accessed 31 January 2024).

Roßnagel, Alexander, 'Fahrzeugdaten – wer darf über sie entscheiden?', 14 *SVR – Straßenverkehrsrecht* (2014), pp. 281–287.

– 'Kein "Verbotsprinzip" und kein "Verbot mit Erlaubnisvorbehalt" im Datenschutzrecht', 72 *NJW – Neue Juristische Wochenschrift* (2019), pp. 1–5.

Rowan, Mark and Dehlinger, Josh, 'Observed gender differences in privacy concerns and behaviors of mobile device end users', 37 *Procedia Computer Science* (2014), pp. 340–347.

Ruohonen, Jukka and Mickelsson, Sini, 'Reflections on the Data Governance Act', 2 *Digital Society* (2023), pp. 1–9.

Säcker, Franz Jürgen et al. (eds.), *Münchener Kommentar zum Bürgerlichen Gesetzbuch* (8th edition, Munich: C.H. Beck, 2020).

Sánchez, Sara Iglesias, 'The Court and the Charter: The impact of the entry into force of the Lisbon Treaty on the ECJ's approach to fundamental rights', 49 *Common Market Law Review* (2012), pp. 1565–1611.

Sarmiento, Daniel, 'Who's afraid of the Charter? The Court of Justice, national courts and the new framework of fundamental rights protection in Europe', 55 *Common Market Law Review* (2013), pp. 1267–1304.

Sattler, Andreas, *Informationelle Privatautonomie – Synchronisierung von Datenschutz- und Vertragsrecht* (Tübingen: Mohr Siebeck, 2022).

– 'Personenbezogene Daten als Leistungsgegenstand', 72 *JZ – Juristen Zeitung* (2017), pp. 1036–1046.

Scarcello, Orlando, 'Preserving the "Essence" of Fundamental Rights under Article 52(1) of the Charter: A Sisyphean Task?', 16 *European Constitutional Law Review* (2020), pp. 647–668.

Schmid, Alain, Schmidt, Kirsten Johanna and Zech, Herbert, 'Rechte an Daten zum Stand der Diskussion', 22 *sic! – Zeitschrift für Immaterialgüter-, Informations- und Wettbewerbsrecht* (2018), pp. 627–641.

Schmitz, Barbara, 'Digitale-Gesetze-Strategie – Agilität oder "Act"ionismus?', 12 *ZD – Zeitschrift für Datenschutz* (2022), pp. 189–190.

Schofield, Jack, 'Woman 4 times more likely than men to give passwords for chocolate', *The Guardian* (2008), https://www.theguardian.com/technology/blog/2008/apr/16/woman4timesmorelikelythan (accessed 31 January 2024).

Schreiner, Michel et al., 'On The Willingness To Pay For Privacy As A Freemium Model: First Empirical Evidence', *Proceedings of the 21st European Conference on Information Systems* (2013), pp. 1–7.

Schreiner, Michel and Hess, Thomas, 'Why Are Consumers Willing to Pay for Privacy? An Application of the Privacy-freemium Model to Media Companies', *Proceedings of the 23rd European Conference on Information Systems* (2015), pp. 1–15.

Schüritz, Ronny and Satzger, Gerhard, 'Patterns of Data-Infused Business Model Innovation', *IEEE 18th Conference on Business Informatics* (2018), pp. 133–142.

Schuster, Fabian and Hunzinger, Sven, 'Vor- und nachvertragliche Pflichten beim IT-Vertrag – Teil II: Nachvertragliche Pflichten', 31 *CR – Computer und Recht* (2015), pp. 277–286.

Schütze, Robert, 'Three "Bills of Rights" for the European Union', 30 *Yearbook of European Law* (2011), pp. 131–158.

Schwartz, Adam, 'The Payoff From California's "Data Dividend" Must be Stronger Privacy Laws', *Electronic Frontier Foundation* (2019), https://www.eff.org/de/deeplinks/2019/02/payoff-californias-data-dividend-must-be-stronger-privacy-laws (accessed 31 January 2024).

Schwartz, Paul M., 'Property, Privacy, and Personal Data', 117 *Harvard Law Review* (2004), pp. 2056–2128.

Schwartz, Paul M. and Solove, Daniel J., 'The PII Problem: Privacy and a New Concept of Personally Identifiable Information', 86 *New York University Law Review* (2011), pp. 1814–1894.

– 'Reconciling Personal Information in the United States and European Union', 102 *California Law Review* (2014), pp. 877–916.

Seetharaman, Deepa, 'Former Facebook, WhatsApp Employees Lead New Push to Fix Social Media', *The Wall Street Journal* (2022), https://www.wsj.com/articles/social-media-startups-take-aim-at-facebook-and-elon-musk-11651656600 (accessed 31 January 2024).

Sein, Karin and Spindler, Gerald 'The new Directive on Contracts for the Supply of Digital Content and Digital Services – Scope of Application and Trader's Obligation to Supply – Part 1', 15 *European Review of Contract Law* (2019), pp. 257–279.

Shapiro, Robert, 'What Your Data Is Really Worth to Facebook', *Washington Monthly* (2019), https://washingtonmonthly.com/magazine/july-august-2019/what-your-data-is-really-worth-to-facebook/ (accessed 31 January 2024).

