Master's Degree Programme Law and Technology

July 2021

The (im)possibility of personal data as an object of contracts: An analysis of the GDPR and the Digital Content Directive

Furkan Güven Taştan
2045431

Supervisor: dr. Nadezhda Purtova LLM MSc

Second reader: Magdalena Brewczyńska

CONTENTS

CONTENTS ..... **ii**

LIST OF ABBREVIATIONS ..... **iv**

§ 1. INTRODUCTION **5**

1.1. BACKGROUND 5

1.2. OBJECTIVE 6

1.3. LITERATURE REVIEW 6

1.4. MAIN RESEARCH QUESTION AND SUB-QUESTIONS 9

1.5. LIMITATIONS AND PERSPECTIVE 10

1.6. METHODOLOGY 10

§ 2. TRADING PERSONAL DATA WITHIN THE GDPR **11**

2.1. HUMAN RIGHTS FOUNDATIONS OF THE GDPR 11

2.2. CONDITIONS DETERMINED IN THE GDPR 12

2.2.1. SELECTED PRINCIPLES 13

2.2.1.1. Lawfulness, fairness, and transparency 13

2.2.1.2. Purpose limitation 15

2.2.1.2.1. The purposes related to monetising personal data 15

2.2.1.2.2. Other purposes 16

2.2.1.3. Data minimisation 16

2.2.2. POSSIBLE LEGAL GROUNDS FOR PROCESSING 17

2.2.2.1. Consent of the Consumer 18

2.2.2.2. Necessity for the Performance of a Data as Counter-Performance Contract 21

2.2.2.3. Legitimate Interests Pursued by the Supplier 23

2.3. CONCLUDING REMARKS 25

§ 3. PERSONAL DATA AS OBJECT OF CONTRACTUAL OBLIGATION WITHIN THE DIGITAL CONTENT DIRECTIVE 27

3.1. THE DCD'S APPROACH REGARDING PERSONAL DATA 27

3.2. CONDITIONS DETERMINED IN THE DCD 28

3.2.1. CONTRACTING PARTIES 28

3.2.2. SUBJECT MATTER OF THE CONTRACT 28

3.2.2.1. Supplying digital content and digital service 29

3.2.2.2. Providing personal data 30

3.2.2.2.1. The nature of the consumer's obligation 32

3.2.2.2.2. Non-conforming performance of the consumer's obligation 32

3.2.2.2.3. Restrictions regarding the provision of personal data 33

3.2.2.2.4. Debates over the two predecessor concepts 34

3.3. CONCLUDING REMARKS 36

§ 4. RECONCILIATION OF THE GDPR'S AND THE DCD'S APPROACHES 37

4.1. OVERVIEW OF THE APPROACHES 38

4.2. CONFLICTING POINTS 39

4.2.1. The Tension between the Contractual Freedom Principle in the DCD and Human Rights Foundations of the GDPR 39

4.2.2. Validity of Consent according to the Art. 7(4) GDPR in Data as Counter-Performance Contracts 41

4.2.3. The Interplay between Exceptions in the DCD and Legal Grounds for Processing of Personal Data in the GDPR 41

4.3. RECONCILIATION OF CONFLICTING POINTS 42

4.3.1. Limiting Contractual Freedom by Determination of the Risks for Processing Personal Data in Data as Counter Performance Contracts 42

4.3.2. Distinguishing Data as Counter-Performance Contracts from Traditional Ones 45

4.3.3. Formulating an Interpretation on the Exceptions of the DCD 46

4.4. ADOPTING RECONCILIATIONS TO THE LEGAL FRAMEWORK 48

4.5. CONCLUDING REMARKS 49

§ 5. CONCLUSION 51

BIBLIOGRAPHY 54

LIST OF ABBREVIATIONS

A29WP	Article 29 Working Party
Charter	Charter of Fundamental Rights of the European Union
CJEU	Court of Justice of the European Union
DACP Contract	Data as counter-performance contract
DCD	Directive 2019/770 on certain aspects concerning contracts for the supply of digital content and digital services
DGA Proposal	Proposal for a Regulation of the European Parliament and of the Council on European Data Governance
DSM	Digital Single Market
e-Privacy Directive	Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector
ECHR	European Convention of Human Rights
GDPR	General Data Protection Regulation
TFEU	The Treaty on the Functioning of the European Union

§ 1. INTRODUCTION

1.1. BACKGROUND

Personal data is increasingly regarded as a tradable asset as surveillance capitalist companies gain economic power.[1] Accordingly, de facto value of personal data can be noticed even in physical goods and services. For instance, Shiru Coffee in Rhode Island allows students to exchange their personal data in consideration of a drink. Students are asked to provide certain personal information, including student number, gender, date of birth, phone number, and nationality, in exchange for their morning coffee.[2] This case illustrates that personal data can be considered an object of contractual obligation through the freedom of contract principle, which means the parties have the right to bind themselves legally with their free choices within the limits of mandatory rules. Inherently, the question should be what are the limits of mandatory rules regarding the contractualisation of personal data, which is protected with strict rules in the EU.

The right to data protection is a matter of fundamental human rights and subject to strict limitations in Europe,[3] which is derived from the interpretation of Art. 8 of the European Convention of Human Rights ("*ECHR*").[4] Accordingly, the perspective of "privacy is priceless and inalienable" affects the processing of personal data in legal transactions.[5] . In the EU, the right to data protection is interpreted similarly with the Council of Europe approach by putting that right under the protection of fundamental human rights. The Court of Justice of the European Union ("*CJEU*") has confirmed this perspective with the Rundfunk decision, which states that "it should also be noted that the provisions of Directive 95/46 insofar as they govern the processing of personal data liable to infringe fundamental freedoms … must necessarily be interpreted in the light of fundamental rights".[6] As a result of this approach, the right to data protection is codified in the Charter of Fundamental Rights of the European Union ("*Charter*")

[1] Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (PublicAffairs 2019) 214.

[2] Is sharing personal data for free java worth the risk?, <https://blog.avast.com/shiru-cafe-offers-free-coffee-for-personal-data > accessed 20 July 2021.

[3] Douwe Korff, *EC Study on Implementation of Data Protection Directive, Comparative Summary of National Laws* (2002) 9 <http://194.242.234.211/documents/10160/10704/Stato+di+attuazione+della+Direttiva+95-46-CE> accessed 11 June 2016.

[4] Nadezhda Purtova, 'Private Law Solutions in European Data Protection: Relationship to Privacy, and Waiver of Data Protection Rights' (2010) 28 Neth. Q. Hum. Rts. 179, 186.

[5] Lucas Bergkamp, 'EU Data Protection Policy' (2002) 18 Computer Law & Security Review 31, 33.

[6] CJEU, Case C-139/01 Österreichischer Rundfunk and Others [2003].

as a fundamental right[7] and the General Data Protection Regulation ("*GDPR*") has been formulated to comply with the Charter. [8]

Interestingly, the EU might have deviated from the consistent approach rooted to the ECHR regarding personal data following the enactment of the Directive 2019/770 on certain aspects concerning contracts for the supply of digital content and digital services ("*DCD*"). Because one of the major novelties in the DCD is identifying the possibility that the consumer can provide or undertake to provide personal data to the supplier in exchange for receiving digital content or digital services. Therefore, consumers are now able to gain access to digital content and digital services with their personal data in contractual relationships, which can be called as data as counter-performance contract ("*DACP contract*").[9] This covers, for instance, personal data such as the consumer's gender, e-mail address, photos etc. By virtue of that possibility, the risk has emerged that personal data is being commercialised within the territory of the EU in opposition to its human right foundations. Although Rec. 24 of the DCD expressly states that a price tag cannot be put on personal data, the Directive has opened the Pandora's Box that involves conflicting points between the monetisation of personal data and its human rights foundations.[10]

1.2. OBJECTIVE

The main purpose of the research is to analyse the relationship between the approaches of the GDPR and the DCD to reveal any conflict between the two regimes by taking a snapshot of current legal framework of the EU. Accordingly, GDPR's approach reflects that personal data must be based on human rights foundations while the DCD's point of view primarily considers freedom of contract principle. Furthermore, the research seeks solutions to reconcile the conflicts if at all.