Shapiro, Robert and Aneja, Siddhartha, 'Who Owns Americans' Personal Information and What Is It Worth?', *Future Majority* (2019), https://assets.futuremajority.org/uploads/report-for-future-majority-on-the-value-of-people-s-personal-data-shapiro-aneja-march-8-2019.pdf (accessed 31 January 2024).

Shepard, Brook, 'The New Rise of Contextual Advertising', *Forbes* (2021), https://www.forbes.com/sites/forbesagencycouncil/2021/07/22/the-new-rise-of-contextual-advertising/?sh=3114abb65e5d (accessed 31 January 2024).

Simonite, Tom, 'Datacoup Wants to Buy Your Credit Card and Facebook Data', *MIT Technology Review* (2014), https://www.technologyreview.com/2014/09/08/171469/datacoup-wants-to-buy-your-credit-card-and-facebook-data/ (accessed 31 January 2024).

Singer, Natasha, 'Mapping, and Sharing, The Consumer Genome', *The New York Times* (2012), https://www.nytimes.com/2012/06/17/technology/acxiom-the-quiet-giant-of-consumer-database-marketing.html?_r=0%20 (accessed 31 January 2024).

Singer, Natasha and Conger, Kate, 'Google is Fined $170 Million for Violating Children's Privacy on YouTube', *The New York Times* (2019), https://www.nytimes.com/2019/09/04/technology/google-youtube-fine-ftc.html (accessed 31 January 2024).

Specht, Louisa, 'Ausschließlichkeitsrechte an Daten – Notwendigkeit, Schutzumfang, Alternativen', 32 *CR – Computer und Recht* (2016), pp. 288–296.

– 'Daten als Gegenleistung – Verlangt die Digitalisierung nach einem neuen Vertragstypus?', 72 *JZ – Juristenzeitung* (2017), pp. 763–770.

Specht-Riemenschneider, Louisa et al., 'Die Datentreuhand', 24 *MMR-Beilage* (2021), pp. 25–48.

Spiecker gen. Döhmann, Indra and Eisenbarth, Markus, 'Kommt das "Volkszählungsurteil" nun durch den EuGH? – Der Europäische Datenschutz nach Inkrafttreten des Vertrags von Lissabon', 66 *JZ – Juristen Zeitung* (2011), pp. 169–177.

Spiekermann, Sarah et al., 'The challenges of personal data markets and privacy', 25 *Electronic Markets* (2015), pp. 161–167.

Spiekermann, Sarah and Korunovska, Jana, 'Towards a value theory for personal data', 32 *Journal of Information Technology* (2017), pp. 62–84.

Spies, Ulrich, 'Zweckfestlegung der Datenverarbeitung durch den Verantwortlichen', 12 *ZD – Zeitschrift für Datenschutz* (2022), pp. 75–81.

Staiano, Jacopo et al., 'Money Walks: A Human-Centric Study on the Economics of Personal Mobile Data', *Proceedings of the 2014 ACM Conference on Ubiquitous Computing* (2014), pp. 1–15.

Steel, Emily, 'Financial worth of data comes in at under a penny a piece', *The Financial Times* (2013), https://www.ft.com/content/3cb056c6-d343-11e2-b3ff-00144feab7de (accessed 31 January 2024).

Steel, Emily et al., 'How much is your personal data worth?', *The Financial Times* (2013), http://ig-legacy.ft.com/content/927ca86e-d29b-11e2-88ed-00144feab7de#axzz70TwxUoqY (accessed 31 January 2024).

Steinrötter, Björn, 'Datenaltruismus', 11 *ZD – Zeitschrift für Datenschutz* (2021), pp. 61–62.

Stepanov, Ivan, 'Introducing a property right over data in the EU: the data producer's right – an evaluation', 34 *International Review of Law, Computers & Technology* (2020), pp. 65–86.

Stern, Klaus and Sachs, Michael (eds.), *GRCh – Europäische Grundrechte-Charta* (Munich: C.H. Beck, 2016).

Streinz, Rudolf and Michl, Walther, 'Die Drittwirkung des europäischen Datenschutzgrundrechts (Art. 8 GRCh) im deutschen Privatrecht', 22 *EuZW – Europäische Zeitschrift für Wirtschaftsrecht* (2011), pp. 384–388.

Stück, Volker, 'Dynamische IP-Adressen sind personenbezogene Daten', 10 *CCZ – Corporate Compliance* (2017), pp. 228–230.

Summerson, Cameron, 'Jumbo Privacy is the Only App You Need to Protect Your Online Info', *ReviewGeek* (2021), https://www.reviewgeek.com/65253/jumbo-privacy-is-the-only-app-you-need-to-protect-your-online-info/ (accessed 31 January 2024).

Swant, Marty, *'The world's most valuable brands 2020', Forbes* (2020), https://www.forbes.com/the-worlds-most-valuable-brands/#41073ad5119c (accessed 31 January 2024).

Sydow, Gernot (ed.), *Europäische Datenschutzgrundverordnung* (2nd edition, Baden-Baden: Nomos Verlag, 2018).

Tau, Byron and Wells, Georgia, 'Grindr User Data Was Sold Through Ad Networks', *The Wall Street Journal* (2022), https://www.wsj.com/articles/grindr-user-data-has-been-for-sale-for-years-11651492800 (accessed 31 January 2024).

Torres Pérez, Aida, 'Rights and Powers in the European Union: Towards a Charter that is Fully Applicable to the Member States?', 22 *Cambridge Yearbook of European Legal Studies* (2020), pp. 279–300.

Tzanou, Maria, 'Balancing Fundamental Rights: United in Diversity? Some Reflections on the Recent Case Law of the European Court of Justice on Data Protection', 6 *Croatian Yearbook of European Law & Policy* (2010), pp. 53–74.

– 'Data protection as a fundamental right next to privacy? "Reconstructing" a not so new right', 3 *International Data Privacy Law* (2013), pp. 88–99.

van der Sloot, Bart, 'Privacy as Personality Right: Why the ECtHR's Focus on Ulterior Interests Might Prove Indispensable in the Age of "Big Data"', 31 *Utrecht Journal of International and European Law* (2015), pp. 25–50.

van Erp, Sjef, 'Ownership of data: the numerus clausus of legal objects', 6 *Brigham-Kanner Property Rights Conference Journal* (2017), pp. 235–257.

Véliz, Carissa, *Privacy Is Power* (London: Penguin Random House, 2020).

Versaci, Giuseppe, 'Personal Data and Contract Law: Challenges and Concerns about the Economic Exploitation of the Right to Data Protection', 14 *European Review of Contract Law* (2018), pp. 374–392.

Victor, Jacob M., 'The EU General Data Protection Regulation: Toward a Property Regime for Protecting Data Privacy', 123 *The Yale Law Journal* (2013), pp. 513–528.

von der Groeben, Hans, Schwarze, Jürgen and Hatje, Armin (eds.), *Europäisches Unionsrecht* (7th edition, Baden-Baden: Nomos Verlag, 2015).

von Ditfurth, Luklas and Lienemann, Gregor, 'The Data Governance Act: Promoting or Restricting Data Intermediaries', 23 *Competition and Regulation in Network Industries* (2022), pp. 270–295.

von Grafenstein, Maximilian, 'Refining the Concept of the Right to Data Protection in Article 8 ECFR – Part I', 6 *EDPL – European Data Protection Law Review* (2020), pp. 509–521.

– 'Refining the Concept of the Right to Data Protection in Article 8 ECFR – Part II', 7 *EDPL – European Data Protection Law Review* (2021), pp. 190–205.

– 'Refining the Concept of the Right to Data Protection in Article 8 ECFR – Part III', 7 *EDPL – European Data Protection Law Review* (2021), pp. 373–387.

Voss, W. Gregory and Houser, Kimberly A., 'Personal Data and the GDPR: Providing a Competitive Advantage for U.S. Companies', 56 *American Business Law Journal* (2019), pp. 287–344.

Wagner, Amina et al., 'Putting a Price Tag on Personal Information – A Literature Review', *Proceedings of the 51st Hawaii International Conference on System Sciences* (2018), pp. 3760–3769.

Walrave, Michael at al., 'Connecting and protecting? Comparing predictors of self-disclosure and privacy setting use between adolescents and adults', 6 *Cyberpsychology: Journal of Psychosocial Research on Cyberspace* (2012), https://cyberpsychology.eu/article/view/4259/3297 (accessed 31 January 2024).

Wandtke, Artur-Axel, 'Ökonomischer Wert von persönlichen Daten', 20 *MMR – Zeitschrift für IT-Recht und Recht der Digitalisierung* (2017), pp. 6–12.

Waterson, Jim, 'Cambridge Analytica did not misuse data in EU referendum, says watchdog', *The Guardian* (2020), https://www.theguardian.com/uk-news/2020/oct/07/cambridge-analytica-did-not-misuse-data-in-eu-referendum-says-watchdog (accessed 31 January 2024).

Weber, Beatrix 'Datenschutz 4.0 – Daten als Wirtschaftsgut in digitalisierten Märkten' in Dietmar Wolff and Richar Göbel (eds.), *Digitalisierung: Segen oder Fluch* (Berlin: Springer Verlag, 2018), pp. 101–123.

Wetsman, Nicole, 'Cycle-tracking apps stand behind their privacy policies as Roe teeters', *The Verge* (2022), https://www.theverge.com/2022/5/6/23060000/period-apps-privacy-abortion-roe-supreme-court (accessed 31 January 2024).

Wiebe, Andreas, 'Von Datenrechten zu Datenzugang – Ein rechtlicher Rahmen für die europäische Datenwirtschaft', 33 *CR – Computer und Recht* (2017), pp. 87–93.

Wixom, Barbara H. and Ross, Jeanne W., 'How to monetize your data', 58 *MIT Sloan Management Review* (2017), pp. 10–13.

Woollacott, Emma, 'What are You Worth on the Dark Web?', *Forbes* (2021), https://www.forbes.com/sites/emmawoollacott/2021/03/09/what-are-you-worth-on-the-dark-web/?sh=6c77af73cbca (accessed 31 January 2024).