1.3. LITERATURE REVIEW

Consumers had already been using their personal data in practice to have access to digital content and digital services prior to the adoption of the DCD. That is to say, the data-driven

[7] Orla Lynskey, *The Foundations of EU Data Protection Law* (First edition, Oxford University Press 2015) 39.

[8] ibid 36.

[9] Narciso uses the phrase "gratuitous digital content contracts" in order to signifying no monetary price in exchange for digital content or service. Madalena Narciso, '"Gratuitous" Digital Content Contracts in EU Consumer Law' [2017] EuCML 9, 198.

[10] Christiane Wendehorst, 'Personal Data in Data Value Chains – Is Data Protection Law Fit for the Data Economy?' in Reiner Schulze and Dirk Staudenmayer (eds), *Data as Counter-Performance - Contract Law 2.0?: Münster Colloquia on EU Law and the Digital Economy V* (Nomos 2020) 193; Rebekka Weiß, 'Data as Counter-Performance & the Digital Content Directive – The End of a Debate?' in Reiner Schulze and Dirk Staudenmayer (eds), *Data as Counter-Performance - Contract Law 2.0?: Münster Colloquia on EU Law and the Digital Economy V* (Nomos 2020) 280.

economy has monetised the personal data in at least three contexts without having a dedicated legal framework: "(i) in exchange for the free or discounted provision of online services, (ii) in exchange for the free or discounted provision of (valuable) online content, (iii) and in exchange for a free or discounted provision of an "offline" services" [11] (Shiru Coffee example). However, the emergence of new business models and their reliance on personal data have forced the legislator to provide a new legal framework that acknowledges the possibility of providing personal data in exchange for digital contents and services.[12] Therefore, consumer's lack of protection about their provision of personal data in return for digital content and digital services could be eliminated with a regulation that provides them with certain rights.

It is widely recognised that the EU has pursued the combination of the objectives of both right to data protection and free flow of personal data in legal instruments related to data protection. Serving the aim to ensuring free flow of personal data, the EU has issued the Digital Single Market ("*DSM*") Strategy. [13] A significant agenda topic of the DSM strategy was regulating digital content and digital services. Consequently, they are regulated under the Digital Content Directive in harmony with the DSM Strategy.[14] With this Directive, the EU legislator has provided consumers with certain rights and remedies while they are using their personal data as counter-performance. Therefore, the monetary value of personal data has been identified in contractual relations.

The European Commission's proposal of the DCD explicitly acknowledged that personal data to be provided actively by the consumer can be used as counter-performance instead of money in the contracts of digital content and digital services.[15] This provision was heavily criticised by scholars, data protection advocates, and the EDPS due to its deviation from the already established data protection framework.[16] Because the framework does not expressly let personal

[11] Gianclaudio Malgieri and Bart Custers, 'Pricing Privacy – the Right to Know the Value of Your Personal Data' (2018) 34 Computer Law & Security Review 289, 292.

[12] Sloboda Midorović and Miloš Sekulić, 'A New Function of Personal Data in the Light of the Contract for the Supply of Digital Content and Digital Services' (2019) 53 Zbornik radova Pravnog fakulteta, Novi Sad 1145, 1155.

[13] 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/2015/0192 final) 4.2.

[14] Giuseppe Versaci, 'Personal Data and Contract Law: Challenges and Concerns about the Economic Exploitation of the Right to Data Protection' (2018) 14 European Review of Contract Law 374, 377.

[15] Art. 3(1) of the Proposal (09.12.2015) for a Directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content: "This Directive shall apply to any contract where the supplier supplies digital content to the consumer or undertakes to do so and, in exchange, a price is to be paid or the consumer actively provides counter-performance other than money in the form of personal data or any other data."

[16] Paula Giliker, 'Adopting a Smart Approach to EU Legislation: Why Has It Proven So Difficult to Introduce a Directive on Contracts for the Supply of Digital Content?' in Tatiana-Eleni Synodinou and others (eds), *EU Internet Law in the Digital Era: Regulation and Enforcement* (Springer International Publishing 2020) 299; EDPS,

data is being an object of commercial transactions instead of money. Furthermore, this proposal was ignoring the current regime for data protection by introducing some rights that were already regulated in the GDPR.[17]

In line with these critiques, the wording of the provision regulating the inclusion of personal data as a counter performance has been changed and the expression of "counter performance" has been removed. However, it was still questionable whether this "make-up" has solved the problem or not[18] since many still use the notion of contracts with data as counter-performance.[19] In order to prevent further debates, it is added in the Rec. 36 DCD that the Directive shall be without prejudice to the GDPR and the Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector ("*e-Privacy Directive*"). Although at first glance the alteration of wording was seen as a solution of the problem, these provisions have not been able to prevent the emergence of legal disputes within the intersection area between the GDPR and the DCD.

It is still believed that considering personal data as an object of contract under the DCD leads to the conclusion that it is a way of legitimising the monetisation of personal data in the legal framework. In this context, the critiques focus on the compatibility of freedom of contract principle with the well-set human rights approach to personal data.[20] That is to say, the DCD has arguably deviated from the fundamental rights approach adopted by the GDPR and the e-Privacy Directive despite the EU underlines that approach in almost every regulation touching personal data.[21] Then, the question is raised in the literature whether the EU accepts legally that personal data can be monetised.[22]

In the literature, many pointed out that the GDPR and the DCD have two divergent perspectives, and these are not comfortable with each other but there is no solution yet regarding how these two perspectives can coexist together.[23] One of the proposals for these problems is that the DCD

'Opinion 4/2017 on the Proposal for a Directive on Certain Aspects Concerning Contracts for the Supply of Digital Content' (2017) paras 14, 18, 29.

[17] Midorović and Sekulić (n 12) 1160.

[18] ibid 1156; Giliker (n 16) 310.

[19] Axel Metzger, 'Data as Counter-Performance' [2017] Journal of Intellectual Property, Information Technology and Electronic Commerce Law 1, 3; Karin Sein and Gerald 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' (2019) 15 European Review of Contract Law 257, 263.

[20] Midorović and Sekulić (n 12) 1156.

[21] Versaci (n 14) 379.

[22] Midorović and Sekulić (n 12) 1147.

[23] *Versaci* argues that issue of commodification of personal data has not been deeply investigated in the European context. Versaci (n 14) 382. According to *Efroni*, [the] "tension between the two regimes, which has been intensively discussed in the literature but not yet conclusively resolved". Zohar Efroni, 'Gaps and Opportunities: The Rudimentary Protection for "Data-Paying Consumers" Under New EU Consumer Protection Law' [2020] Common Market Law Review 806.

should be applied only provided that the consumer "*actively imparted his personal data*" to the supplier.[24] However, this approach is not intended for analysing the relationship between the DCD and the GDPR. In addition, *Janeček* and *Malgieri* developed the *dynamically limited alienability rule* to establish a link between data protection laws and contract law rules and principles.[25] Indeed, this perspective has not formed a new interpretation for the decent application of the DCD but systematized the conditions regarding processing of personal data in the GDPR. Besides, *Sattler* states that the incompatibilities in question should be resolved by courts –especially by the CJEU- as the bridge builder.[26] According to him, European institutions are well aware of the conflicts in the trialogue phase of the Directive. Thus, the task to resolve the incompatibilities -he called it "*hot potato*"- should be transferred to courts. Since this opinion is related to the adoption of already identified reconciliation, it is still unanswered the questions of what the conflicting points are and how we can reconcile them.

1.4. MAIN RESEARCH QUESTION AND SUB-QUESTIONS

In the paradigm of the stated aim and the determined literature gap, this research answers the following main research question:

> Is there a conflict between the DCD's regime of regulating personal data as an object of commercial transaction and the GDPR's approach where personal data must be protected based on human rights foundations? If yes, how can this conflict be reconciled?

In order to build towards a comprehensive answer to this question, the following sub-questions must be dealt with first:

> 1. Under which circumstances can the personal data of the consumer be used as counter-performance under the GDPR?
>
> 2. In which conditions can personal data be used as counter-performance under the DCD?
>
> 3. Are there any conflicting points between the approaches of the GDPR and the DCD?
>
> 4. How can the identified conflicts be reconciled if at all?

[24] Midorović and Sekulić (n 12) 1156.