Yan, Jun et al., 'How much Can Behavioral Targeting Help Online Advertising?', *Proceedings of the 18th International Conference on World Wide Web* (2009), pp. 261–270.

Yaveroglu, Idil and Donthu, Naveen, 'Advertising repetition and placement issues in online environments', 37 *Journal of Advertising* (2008), pp. 31–44.

Zdanowiecki, Konrad, 'Recht an den Daten' in Peter Bräutigam and Thomas Klindt (eds.), *Digitalisierte Wirtschaft / Industrie 4.0* (2015), pp. 19–29.

Zech, Herbert, 'Daten als Wirtschaftsgut – Überlegungen zu einem Recht des Datenerzeugers', 31 *CR – Computer und Recht* (2015), pp. 137–146.

– 'Data as a Tradeable Commodity' in Alberto De Franceschi (ed.), *European Contract Law and the Digital Single Market* (Cambridge: Intersentia, 2016), pp. 51–79.

Zhang, Kaifu and Katona, Zsolt, 'Contextual Advertising', 6 *Journal of Business Ethics* (2012), pp. 980–994;

Ziegenhorn, Gero, 'Speicherung von IP-Adressen beim Besuch einer Website', 36 *NVwZ – Neue Zeitschrift für Verwaltungsrecht* (2017), pp. 213–218.

Zöchling-Jud, Brigitta, 'Daten als Leistung' in Nikolaus Forgó and Brigitta Zöchling-Jud (eds.), *Das Vertragsrecht des ABGB auf dem Prüfstand: Überlegungen im digitalen Zeitalter* (Wien: Manz Verlag, 2018), pp. 239–272.

Zoltan, Miklos, 'Dark Web Price Index 2023', *Privacy Affairs* (2023), https://www.privacyaffairs.com/dark-web-price-index-2023/ (accessed 31 January 2024).

Zuboff, Shoshana, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (New York City: PublicAffairs, 2019).

Zuiderveen Borgesius, Frederik, 'Legal basis for behavioural targeting', 5 *International Data Privacy Law* (2015), pp. 163–176.

– 'The Breyer Case of the Court of Justice of the European Union: IP Addresses and the Personal Data Definition', 3 *European Data Protection Law Review* (2017), pp. 130–137.

Zuiderveen Borgesius, Frederik and Poort, Joost, 'Online Price Discrimination and EU Data Privacy Law', 40 *Journal of Consumer Policy* (2017), pp. 347–366.

Other documents

Acxiom, https://www.acxiom.com (accessed 31 January 2024).

Amazon, *Privacy Notice*, 12 February 2021, https://www.amazon.com/gp/help/customer/display.html?nodeId=GX7NJQ4ZB8MHFRNJ (accessed 31 January 2024).

Amended proposal for a Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data, COM (92) 422 final.

Article 29 Working Party opinion 4/2007 on the concept of personal data, 20 June 2007 ('WP136').

Article 29 Working Party opinion 03/2013 on purpose limitation, 2 April 2013 ('WP203').

Article 29 Data Protection Working Party opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, 14 November 2014 ('WP217').

Article 29 Working Party Guidelines on the right to data portability, 5 April 2017 ('WP242').

Avast Antitrack, https://www.avast.com/en-us/antitrack#mac (accessed 31 January 2024).

Avast, *Avast to Commence Wind Down of Subsidiary Jumpshot,* 30 January 2020, https://press.avast.com/en-gb/avast-to-commence-wind-down-of-subsidiary-jumpshot (accessed 31 January 2024).

BBC, *British Airways fined 20 million pounds over data breach*, 16 October 2020 https://www.bbc.com/news/technology-54568784 (accessed 31 January 2024).

Buckles, Shawn, *Data for Sale*, https://shawnbuckles.nl/dataforsale/ (accessed 31 January 2024).

Cambridge Dictionary, https://dictionary.cambridge.org/dictionary/english/asset (accessed 31 January 2024).

Chrome, *The next step toward phasing out third-party cookies in Chrome*, 14 December 2023, https://blog.google/products/chrome/privacy-sandbox-tracking-protection/ (accessed 31 January 2024)

Commission Staff Working Document on the free flow of data and emerging issues of the European data economy, (SWD 2017) 2 final.

Committee on Commerce, Science, and Transportation, *A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes*, 18 December 2013, https://www.commerce.senate.gov/services/files/bd5dad8b-a9e8-4fe9-a2a7-b17f4798ee5a (accessed 31 January 2024).

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – A Digital Single Market Strategy for Europe, COM(2015) 182 final.

Communication from the Commission to the European Parliament, the Council, the European economic and social committee and the committee of the regions – A European strategy for data, COM(2020) 66 final.

Communication from the Commission to the European Parliament and the Council, 'Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition – two years of application of the General Data Protection Regulation', COM(2020) 264 final ('Communication – two years of application of the General Data Protection Regulation').

Computer Hope, *How much is 1 byte, kilobyte, megabyte, gigabyte, etc.?,* https://www.computerhope.com/issues/chspace.htm (accessed 31 January 2024).

DataGuidance, *UK: ICO takes enforcement action against Experian after data broking investigation*, 28 October 2020, https://www.dataguidance.com/news/uk-ico-takes-enforcement-action-against-experian-after (accessed 31 January 2024).

Digital Austria, https://www.digitalaustria.gv.at (accessed 31 January 2024).

Domo, *Data never sleeps 9.0*, https://www.domo.com/learn/infographic/data-never-sleeps-9 (accessed 31 January 2024).

Dutch Data Protection Authority, *TikTok fined for violating children's privacy*, 22 July 2021, https://autoriteitpersoonsgegevens.nl/en/news/tiktok-fined-violating-children's-privacy (accessed 31 January 2024).

The Economist, *The world's most valuable resource is no longer oil, but data,* 6 May 2017, https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data (accessed 31 January 2024).

European Commission, *A European strategy for data*, 9 March 2021, https://digital-strategy.ec.europa.eu/en/policies/strategy-data (accessed 31 January 2024).

– *Do the data protection rules apply to data about a company?*, https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/application-regulation/do-data-protection-rules-apply-data-about-company_en (accessed 31 January 2024).
– *What is personal data?,* https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en (accessed 31 January 2024).
– *European Health Union: A European Health Data Space for people and science*, 3 May 2022, https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2711 (accessed 31 January 2024).

European Data Protection Board, *Article 29 Working Party,* https://edpb.europa.eu/our-work-tools/article-29-working-party_en (accessed 31 January 2024).

– *Endorsement of GDPR WP29 guidelines by the EDPB,* 25 May 2018, https://edpb.europa.eu/news/news/2018/endorsement-gdpr-wp29-guidelines-edpb_de (accessed 31 January 2024).
– *EDPB-EDPS Joint Opinion 03/2021 on the Proposal for a regulation of the European Parliament and of the Council on European data governance (Data Governance Act)*, 10 March 2021.
– *EDPB-EDPS Joint Opinion 2/2022 on the Proposal of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act),* 4 May 2022.
– *Guidelines 3/2018 on the territorial scope of the GDPR (Article 3)*, 12 November 2019.
– *Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects*, 9 April 2019.
– *Guidelines 05/2020 on consent under Regulation 2016/679*, 13 May 2020.

European Data Protection Supervisor, *Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy*, 26 March 2014.

– *EDPS Opinion on coherent enforcement of fundamental rights in the age of big data (Opinion 8/2016)*, 23 September 2016.

– *Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content*, 14 March 2017.
Experian Identity Theft Protection, https://www.experian.com/consumer-products/identity-theft-and-credit-protection.html (accessed 31 January 2024).
Facebook, *Ad targeting*, https://www.facebook.com/business/ads/ad-targeting (accessed 31 January 2024).
– *An Update on Our Plans to Restrict Data Access on Facebook,* 4 April 2018, https://about.fb.com/news/2018/04/restricting-data-access/ (accessed 31 January 2024).
– *Annual Report*, 28 January 2021, https://investor.fb.com/financials/default.aspx (accessed 31 January 2024).
– *Annual Report*, 3 February 2022, https://investor.fb.com/financials/default.aspx (accessed 31 January 2024).
– *Privacy Policy*, 3 November 2023, https://en-gb.facebook.com/policy.php (accessed 31 January 2024).
– *Terms of Service*, 12 January 2024, https://www.facebook.com/terms.php (accessed 31 January 2024).
Facebook Help Centre, https://www.facebook.com/help/contact/2032834846972583 (accessed 31 January 2024).
Federal Trade Commission, *FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook*, 24 July 2019, https://www.ftc.gov/news-events/news/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions-facebook (accessed 31 January 2024).
Federal Trade Commission, *Equifax Data Breach Settlement*, February 2022, https://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement (accessed 31 January 2024).
Gaia-X, *What is Gaia-X*, https://gaia-x.eu/what-is-gaia-x/ (accessed 31 January 2024).
Google, *Transparency Report*, https://transparencyreport.google.com/eu-privacy/overview?delisted_urls=start:1401235200000;end:1634687999999;country:AT&lu=delisted_urls (accessed 31 January 2024).
Help Net Security, *Office Workers Give Away Passwords for a Chocolate Bar*, 20 April 2004, https://www.helpnetsecurity.com/2004/04/20/office-workers-give-away-passwords-for-a-chocolate-bar/ (accessed 31 January 2024).
Human Rights Watch, *How Dare They Peep into My Private Life?,* 25 May 2022, https://www.hrw.org/report/2022/05/25/how-dare-they-peep-my-private-life/childrens-rights-violations-governments (accessed 31 January 2024).
IBM, *How much does a data breach cost?,* https://www.ibm.com/security/data-breach (accessed 31 January 2024).
Information Commissioner's Office, *Investigation into data protection compliance in the direct marketing data broking sector*, October 2020, https://ico.org.uk/media/action-weve-taken/2618470/investigation-into-data-protection-compliance-in-the-direct-marketing-data-broking-sector.pdf (accessed 31 January 2024).
– *Enforcement notice to Experian Limited*, 27 October 2020, https://ico.org.uk/action-weve-taken/enforcement/experian-limited/ (accessed 31 January 2024).
Ipsos Screenwise Panel, https://screenwisepanel.com/home (accessed 31 January 2024).
Iqbal, Umar et al., *Your Echos are Heard: Tracking, Profiling, and Ad Targeting in the Amazon Smart Speaker Ecosystem*, 28 April 2022, https://alexaechos.com/amazon_echo.pdf (accessed 31 January 2024).
Irish Council for Civil Liberties, *Landmark Litigation.*, 15 June 2021, https://www.iccl.ie/rtb-june-2021/#scale (accessed 31 January 2024).