[25] Václav Janeček and Gianclaudio Malgieri, 'Commerce in Data and the Dynamically Limited Alienability Rule' (2020) 21 German Law Journal 924.

[26] Andreas Sattler, 'Neues EU-Vertragsrecht für digitale Güter' [2020] Computer und Recht 145, para 55.

The first and second sub-question are separately answered respectively in Chapters 1 and 2, third and fourth questions are answered in Chapter 3.

1.5. LIMITATIONS AND PERSPECTIVE

The first and foremost element that defines this thesis's context is the contractual relationship in which the consumer is obligated to provide personal data in return for digital content or services. Accordingly, this thesis focuses on such contractual relationships that may be dubbed as data as counter-performance contracts including both paid and gratuitous ones. The perspective taken by this thesis is essentially data protection law rather than contract law rules. In addition, this thesis focuses on the GDPR and the DCD as the legal framework. On the GDPR side, principles and legal grounds, especially consent, relating to processing of personal data are taken into account as a principal focal point. On the other side, the DCD is solely considered within its data-related provisions. In relation to the legal framework, this thesis focuses on the human rights foundations of the GDPR and the contractual freedom principle behind the DCD. These limitations make it possible to go in-depth rather than summarise multiple legal issues emerging from the interplay between these two legal instruments.

1.6. METHODOLOGY

This thesis is mainly based on doctrinal research methodology with the tools of statutory legislation, academic literature, and case law on data protection law in the EU as well as contract law with a focus on the freedom of contract principle. A doctrinal research methodology encompasses a critical conceptual analysis of applicable rules, selected literature, and case law. Accordingly, related provisions of the DCD and the GDPR are analysed in-depth. The ideas that have been stated in the literature so far and the decisions made by the CJEU regarding the legal value of personal data and digital content and digital services are systematized.

§ 2. TRADING PERSONAL DATA WITHIN THE GDPR

The main aim of this chapter is to determine whether using personal data as counter-performance in contracts related to digital content and digital services is possible or not, solely within the spirit and provisions of the GDPR. In addition, its connecting points with the DCD are also mentioned. In this part, the human rights foundations of the GDPR are reviewed to determine whether it prevents using personal data as object of contracts. Following this, selected principles and possible legal grounds, which are the essential conditions for lawful processing of personal data, are analysed (*the first sub-question*). Consequently, the matter on the possibility of considering personal data in exchange for digital content and digital services is reviewed under the GDPR.

2.1. HUMAN RIGHTS FOUNDATIONS OF THE GDPR

The GDPR is considered as a third-generation regulation on data protection within the EU. It arrived after the enactment of national legislation in the 1970s and the EU Data Protection Directive 95/46/EC.[27] In order to identify whether and to what extent the GDPR has a human rights foundation, related provisions of the TFEU and the Charter, which are the primary sources of the EU Law, must be reviewed. Art. 16 of the TFEU, which is adopted with the Lisbon Treaty, has introduced an explicit legal ground for the enactment of data protection legislation. Accordingly, the EU legislator has ratified the Charter, which introduces a fundamental right to data protection in the Art. 8, and, therefore, the right to data protection is considered as a fundamental right through these legal instruments.

Based on the primary sources of the EU law regarding data protection, the Rec. 1 GDPR refers to the Art. 8 Charter and the Art. 16(1) TFEU. Therefore, it could be argued that the EU's regulatory framework for data protection that also consists of the GDPR, has a 'fundamental rights character'.[28] Even prior to the adoption of the Charter and the GDPR, the CJEU explicitly confirms that the Data Protection Directive 95/46/EC must be interpreted in light of fundamental rights in Rundfunk decision.[29] Similarly, the Article 29 Working Party explicitly states that the EU offers a "minimum and non-negotiable level of privacy protection for all individuals".[30]

[27] University of Cambridge, Centre for Intellectual Property and Information Law, 'European Data Protection - National Laws: Current and Historic' <https://www.cipil.law.cam.ac.uk/resources/european-data-protection-national-laws-current-and-historic> accessed 10 March 2021.

[28] Lynskey (n 7) 38.

[29] CJEU, Case C-139/01 Österreichischer Rundfunk and Others [2003] para. 68.

[30] A29WP, 'Opinion 1/98: Platform for Privacy Preferences (P3P) and the Open Profiling Standard (OPS)' (1998) 2.

Based on human right foundations, it is argued that right to data protection is inalienable and non-waivable.[31] As stated by *Prins*, property rights cannot be embedded in privacy, simply because "privacy is attached to individuals by virtue of their personhood, and, as such, this right cannot be waived or transferred to others".[32] Even if individuals would like to surrender their right to data protection, EU law and in particular the GDPR will not let them do so. The main takeaway from this approach is that contractual relationship between an individual and the controller must be limited with inalienable and non-waivable features.

Considering the human rights character of the GDPR and the regulatory framework behind it, the EU legislator refrains from making an explicit statement either imposing a prohibition on legal transactions involving personal data or enabling individuals to enter into contractual relationships over their personal data.[33] In addition, the contractualisation of personal data cannot be forbidden *ex-ante* due to the fundamental right status of data protection.[34] It can be argued that concluding contracts between individuals and controllers over individuals' personal data would be considered an ordinary circumstance in the age of data-driven economies; however, while doing so, the GDPR and its provisions, particularly those regarding the principles and legal grounds relating to processing of personal data, must be considered. Nevertheless the way on the integration of commercialisation into the GDPR has still uncertainties.

2.2. CONDITIONS DETERMINED IN THE GDPR

Since the supplier of digital content or service determines the purposes and means of the processing of personal data in data as counter-performance contracts, he has to be considered as a controller in the GDPR.[35] This section presents selected principles, and possible legal grounds for the processing activity by the supplier as a controller.

[31] Bergkamp (n 5) 34.

[32] JEJ Prins, 'The Propertization of Personal Data and Identities' (2004) 8 Electronic Journal of Comparative Law 1, 234.

[33] Lynskey (n 7) 40. *Versaci* argues that "the economic exploitation of the right to data protection should not be considered a waiver of the same right." and "the commercial exploitation of personal data can be conceived as an economic dimension of an individual's right to control their personal data, which starts by giving their consent for the processing of their data. Indeed, the same consent is not a waiver of protection, but it is an expression of self-determination." Versaci (n 14) 391.

[34] Versaci (n 14) 386.

[35] For instance, a cloud computing firm might process consumer's personal data to put personalised advertisements on cloud applications through modelling consumer's behaviours. The firm might prefer to analyse its uploaded content via AI-based systems to achieve that purpose. The firm, therefore, determines the purpose and means as a controller.

2.2.1. SELECTED PRINCIPLES

Processing of personal data in the contracts regarding supplying of digital content and digital services should be carried out within the paradigm of the GDPR principles. Violating these principles will generally indicate a significant breach of good faith.[36] Furthermore, the Rec. 48 DCD states that lack of compliance with the GDPR's principles might be considered as "lack of conformity of the digital content or digital service with subjective or objective requirements for conformity provided for in the Directive". Although all principles of the GDPR must be applied to the processing; most related principles to contractual relationship might be chosen as (i) lawfulness, fairness and transparency (ii) purpose limitation, and (iii) data minimisation with certain reasons [37]. Accordingly, these principles are reviewed in terms of possible problems in relation to personal data processing activities under the following titles.

2.2.1.1. Lawfulness, fairness, and transparency

Personal data processing activities should be performed lawfully, fairly, and in a transparent manner according to the Art. 5(1)(a) GDPR. Lawful processing signifies that data processing must respect all applicable legal requirements, within and beyond the GDPR.[38] One of the substantial requirements for lawful processing is based upon a legal ground stipulated under the Art. 6(1) GDPR, three of which are elucidated below. Furthermore, some argue that this part of the principle also covers the conditions for lawful limitations of the right to data protection in light of the Art. 52(1) Charter. Accordingly, processing of personal data should "pursue a legitimate purpose and be necessary and proportionate in a democratic society".[39]

Fair processing requires that personal data should not be processed through unfair ways, e.g., deception or without the data subject's knowledge.[40] That is to say, it aims to prevent adverse effects in processing activities, in particular when conflicting interests between the controller

[36] Philipp Hacker, 'Regulating the Economic Impact of Data as Counter-Performance: From the Illegality Doctrine to the Unfair Contract Terms Directive' in Sebastian Lohsse, Reiner Schulze and Dirk Staudenmayer (eds), *Data as Counter-Performance Contract Law 2.0?* (2019) 70. ibid.