Jumbo, *Jumbo 2: A step closer to our vision*, 24 June 2020, https://blog.jumboprivacy.com/jumbo-2.0-a-step-closer-to-our-vision.html (accessed 31 January 2024).

NBCnews, *Priest outed via Grindr App highlights rampant data tracking*, 22 July 2021, https://www.nbcnews.com/tech/security/priest-outed-grindr-app-highlights-rampant-data-tracking-rcna1493 (accessed 31 January 2024).

NortonLifeLock, https://www.nortonlifelock.com/us/en/ (accessed 31 January 2024).

OECD, *Exploring the Economics of Personal Data*, 2 April 2013, https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en (accessed 31 January 2024).

Open Data Österreich, https://www.data.gv.at (accessed 31 January 2024).

PRIVO, *History of COPPA Violations*, 18 February 2022, https://www.privo.com/history-of-coppa-violations (accessed 31 January 2024).

Saferinternet, *Jugend-Internet-Monitor 2023*, https://www.saferinternet.at/services/jugend-internet-monitor/ (accessed 31 January 2024).

Solid, *Solid: Your data, your choice.*, https://solidproject.org (accessed 31 January 2024).

The Washington Post, *Transcript of Mark Zuckerberg's Senate hearing*, 11 April 2018, https://www.washingtonpost.com/news/the-switch/wp/2018/04/10/transcript-of-mark-zuckerbergs-senate-hearing/ (accessed 31 January 2024).

WebFX, *What Are Data Brokers – And What is Your Data Worth?*, 16 March 2020, https://www.webfx.com/blog/internet/what-are-data-brokers-and-what-is-your-data-worth-infographic/ (accessed 31 January 2024).

WhatsApp, *WhatsApp Privacy Policy,* 25 August 2016, https://www.whatsapp.com/legal/privacy-policy/revisions/20160825 (accessed 31 January 2024).

– *WhatsApp Privacy Policy*, 4 January 2021, https://www.whatsapp.com/legal/updates/privacy-policy-eea#CiIOqowf5JJ18ztWP (accessed 31 January 2024).

Case law

BGH, 06.06.1984, VIII ZR 83/83.
BGH, 02.05.1985, I ZB 8/84.
BGH, 07.03.1990, VIII ZR 56/89.
BGH, 14.07.1993, VIII ZR 147/92.
BGH, 04.03.1997, X ZR 141/95.
BGH, 23.06.2009, VI ZR 196/08.
BGH, 10.07.2015, V ZR 206/14.
BVerfG, 15.12.1983, I BvR 209/83, DE:BVerfG:1983:rs19831215.1bvr020983.
BVerfG, 26.02.2020, 2 BvR 2347/15, DE:BVerfG:2020:rs20200226.2bvr234715.
Case C-36/74 *Walrave*, EU:C:1974:140.
Case C-43/75 *Defrenne* / *SABENA*, EU:C:1976:56.
Case C-5/88 *Wachauf*, EU:C:1989:321.
Case C-260/89 *ERT*, EU:C:1991:254.
Case C-415/93 *Bosman*, EU:C:1995:463.
Case C-299/95 *Kremzow*, EU:C:1997:254.
Case C-368/95 *Familiapress*, EU:C:1997:325.
Case C-309/96 *Annibaldi*, EU:C:1997:631.
Case C-281/98 *Angonese*, EU:C:2000:296.
Case C-465/00 *Österreichischer Rundfunk*, EU:C:2003:294.
Case C-101/01 *Lindqvist*, EU:C:2003:596.
Case C-203/02 *The British Horseracing Board*, EU:C:2004:695.
Case C-444/02 *Fixtures Marketing*, EU:C:2004:697.
Case C-144/04 *Mangold*, EU:C:2005:709.
Case C-438/05 *Viking*, EU:C:2007:772.
Case C-275/06 *Promusicae*, EU:C:2008:54.
Case C-524/06 *Huber*, EU:C:2008:724.
Case C-73/07 *Satakunnan Markkinapörssi und Satamedia*, EU:C:2008:727.
Case C-557/07 *LSG*, EU:C:2009:107.
Case C-553/07 *Rijkeboer*, EU:C:2009:293.
Case C-555/07 *Kücükdeveci*, EU:C:2010:21.
Case C-28/08 P *Bavarian Lager*, EU:C:2010:378.
Case C-92/09 *Volker und Markus Schecke und Eifert*, EU:C:2010:662.
Case C-236/09 *Test-Achats*, EU:C:2011:100.
Case C-457/09 *Chartry*, EU:C:2011:101.
Case C-543/09 *Deutsche Telekom*, EU:C:2011:279.
Case C-400/10 PPU *McB*, EU:C:2010:582.
Case C-70/10 *Scarlet*, EU:C:2011:771.
Case C-411/10 *N.S. and Others*, EU:C:2011:865.
Case C-468/10 *ASNEF*, EU:C:2011:777.