[37] Reasons can be summarised as follows: The lawfulness requires a valid legal ground stipulated under the Art. 6 GDPR, the fairness concerns with the limiting monetisation of personal data, the transparency involves provision of detailed information to consumers about the complex and unfamiliar contractual relationship, determination of purpose is a prerequisite for other principles such as accuracy and data minimisation, and the data minimisation's key terms adequacy and relevance determine the volume and categories of personal data. These are, also, mostly mentioned principles in the literature. Reiner Schulze and Dirk Staudenmayer (eds), *EU Digital Law: Article-by-article commentary* (Nomos 2020) 286; Sergio Cámara Lapuente, 'Termination of the Contract for the Supply of Digital Content and Services, and Availability of Data: Rights of Retrieval, Portability and Erasure in EU Law and Practice' in Sebastian Lohsse, Reiner Schulze and Dirk Staudenmayer (eds), *Data as Counter-Performance - Contract Law 2.0?: Münster Colloquia on EU Law and the Digital Economy V* (Nomos 2020) 176.

[38] Christopher Kuner, Lee A Bygrave and Christopher Docksey (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020) 314.

[39] ibid. Their opinion is based upon the comment made by the European Union Agency for Fundamental Rights and the Council of Europe: European Union Agency for Fundamental Rights and Council of Europe, *Handbook on European Data Protection Law* (2018) 36 et seq.

[40] Kuner, Bygrave and Docksey (n 38) 314.

and the consumer need to be balanced.[41] This rebalance involves adopting *specific procedures* to reach a fair balance between different interests through appealing the notion of *proportionality*.[42] From this point of view, the fairness, by going beyond transparency obligations, is a corrective tool for rebalancing asymmetric relationships and could be linked to processing personal data in an ethical manner.[43] The question related to fairness could be whether controllers should consider any limitations on the monetisation of individual's personal data in accordance with the notion of *proportionality*. Arguably, controllers should consider the worth of the digital content or digital service in data as counter-performance contracts except for gratuitous ones. I.e., identifying a limit for the monetisation of personal data might be a *specific procedure* for data as counter-performance contracts. Therefore, transcending the digital content or service's price in the monetisation process would be regarded as a violation of the fairness principle.

The transparency principle requires that any treatment on the consumer's personal data should be made in a transparent way to them (Rec. 39 GDPR). It does not only cover the information given to the consumer prior to processing but also the information provided to consumers following a request of access to their data.[44] Within this principle, the controller is obliged to provide certain information to consumers according to the Art. 13-14 GDPR.[45] Apart from regulated elements of the certain information to be provided to the consumer, one argues that it should be added a new right to information to Art. 13-14 GDPR.[46] According to this *de lege ferenda* proposal, the controller should also declare and inform individuals about the price of their personal data when collecting them.[47] It is, seemingly, an appropriate proposal to provide individuals with control over their personal data in the data-driven economy. However, it must be underlined that there are many practical and ethical problems related to determining the worth of personal data.[48]

[41] Gianclaudio Malgieri, 'The Concept of Fairness in the GDPR: A Linguistic and Contextual Interpretation' (ACM 2020) 3.
[42] ibid 4–5. "Many commentators argued that the inherent link between proportionality and fairness reflected in the CJEU case-law and in the relationship between Art. 8 and 52 in the Charter." ibid 9.
[43] European Union Agency for Fundamental Rights and Council of Europe (n 39) 119; Malgieri (n 41) 6.
[44] European Union Agency for Fundamental Rights and Council of Europe (n 39) 120. This principle also requires that "any information relating to the processing of personal data be easily accessible and easy to understand, and that clear and plain language be used" (Rec. 39 GDPR).
[45] Kuner, Bygrave and Docksey (n 38) 315.
[46] "in each data processing where the value of customers' personal data is relevant for the economic transaction, the price of these data should be communicated to the consumer." Malgieri and Custers (n 11) 298.
[47] The reason for this proposal is that the value of personal data is relevant for commercial transactions in data as counter-performance contracts. ibid.
[48] ibid 294.

2.2.1.2. Purpose limitation

The purpose limitation principle requires collecting personal data for "specified, explicit and legitimate purposes and not further processing in a manner that is incompatible with those purposes" according to the Art. 5(1)(b) GDPR. *Specification* of purpose is a prerequisite for other principles related to data quality, such as accuracy and data minimisation.[49] *Explicit* purpose determination means that purposes must be explicitly stated to individuals prior to collecting their personal data. Individuals should have no doubt in understanding the purposes and other processing conditions after getting a notice from the controller.[50] *Legitimacy* of purposes has a broader meaning than legality, and it extends to other fields of law and its principles[51] such as human rights foundations of the EU's framework on data protection. From this aspect, inalienable and non-waivable features of right to data protection have a close connection with legitimacy of purposes. Controllers should keep those features in sight while determining the purposes.

In line with the requirements of the principle, the supplier as a controller must define the purpose of processing personal data before processing is started. Accordingly, following subtitles focuses on monetisation purposes, which is closely connected to objectives of data as counter-performance contracts and might be highly likely used in these contracts.

2.2.1.2.1. The purposes related to monetising personal data

The idea of considering personal data as a resource and exchangeable asset was introduced by *Laudon* in 1996, where he argued that data could be bought and sold in a national market.[52] In today's world, emerging technologies have paved the way for new facilities that enable personal data to be exchanged in a wide array of means.[53] Thus, monetisation has been a *de facto* reality in almost all fields of the digital market.[54]

Monetisation of personal data may be materialised through directly selling data to third parties and making profit from them in this way. I.e., the supplier can entirely build his business model upon collecting personal data in order to sell them by complying data protection rules and principles. In terms of purpose limitation principle, it should be considered that the purpose relating to selling personal data must be specific, explicit and legitimate. Apart from directly

[49] A29WP, 'Opinion 03/2013 on Purpose Limitation' (2013) 12.

[50] ibid 17.

[51] "This includes all forms of written and common law, primary and secondary legislation, municipal decrees, judicial precedents, constitutional principles, fundamental rights, other legal principles, as well as jurisprudence, as such 'law' would be interpreted and taken into account by competent courts." ibid 19.

[52] Kenneth C Laudon, 'Markets and Privacy' (1996) 39 Communications of the ACM 92, 93.

[53] Chao Li and others, 'A Theory of Pricing Private Data' (2017) 60 Communications of the ACM 79 <https://dl.acm.org/doi/10.1145/3139457> accessed 26 February 2021.

[54] Malgieri and Custers (n 11) 292; Rafał Mańko and Shara Monteleone, 'Contracts for the Supply of Digital Content and Personal Data Protection (European Parliament Research Service, Briefing)' (2017) 3.

selling it to third parties, the supplier may also appeal to other appropriate means for monetisation. These ways are not exhaustive and can be diversified in accordance with the technological circumstances, since the issue of monetising personal data has been rather technological currently. [55] Most characterised means can be summarised as follows:

As an epitome of monetising personal data in the data-driven world, *the first way* might be where personal data is used for the purpose of targeted online advertisements. Thus, it contributes to the value of the advertising process through rendering advertisements more targeted. *Another way* of using personal data as a resource is the modelling of consumer behaviour. In this way, the controller can use data mining techniques for acquiring consumer data to predict consumer behaviours and extract significant trends from the personal data which is provided by the consumer.[56]

The consumer's data can also be used for tailoring digital content and digital services. Personalisation provides suppliers with the possibility of tailoring different types of content and services to consumers, based on their personal data made available by consumers.[57] Thus, a more sustainable and 'loyal' relationship can be established between the supplier and the consumer to acquire profit in the long term. Moreover, personal data can be monetised in various other ways depending on technological facilities.

2.2.1.2.2. Other purposes

The supplier processes consumers' personal data to *verify their identity* in all types of distance contracts. This purpose is also valid in terms of contracts for the supply of digital content and digital services. Similarly, *ensuring security of digital contents or services* might also require to processing of personal data. For instance, the trader can process users' IP addresses or session data to serve them a decent digital service. Furthermore, these data categories might also be processed for the purpose of *complying with legal requirements* of the national law or the EU law. In line with this aim, the supplier can, e.g., transfer consumers' data to competent authorities.

2.2.1.3. Data minimisation

The principle of data minimisation warrants that personal data processed must be "adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed" according to the Art. 5(1)(c) GDPR. There is a close connection between the

[55] Laura Kemppainen and others, 'Emerging Revenue Models for Personal Data Platform Operators: When Individuals Are in Control of Their Data' (2018) 6 27, 80.

[56] Management Study Guide, Customesr Modeling - Meaning and its Different Aspects, <https://www.managementstudyguide.com/customser-modeling.htm>, last accessed 6 March 2021.

[57] For instance, this tailored service would be a search engine or social network. Malgieri and Custers (n 11) 293.

principle of data minimisation with the principle of purpose limitation.[58] Accordingly, if the processing of personal data is not necessary for the purposes of the processing, it has to be prohibited. While data minimisation principle handles the "inner world" of processing via determining data categories to be processed, purpose limitation deals with identifying purposes without touching upon the content of processing. In the purpose limitation principle, the most important issue is specifying explicit and legitimate purposes of processing. Relatedly, the principle of data minimisation addresses the matter of minimisation of personal data with the terms of adequate, relevant and limited within the specified purposes.[59]

The key question, thus, should be which categories of personal data can be adequate, relevant and limited in terms of purposes related to monetisation of personal data in the contract regarding the supply of digital content and digital services. In terms of the purpose of selling personal data to third parties, adequacy, relevancy and limit may be determined more easily than other substantive purposes, like targeted online advertisements, personalisation of digital content and services etc. Because, other substantive purposes require sophisticated data processing techniques and, therefore, determining the worth of personal data within these purposes might be more complex compared to selling personal data directly to third parties. In sum, even if the purpose is monetising personal data, volume and categories of personal data should be limited in accordance with the key terms of adequacy and relevance.

2.2.2. POSSIBLE LEGAL GROUNDS FOR PROCESSING

The supplier as a controller must consider one of the six possible valid legal grounds for the processing of personal data.[60] Out of the six, the primary focus will be directed towards the consent -Art. 6(1)(a) GDPR-, necessity for the performance of data as counter-performance contracts -Art. 6(1)(b)-, and legitimate interest pursued by the supplier -Art. 6(1)(f)- simply because they are mostly linked grounds to the data as counter-performance contracts.[61]

[58] ibid 298; Sonja Bühler, 'Conditional Consent as a Valid Legal Ground for Data Processing - a Misbelief?' 8, 30.

[59] In the Digital Rights Ireland Case, purposes of processing personal data were considered to satisfying an objective of general interest which are such as to fight organised crime and terrorism. However, not to be limiting personal data categories, was considered problematic. CJEU, Joined cases C-293/12 and C-594/12, Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others [GC], 8 April 2014, pars. 44 and 57.

[60] Rec. 38, 2nd sentence of the DCD: "As a consequence, any processing of personal data in connection with a contract falling within the scope of this Directive is lawful only if it is in conformity with the provisions of Regulation (EU) 2016/679 relating to the legal grounds for the processing of personal data."

[61] Mańko and Monteleone (n 54) 7. Legal obligation as a legal valid basis in the Art. 6(1)(c), is also reviewed in the literature as well as mostly referred those three See: Midorović and Sekulić (n 12) 1157; EDPS (n 16) Par. 65. According to EDPB, an online service provider can base upon the Art. 6(1)(c) after the termination of contract, if he has an obligation to retain personal data for relevant legal claims or legal requirements. 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 (v 2.0)' (2019) para 44.

Therefore, this subsection answers the question of under which conditions these legal grounds might be used in contracts.

On the other hand, conditions of processing special categories of personal data deviates from the conditions of processing of personal data. According to the Art. 9 GDPR, explicit consent can be a legal valid base if it is given in an explicit way, and grounds of performance of contract and legitimate interest are not considered as valid basis for those categories. Because of the deviation, special categories of personal data are excluded in the following parts.

2.2.2.1. Consent of the Consumer

The data subject's consent means "any freely given, specific, informed an unambiguous indication of his wishes by a statement or by a clear affirmative action, which implies agreement to the processing of personal data relating to him or her" (Art. 4(11) GDPR). Many has emphasised that consent is a key legal ground for processing consumer's personal data in data as counter-performance contracts.[62] Moreover, there are many references to consent as one of the possible legal valid grounds in the DCD (Recitals 24, 38, 39 and 40).[63]

Data subject's consent should be specific to prevent function creep, which means "the gradual widening or blurring of purposes" that is a risk for individuals.[64] This is closely linked to the purpose limitation principle, which safeguards against blurring purposes.[65] In terms of data as counter-performance contracts, the purpose of monetisation should be specified at the level of monetisation technique like modelling customer behaviour, profiling, etc. If the purpose is not determined at the level of monetisation technique, suppliers might appeal to other monetisation techniques without noticing consumers, which leads the blurring of purposes in the context of DACP contracts. Similarly, the purpose of selling personal data to third parties can be considered as specific purpose in this context. However, since the EU's legal framework has not been familiar with the commodification of personal data, it is still unclear whether and to what extent details of selling purpose should be determined, and consumers should be informed in this direction. In addition, to meet the requirement of being 'specific', the controller should

[62] Schulze and Staudenmayer (n 37) 73, 276; Janeček and Malgieri (n 25) 12.

[63] Recital 24: "(…) The personal data could be provided to the trader either at the time when the contract is concluded or at a later time, such as when the consumer gives consent for the trader to use any personal data that the consumer might upload or create with the use of the digital content or digital service. (…)"

Recital 38: "(…) Where processing of personal data is based on consent, in particular pursuant to point (a) of Article 6(1) of Regulation (EU) 2016/679, the specific provisions of that Regulation including those concerning the conditions for assessing whether consent is freely given apply. (…)"

Recital 39: "The right to erasure and the consumer's right to withdraw consent for the processing of personal data should apply fully also in connection with the contracts covered by this Directive. (…)"

Recital 40: "This Directive should not regulate the consequences for the contracts covered by this Directive in the event that the consumer withdraws the consent for the processing of the consumer's personal data. (…)"

[64] EDPB, 'Guidelines 05/2020 on Consent under Regulation 2016/679 (v1.1)' (2020) 14.

[65] A29WP, 'Guidelines on Consent under Regulation 2016/679' (2018) 12.

obtain a separate consent for each purpose by providing certain information.[66] For instance, if the means of monetisation changes, e.g., from modelling customer behaviour to selling consumer's personal data to third parties, the supplier as the controller has to seek additional consent or another lawful basis for this purpose.

The Art. 7 GDPR presents requirements of legally binding consent that also seem as difficulties in data as counter-performance contracts.[67] This part of the thesis discusses solely problematic requirements of consent which stems from the conflict between the DCD and the GDPR.[68] According to the Art. 13, 14 and 15 GDPR, data subjects should be informed regarding processing activities. In the context of data as counter-performance contracts, the supplier has to give reasonable explanations on the issue. Since the Art. 7(2) GDPR requires that written request for consent shall be distinguishable from the other matters such as consent to contract, personal data processing conditions must be explained to the consumer in a different layer than the contract.[69] For instance, controller might create a dynamic two-layer web page where in the first layer the consumer could accept the conditions of contract, and in the second layer he could give consent to the conditions of processing of personal data. Therefore, the dividing line between consent to contract and consent to processing might be created in a clear manner in practice.

The phrase "freely given" has a significance in cases where the consent is legal ground.[70] Assessment of "freely given consent" requires reviewing concerns such as data subject's vulnerable position, imbalance due to lack of real choice, and arising damage when withdrawing the consent.[71] *First of all*, there is an imbalance between the controller and the data subject's due to the latter's weaker bargaining position, and thus he might not have the possibility to claim his own interests in the contract.[72] Although contracting parties are at equal in theory, it is still debateable whether this will occur in practice e.g. a contract on over-the-top

[66] ibid.

[67] Midorović and Sekulić (n 12) 1158.