Case C-360/10 *SABAM*, EU:C:2012:85.
Case C-604/10 *Football Dataco*, EU:C:2012:115.
Case C-461/10 *Bonnier*, EU:C:2012:219.
Case C-617/10 *Åkerberg Fransson*, EU:C:2013:105.
Case C-256/11 *Dereci and Others*, EU:C:2011:734.
Case C-128/11 *UsedSoft*, EU:C:2012:407.
Case C-40/11 *Iida*, EU:C:2012:691.
Joined Cases C-356/11 and C-357/11 *O and S*, EU:C:2012:776.
Case C-283/11 *Sky Österreich*, EU:C:2013:28.
Case C-12/11 *McDonagh*, EU:C:2013:43.
Case C-426/11 *Alemo-Herron*, EU:C:2013:521.
Case C-87/12 *Ymeraga and Others*, EU:C:2013:291.
Case C-342/12 *Worten*, EU:C:2013:355.
Case C-291/12 *Schwarz*, EU:C:2013:670.
Case C-473/12 *IPI*, EU:C:2013:715.
Case C-176/12 *Association de médiation sociale*, EU:C:2014:2.
Case C-141/12 *YS*, EU:C:2014:2081.
Case C-293/12 *Digital Rights Ireland*, EU:C:2014:238
Case C-131/12 *Google Spain and Google*, EU:C:2014:317.
Case C-446/12 *Willems and Others*, EU:C:2015:238.
Case C-206/13 *Siragusa*, EU:C:2014:126.
Case C-198/13 *Julian Hernández and Others*, EEU:C:2014:2055.
Case C–212/13 *Ryneš*, EU:C:2014:2428.
Case C-316/13 *Fenoll*, EU:C:2015:200.
Case C-580/13 *Coty Germany*, EU:C:2015:485.
Case C-615/13 P *ClientEarth*, EU:C:2015:489.
Case C-201/14 *Bara*, EU:C:2015:638.
Case C-230/14 *Weltimmo*, EU:C:2015:639.
Case C-362/14 *Schrems*, EU:C:2015:650.
Case C-419/14 *WebMindLicenses*, EU:C:2015:832.
Case C-547/14 *Philip Morris Brands*, EU:C:2016:325.
Case C-582/14 *Breyer*, EU:C:2016:779.
Case C-258/14 *Florescu*, EU:C:2017:448.
Case C-191/15 *Verein für Konsumenteninformation*, EU:C:2016:612.
Case C-8/15 P *Ledra Advertising v Commission and ECB*, EU:C:2016:701.
Case C-203/15 *Tele2 Sverige*, EU:C:2016:970.
Case C-398/15 *Manni*, EU:C:2017:197.
Case C-157/15 *Achbita*, EU:C:2017:203.
Case C-528/15 *Al Chodor*, EU:C:2017:213.
Case C-682/15 *Berlioz Investment Fund*, EU:C:2017:373.
Case C-13/16 *Rīgas satiksme*, EU:C:2017:336
Case C–73/16 *Puškár*, EU:C:2017:725.
Case C-234/16 *Miravitlles Ciurana and Others*, EU:C:2017:969.
Case C-434/16 *Nowak,* EU:C:2017:994.
Case C-473/16 *F*, EU:C:2018:36.
Case C-414/16 *Egenberger*, EU:C:2018:257.
Case C-673/16 *Coman*, EU:C:2018:385.
Case C-210/16 *Wirtschaftsakademie Schleswig-Holstein*, EU:C:2018:388.