[68] According to *Robert-Smith*, the challenge here is reconciling the tough conditions set by the GDPR -and in a near future by the new ePrivacy regulation- about the consent's validity. Romain Robert and Lara Smit, 'The Proposal for a Directive on Digital Content: A Complex Relationship with Data Protection Law' (2018) 19 ERA Forum 159, 10.

[69] See for the relationship distinction of consent to contract and consent to processing: Cemre Bedir, 'Contract Law in the Age of Big Data' (2020) 16 European Review of Contract Law 347, 357. Rec. 39 of the DCD also emphasises the distinction between those two layers: "(…) The right of the consumer to terminate the contract in accordance with this Directive should be without prejudice to the consumer's right under Regulation (EU) 2016/679 to withdraw any consent given to the processing of the consumer's personal data."

[70] Rec. 38 of the DCD states the importance of the notion 'freely given' as follows: "(…) Where processing of personal data is based on consent, in particular pursuant to point (a) of Article 6(1) of Regulation (EU) 2016/679, the specific provisions of that Regulation including those concerning the conditions for assessing whether consent is freely given apply. This Directive should not regulate the validity of the consent given.(…)"

[71] Bühler (n 58) 26.

[72] EDPS (n 16) para 59; Bühler (n 58) 26.

content between the consumer and the big tech company. Therefore, this imbalance is needed to be taken into account when determining whether the consent is freely given.[73]

Secondly, another imbalance exists if the consumer has no genuine choice whether or not to give consent.[74] The existence of alternatives should be considered for assessing free choice of the individual regarding consent.[75] To do this, the consumer should be able to choose from the options, which are paying a price or using his personal data as-counter-performance, in cases where the digital service includes paid-for premium option. Put differently, the consumer should not be pushed to the option of paying with personal data by the supplier.

Finally, consent can be considered as a valid legal ground, if it can be withdrawn without any type of detriment such as "deception, intimidation, coercion or significant negative consequences".[76] The right to withdraw consent, which has a prominent place in the GDPR[77], is a consequence of the requirement of 'freely given consent'.[78] In theory, this right can be seen as a safeguard for consumers, but which in practice might fail. Because, personal data in data as counter-performance contracts can already be monetised quickly right before the withdrawal of consent. Although withdrawal of consent only has consequences from the moment of withdrawal and does not invalidate the processing that has occurred before, the fact of quick monetisation might dilute the effectiveness of right to withdraw.[79]

It is debateable whether the consent is still freely given according to the Art 7(4) GDPR in a case where consent is withdrawn, and the contractually due performance is no longer delivered.[80] Being due performance that is no longer delivered is a consequence of a contract that is *synallagmatic*[81]. Suppose the consumer would like to proceed with the contractual relationship without providing personal data after the consent is withdrawn. In that case, the controller should provide consumers with a right to proceed with a contractual relationship by paying a price in cases where the digital service includes paid-for premium option. At the time of withdrawal of consent, the consumer should have options to proceed with or terminate the

[73] Because, as stated in the Rec. 43 GDPR "consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller."

[74] Bühler (n 58) 26; EDPB, 'Guidelines 05/2020 on Consent under Regulation 2016/679 (v1.1)' (n 64) para 24.

[75] EDPS (n 16) para 60.

[76] Bühler (n 58) 27; (n 37) 73.

[77] EDPB, 'Guidelines 05/2020 on Consent under Regulation 2016/679 (v1.1)' (n 64) para 112.

[78] Martin Schmidt-Kessel, 'Right to Withdraw Consent to Data Processing The Effect on the Contract' in Reiner Schulze and Dirk Staudenmayer (eds), *Data as Counter-Performance - Contract Law 2.0?: Münster Colloquia on EU Law and the Digital Economy V* (Nomos 2020) 139.

[79] EDPS (n 16) para 69; Dirk Staudenmayer, 'The Directives on Digital Contracts: First Steps Towards the Private Law of the Digital Economy' 32, 227.

[80] Schulze and Staudenmayer (n 37) 73.

[81] "A contract in which the parties obligate themselves reciprocally, so that the obligation of each party is correlative to the obligation of the other." Bryan A Garner (ed), *Black's Law Dictionary* (8th edn, 2004) 987.

contract, in line with the requirements of 'freely given consent'. Furthermore, the contract might contain a clause envisaging the possibility of withdrawal of consent, and of describing the consequences of withdrawal, including switching to paying with money. Therefore, detrimental sides of withdrawal of consent might be eliminated in data as counter-performance contracts, and thus the possibility of violating the contract might be diminished. Besides, since the contractual relationship has a synallagmatic feature, the necessity to pay the price after withdrawal of consent should not be considered as a detrimental consequence even if the parties cannot agree upon contractual provisions regarding withdrawal of consent. In sum, having met the conditions which should be assessed case-by-case set out in the Art. 7 GDPR, the controller can rely on consent. [82]

2.2.2.2. Necessity for the Performance of a Data as Counter-Performance Contract

The Art. 6(1)(b) GDPR stipulates that "if processing is necessary for the performance of a contract to which the data subject is party", the controller can use this contractual relationship as a valid legal ground for processing. This legal ground is referred as a general contract privilege of data protection law.[83] The mandatory element for this legal ground is the "necessity"[84], which refers to more than just the scope and conditions of processing in a clause of contract.[85] That is to say, the controller cannot rely on the Art. 6(1)(b) for every type of processing activity that occurs in the contractual relationship. In order to identify whether processing of personal data is necessary, the EDPB forwards a question: are there any less intrusive alternatives for processing?[86] "If there are realistic, less intrusive alternatives, the processing is not 'necessary', and Article 6(1)(b) will not cover the processing".[87] For instance, if the contract can also be performed without processing of specified categories of personal data, this legal ground cannot be considered valid.

---

[82] EDPS (n 16) para 62.

[83] Schmidt-Kessel (n 78) 132.

[84] 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 (v 2.0)' (n 61) para 24; EDPS (n 16) para 57.

[85] 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 (v 2.0)' (n 61) para 27. According to EDPB, mentioning to profiling in contracts alone does not make it 'necessary' for the performance of the contract (ibid 35.). *Hacker* signifies the risk of using Art. 6(1)(b) that enables including broad service obligations in contracts to legitimise subsequent data processing. Hacker (n 36) 68.

[86] EDPB has also stated a non-exhaustive list in terms of applicability of the Art. 6(1)(b) in the Guidelines: "What is the nature of the service being provided to the data subject? What are its distinguishing characteristics? What is the exact rationale of the contract (i.e. its substance and fundamental object)? What are the essential elements of the contract? What are the mutual perspectives and expectations of the parties to the contract? How is the service promoted or advertised to the data subject? Would an ordinary user of the service reasonably expect that, considering the nature of the service, the envisaged processing will take place in order to perform the contract to which they are a party?" 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 (v 2.0)' (n 61) para 33.

[87] ibid 25.

As regards the monetisation purpose, EDPB's two cases might lead the way for suppliers within data as counter-performance contracts. The first case is related to online behavioural advertising which includes tracking and profiling of data subjects. Due to the fact that the "controller has not been contracted to carry out profiling, but rather to deliver specified goods and services", performance of the contract is not a suitable legal ground.[88] In addition, Article 6(1)(b) cannot provide a valid legal basis for online behavioural advertising because such an activity *indirectly* funds the provision of the service.[89] To come back to our case -data as counter-performance contracts- the main obligation of suppliers is to deliver particular digital content or digital services similar to the EDPB's example. Furthermore, processing consumer's personal data for online behavioural advertising *directly* funds the provision of digital service providers like Facebook. Hence, it can be concluded that EDPB's negative approach to Art. 6(1)(b) in online behavioural advertising is also applicable for our case.

Another example of what is meant by necessity is in a case that consists of processing for personalisation of content. The EDPB acknowledges that personalisation might establish an "intrinsic and expected element" of particular online services.[90] Accordingly, processing of personal data for content's personalisation may be considered as necessary for the performance of the contract in certain cases. If personalisation of content is not a core feature of utilising the service, if it is solely for increasing user engagement, controllers must rely on an alternative lawful basis where applicable. Similar with the EDPS's approach, personalisation of content might not be necessary element for the contractual relationship since the personalisation may not be a core feature of utilising the service, particularly in cases where the trader has chosen a monetisation technique different from personalisation of content.

Since the processing of personal data makes the provided service or content free of charge[91] in data as counter-performance contracts, it is necessary to answer the questions of how to define and who should define the term 'necessary' to perform a contract[92]. It can be argued that the consumer can always pay a price instead of providing personal data in return for receiving digital content or service. Since paying a price might be considered a less intrusive alternative for processing, the purposes related to monetisation of personal data cannot be regarded as necessity for the performance. Therefore, controllers may seek to differentiate the structure of the offered service and provide paid-for premium service[93] in order to rely on the Art. 6(1)(b).

[88] EDPB refers to A29WP Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC (WP217). ibid 51.

[89] ibid 53.

[90] ibid 57.

[91] Weiß (n 10) 280.

[92] Mańko and Monteleone (n 54) 9.

[93] Mateja Durovic and Marco Montanaro, 'Data Protection and Data Commerce: Friends or Foes?' (2021) 17 European Review of Contract Law 1, 31.

In addition to this "less intrusive alternative" concern, there is another significant consideration regarding the obligations of the parties.

Many argue that Art. 6(1)(b) is not applicable for data as counter-performance contracts since providing personal data is not a part of the supplier's performance, but rather the consumers'.[94] Like receiving a price from the consumer, the supplier has the obligation of accepting the consumer's performance. After that, the supplier can choose to monetise or not to monetise the data subject's data. In other words, preferring not to monetise consumer's data does not violate the contractual duties of the supplier. An analysis from that perspective could close the door of processing based on 'necessity for the performance' to suppliers.

Conversely, many advocate that personal data might be counter-performance and, therefore, they should be considered as necessary for the performance of contract.[95] According to *Schmidt-Kessel*, since the performance of the contract is not restricted to duties and obligations of the controller, it would also cover duties and obligations of the data subject.[96] EDPB's foreseeability and necessity criteria can be used to support their idea. Accordingly, sending formal reminders about due payments in a normal contractual relationship[97] is not different from processing of personal data for monetisation purpose in a data as counter-performance contract.

In sum, connections exist between the data as counter-performance contract and the necessity for processing of personal data, however, there is no certain conclusion in view of obligations of parties until the CJEU's prospective analysis. In this regard, the case waiting before the CJEU, which is related to Facebook's 'contractual advertisement duty' and elaborated in the fourth chapter (4.4.), will shed light on the issue.[98]

2.2.2.3. Legitimate Interests Pursued by the Supplier

Legitimate interest is one of the six lawful grounds on which a controller can rely. Art. 6(1)(f) GDPR stipulates that personal data may be processed in a lawful manner if it "is necessary for the purposes of the legitimate interests pursued by the controller, except where such interests

[94] Janeček and Malgieri (n 25) 12; Mańko and Monteleone (n 54) 9. Article 29 Working Party has also clarified that the provision of Art. 6(1)(b) GDPR "must be interpreted strictly and does not cover situations where the processing is not genuinely necessary for the performance of a contract, but rather unilaterally imposed on the data subject by the controller." A29WP, 'Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC' (2014) 16. See also Fryderyk Zoll, 'Personal Data as Remuneration in the Proposal for a Directive on Supply of Digital Content' in Reiner Schulze, Sebastian Lohsse and Dirk Staudenmayer (eds), *Contracts for the Supply of Digital Content: Regulatory Challenges and Gaps* (2017) 182.

[95] Robert and Smit (n 68) 10.

[96] Schmidt-Kessel (n 78) 133.

[97] 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 (v 2.0)' (n 61) para 38.

[98] Facebook's GDPR bypass reaches Austrian Supreme Court, <https://noyb.eu/en/facebooks-gdpr-bypass-reaches-austrian-supreme-court> accessed 9 April 2021.

are overridden by the interests or fundamental rights and freedoms of the data subject which require protection". Similar with the contract as a legal ground, legitimate interest has also been controversial in the literature.[99]

In order to consider legitimate interest as a legal basis for monetisation purposes, three tests determined by the Article 29 Working Party must be carried out.[100] To begin with, the question whether data processing is necessary for the purpose intended by the supplier, has to be analysed (*necessity test*). If there are other less invasive ways available to serve the same aim, such as differentiating the structure of the offered service and providing paid-for premium service[101] which is similar with the necessity test in the contract, Art. 6(1)(f) cannot be used as a legal ground.[102] In addition, pursued interest of the controller at stake must be assessed with respect to legitimacy (*legitimacy test*). Accordingly, identifying the threshold for what constitutes a legitimate interest has to be determined.[103] That interest must necessarily be lawful, sufficiently clear, and represents a real and present interest.[104]

Furthermore, the *balancing test* has to be carried out by the supplier. As regulated under the Rec. 47 and Art. 6(1)(f) GDPR, "legitimate interests of controllers cannot override the fundamental rights and freedoms of data subjects". The balancing test should have an optimal balance between the legitimate interests of controllers and the fundamental rights and freedoms of data subjects, and to "additional safeguards applied by the controller to prevent any undue impact on the data subjects".[105] The CJEU has highlighted that the data subject's fundamental rights override, as a rule, economic interests of the operator, as in the Google Spain Case.[106] Nevertheless, general interests of the supplier such as direct marketing may be accepted as legitimate.[107] Accordingly, controllers may have a legitimate interest to know their consumers'

[99] Janeček and Malgieri (n 25) 12.

[100] ibid.

[101] Durovic and Montanaro (n 93) 31.

[102] A29WP, 'Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC' (n 94) 29.

[103] ibid 24.

[104] ibid 25.

[105] ibid 30; Janeček and Malgieri (n 25) 13.

[106] "[…] in the light of his fundamental rights under Articles 7 and 8 of the Charter, […] it should be held […] that those rights override, as a rule, not only the economic interest of the operator of the search engine but also the interest of the general public in finding that information upon a search relating to the data subject's name." CJEU, Case C-131/12 Google Spain [2014] para. 97.

[107] An example from Rec. 47 of the GDPR might be considered as another pro-argument: "Such legitimate interest could exist for example where there is a relevant and appropriate relationship between the data subject and the controller in situations such as where the data subject is a client or in the service of the controller."

preferences, and, thus, offer goods and services that better fulfil the desires of the consumers by refraining from unduly monitoring online or offline activities of their consumers.[108]

Having regarded all of the aforementioned considerations, it must be highlighted that three-step test makes it difficult to use legitimate interest as a legal ground for exchanging personal data in lieu of paying a price.[109] So, it is arguable that the possibility regarding the applicability of legitimate interest is limited.[110] While comparing the three possible legal grounds, it can be argued that the most suitable valid legal ground would be the consent since contract and the legitimate interest have controversial issues and practical challenges. Furthermore, the consent also serves the autonomy of individuals regarding personal data,[111] then controllers should be based on consent rather than contract and legitimate interest.

2.3. CONCLUDING REMARKS

The GDPR does not expressly prohibit nor allow the possibility of considering personal data as counter-performance in exchange for digital content and digital services, although it has human rights concerns. The fundamental rights character of the GDPR, which includes inalienable and non-waivable features, has to be considered in data as counter-performance contracts since it is a public law instrument of the EU. Therefore, having met the conditions set out in the GDPR and respecting to its human rights foundations, it is possible to use personal data to exchange digital content and digital services.

As regards to the principles, the fairness principle can be used to limit unfair monetisation in accordance with the notion of *proportionality*. As a part of the purpose limitation principle, specified, explicit and legitimate purposes must be identified prior to the processing of personal data by the supplier as a controller. The primary purpose pursued by the supplier as a controller in the data as counter-performance contracts is to monetise the consumer's personal data made available by him. It can be materialised through directly selling data to third parties or other appropriate means such as targeted online advertisements. Notions of adequacy and relevance that are part of the data minimisation principle should be used to determine the data categories to be processed in data as counter-performance contracts.

In terms of freely given consent, the supplier should provide individuals with genuine choices that should be included in the options of paying with a price and paying with personal data. In the event of consent's withdrawal, the consumer should have a right to proceed with the

[108] A29WP, 'Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC' (n 94) 25, 26.

[109] Janeček and Malgieri (n 25) 13.