Case C-25/17 *Jehovan todistajat*, EU:C:2018:551.
Case C-540/16 *Spika*, EU:C:2018:565.
Case C-207/16 *Ministerio Fiscal*, EU:C:2018:788.
Case C-569/16 *Bauer*, EU:C:2018:871.
Case C-684/16 *Max-Planck-Gesellschaft*, EU:C:2018:874.
Case C-68/17 *IR*, EU:C:2018:696.
Case C-152/17 *Consorzio Italian Management e Catania Multiservizi*, EU:C:2018:264.
Case C-384/17 *Link Logistik N&N*, EU:C:2018:810.
Case C-193/17 *Cresco Investigation*, EU:C:2019:43.
Case C-345/17 *Buivids*, EU:C:2019:122.
Case C-235/17 *Commission v Hungary*, EU:C:2019:432.
Case C-40/17 *Fashion ID*, EU:C:2019:629.
Case C-136/17 *GC and* Others, EU:C:2019:773.
Case C-556/17 *Torubarov*, EU:C:2019:626.
Case C-507/17 *Google*, EU:C:2019:772.
Case C-673/17 *Planet49*, EU:C:2019:801.
Case C-609/17 *TSN*, EU:C:2019:981.
Case C-623/17 *Privacy International*, EU:C:2020:790.
Case C-492/18 PPU *TC*, EU:C:2019:108.
Case C-129/18 *SM*, EU:C:2019:248.
Case C-585/18 *A.K.*, EU:C:2019:982.
Case C-708/18 *Asociatia de Proprietari bloc M5A-ScaraA*, EU:C:2019:1064.
Case C-263/18 *Nederlands Uitgeversverbond und Groep Algemene* Uitgevers, EU:C:2019:1111.
Case C-78/18 *European Commission v Hungary*, EU:C:2020:476.
Case C-311/18 *Facebook Ireland and Schrems*, EU:C:2020:559.
Joined Cases C-511/18, C-512/18 and C-520/18 *La Quadrature du Net and Others*, EU:C:2020:791.
Case C-804/18 *WABE*, EU:C:2021:594.
Case C-746/18 *Prokuratuur*, EU:C:2021:152.
Case C-245/19 *État luxembourgeois*, EU:C:2020:795.
Case C-924/19 PPU *FMS and Others*, EU:C:2020:367.
Case C-272/19 *Land Hessen*, EU:C:2020:535.
Case C-233/19 *CPAS de Liège*, EU:C:2020:757.
Case C-243/19 *Veselības ministrija*, EU:C:2020:872.
Case C-61/19 *Orange Romania*, EU:C:2020:901.
Case C-30/19 *Braathens Regional Aviation*, EU:C:2021:269.
Case C-645/19 *Facebook Ireland and Others*, EU:C:2021:483.
Case C-439/19 *Latvijas Republikas Saeima*, EU:C:2021:504.
Case C-140/20 *Commissioner of An Garda Síochána*, EU:C:2022:258.
Case C-817/19 *Ligue des droits humains*, EU:C:2022:491.
Case C-184/20 *Vyriausioji tarnybinės etikos komisija*, EU:C:2022:601.
Joined Cases C-793/19 and C-794/19 *SpaceNet*, EU:C:2022:702.
Joined Cases C-339/20 and C-397/20 *VD*, EU:C:2022:703.
Case C-129/21 *Proximus*, EU:C:2022:833.
Joined Cases C-37/20 and C-601/20 *Luxembourg Business Registers*, EU:C:2022:912.
Case C-460/20 *Google*, EU:C:2022:962.

Case C-154/21 *Österreichische Post*, EU:C:2023:3.
Case C-205/21 *Ministerstvo na vatreshnite raboti*, EU:C:2023:49.
Case C-307/22 *FT*, EU:C:2023:81.
Case C-487/21 *Österreichische Datenschutzbehörde*, EU:C:2023:369.
Case C-579/21 *Pankki S*, EU:C:2023:501.
Case C-252/21 *Meta Platforms and Others,* EU:C:2023:537.
Case C-333/22 *Ligue des droits humains,* EU:C:2023:874.
Joined Cases C-26/22 and C-64/22 *SCHUFA Holding*, EU:C:2023:958.
Corte Costituzionale, 22.11.2019, 242/2019.
DSB, 31.07.2018, DSB-D213.642/0002-DSB/2018,
AT:DSB:2018:DSB.D213.642.0002.DSB.2018.
DSB, 30.11.2018, DSB-D122.931/0003-DSB/2018,
AT:DSB:2018:DSB.D122.931.0003.DSB.2018.
DSB, 16.04.2019, DSB-D213.679/0003-DSB/2018,
AT:DSB:2019:DSB.D213.679.0003.DSB.2018.
ECtHR, *Axel Springer AG v. Germany*, Judgment of 7 February 2012, Application No. 39954/08.
ECtHR, *Bohlen v. Germany*, Judgment of 19 February 2015, Application No. 53495/09.
ECtHR, *Coudec and Hachette Filipacchi Associés v. France*, Judgment of 10 November 2015, Application No. 40454/07.
ECtHR, *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland*, Judgment of 27 June 2017, Application No. 931/13.
GPDP, 16.09.2021, 9706389.
OGH, 13.11.1997, RS0108702, AT:OGH0002:1997:RS0108702.
OLG Karlsruhe, 07.11.1995, 3 U 15/95.
OLG Dresden, 05.09.2012, 4 W 961/12.
OLG Naumburg, 27.08.2014, 6 U 3/14.
Opinion of Advocate General Poiares Maduro in Case C-438/05 *Viking*, EU:C:2007:292.
Opinion of Advocate General Kokott in Case C-275/06 *Promusicae*, EU:C:2007:454.
Opinion of Advocate General Trstenjak in Case C-282/10 *Dominguez*, EU:C:2011:449.
Opinion of Advocate General Cruz Villalón in Case C-176/12 *Association de médiation sociale*, EU:C:2013:491.
Opinion of Advocate General Sánchez-Bordona in Case C-582/14 *Breyer*, EU:C:2016:339.
Opinion of Advocate General Kokott in Case C-434/16 *Nowak*, EU:C:2017:582.
Opinion of Advocate General Bot in Case C-569/16 *Bauer*, EU:C:2018:337.
Referral C-446/21 *Schrems*.
VfGH, 11.12.2020, G 139/2019–71, AT:VFGH:2020:G139.2019.

Index