[110] Robert and Smit (n 68) 11. "The use of 'legitimate interest' as a legal basis for monetization purposes is problematic, especially as regards the necessity test" Janeček and Malgieri (n 25) 12.

[111] Schmidt-Kessel (n 78) 135.

contractual relationship with a possibility of paying a price in paid digital content and digital services. Using ‘necessity for the performance of the contract’ as a legal valid ground might be problematic since paying a price might be considered a less intrusive alternative for processing. In addition, The CJEU’s prospective analysis will be critical on determining conditions of that legal ground. As regards to legitimate interest, a case-by-case analysis, which its conditions of that is determined by the Article 29 Working Party, is necessary.

It seems that consent is the most appropriate valid legal ground for the processing, compared to the grounds of performance of contract and legitimate interest. However, it also might have problematic elements within the context of data as counter-performance contracts. To conclude, a case-by-case assessment is necessary to determine whether the processing activity meets the requirements of the GDPR.

§ 3. PERSONAL DATA AS OBJECT OF CONTRACTUAL OBLIGATION WITHIN THE DIGITAL CONTENT DIRECTIVE

The main aim of this chapter is to determine the conditions of using personal data as counter-performance from contractual point of view within the provisions of the DCD. In this chapter, the DCD's approach regarding personal data, contracting parties, and subject matter of contractual relationship are analysed to identify the essential conditions for using personal data as counter-performance under the DCD (*the second sub-question*). Finally, some conclusions are drawn in the final section regarding the contractual relationship.

3.1. THE DCD'S APPROACH REGARDING PERSONAL DATA

The DCD entered into force with the aim of creating a stable contract law environment for both consumers and traders within the DSM strategy. Accordingly, the EU expressly stipulates fields of digital content and digital services with the DCD, which is a maximum harmonisation directive. It recognises the notion of the digital consumer[112] and aims to ensure digital consumers have better access to digital content and digital services (Rec. 1). By doing so, the DCD is based on the principle of freedom of contract, which means parties have the right to bind themselves legally with their free choices regarding with whom and on which terms they want to conclude contracts, within the limits of mandatory rules, and therefore their choices should not be interfered by external control such as the state.[113] For instance, Article 7(1) DCD regulates that the conformity of digital content or digital service should be determined by the terms of the contract. On the other hand, this principle prohibits parties to reach a result that is most favorable to the consumer as the weaker party.[114]

One of the essential novelties provided in the DCD, relying on that principle, is identifying the possibility of using personal data as counter-performance in exchange for supplying digital content and digital services in contracts. Apart from the paid ones, this novelty also embraces so-called "gratuitous contracts", in which the consumer is not obliged to pay monetary price in return for digital content or services, e.g., free social media and cloud storage applications.[115]

[112] Midorović and Sekulić (n 12) 1153. Narciso call consumers as "non-paying consumers" in gratuitous contracts. Narciso (n 9) 200.

[113] Garner (n 81) 1959; Alan Schwartz, 'Justice and the Law of Contracts: A Case for the Traditional Approach' 108 <https://digitalcommons.law.yale.edu/fss_papers/1122> accessed 22 June 2021.

[114] Prins (n 32) 3.

[115] Narciso (n 9) 200. According to the aim of the proposal of the DCD is recognising same rights for the so-called 'free services'. See: EDPS, 'Opinion 8/2018 on the Legislative Package "A New Deal for Consumers"' (2018) 11.

3.2. CONDITIONS DETERMINED IN THE DCD

The DCD merely regulates contracts regarding supplying digital content and digital services.[116] In case of no contractual relationship between the trader and the consumer, the DCD cannot be applied.[117] For instance, an advertisement exposition that gives access the consumer to a digital content or service falls outside of the DCD provided that there is no contractual relationship (Rec. 25). On the contrary, the GDPR is still applicable for that context since it does not require a contractual relationship as such. Whether the relation between parties forms a contract or not will be determined by national contract laws, according to Art. 3(10) of the DCD.[118]

3.2.1. CONTRACTING PARTIES

The legal definitions of parties determine the DCD's personal scope of application. It merely covers business-to-consumer (B2C) relations rather than business-to-business (B2B) transactions. For the business side, the EU legislator prefers the term of 'trader' instead of the term of 'supplier' to avoid interference with the boundaries of national contract laws.[119] According to Art. 2(5) of the DCD, the trader is "a natural or legal person that is acting for purposes relating to that person's trade, business, craft, or profession". In other respects, the term 'consumer' has been defined in an identical way to the precedent set by consumer law directives such as the 2011/83/EU Consumer Rights Directive. According to Art. 2(6) of the DCD, a consumer is "natural person who is acting for purposes which are outside that person's trade, business, craft, or profession".

3.2.2. SUBJECT MATTER OF THE CONTRACT

The characteristic contractual obligation in contracts covered by the DCD is the supplying of digital content and digital service which is the trader's main obligation. The Directive prioritizes the rights of consumers in contrast to those of traders because of the lack of bargaining power of consumers, which affects party autonomy in a negative manner.[120] For instance, while the main obligation of the trader is elucidated in the Art. 5 which stipulates the supplying of digital content and digital service, the Directive does not have such an article regulating the main

[116] Sein and Spindler (n 19) 260.

[117] Axel Metzger, 'A Market Model for Personal Data: State of Play under the New Directive on Digital Content and Digital Services' in Sebastian Lohsse, Reiner Schulze and Dirk Staudenmayer (eds), *Data as Counter-Performance - Contract Law 2.0?: Münster Colloquia on EU Law and the Digital Economy V* (Nomos 2020) 30.

[118] Rec. 12: "This Directive should not affect national law to the extent that the matters concerned are not regulated by this Directive, such as national rules on the formation, validity, nullity or effects of contracts or the legality of the digital content or the digital service.(…)"

[119] Reiner Schulze and Dirk Staudenmayer (eds), *EU Digital Law* (Nomos 2020) Art 3 para 11.

[120] Bedir (n 69) 351.

obligation of the consumer. In other words, it is not regulated whether the trader has a right to claim the consumer's data in the case where data is not supplied by the consumer.[121]

The Directive covers the cases where the consumer pays a price or provides personal data to the trader in exchange for receiving digital content and digital services. However, there is no answer to the relationship between consumer's obligations and trader's obligations. Put differently, the question of whether this contractual relationship includes 'synallagmatic' feature, which means each party's obligation is correlated with the other ones in a reciprocal way, is not acknowledged expressly in the Directive. If there is an existence of synallagmatic relationship, the trader can request the consumer's performance of the obligation on providing personal data unless differently agreed in the contract. Otherwise, the trader cannot request the consumer's performance. *Metzger* claims that this issue belongs to the discretion of member states[122]. His argument is based upon the removing of wording 'counter-performance' from the Commission's proposal on the DCD,[123] which also means removing the synallagmatic feature. However, considering that that removal was not affected to substance matter of the article, but rather form of statement; the meaning and scope of the Art 3(1) has not been changed.[124] Accordingly, many argue convincingly that the contractual relationship is synallagmatic, and therefore parties can request each other's performance of obligations when respondent party is in default.[125] The conditions of those requests are subject to national laws.

3.2.2.1. Supplying digital content and digital service

The proposal of the DCD had avoided making a distinction among digital materials. Afterwards, to merely clarify the scope of the DCD, they are distinguished into two categories as digital content and digital services and defined in a broad manner by the approach that is technologically neutral.[126]

Digital content is defined in a broad manner as "data which are produced and supplied in digital form" according to the Art. 2(1). Based on the broad definition, video files, music files, e-books or other e-publications, audio files, applications, and computer programmes are covered by the

[121] Sein and Spindler (n 19) 265.

[122] Metzger (n 117) 38.

[123] European Commission's Proposal for a Directive of the European Parliament and of the Council on Certain Aspects Concerning Contracts for the Supply of Digital Content (2015/0287, COD, 9.12.2015), Art. 3(1).

[124] Efroni (n 23) 805.

[125] Midorović and Sekulić (n 12) 1154; Bedir (n 69) 31. *Narciso* emphasises that contracts where supplying digital content or digital service in exchange for providing personal data, is very similar to monetarily paid digital content contracts. This interpretation should be an argument for synallagmatic feature of digital content contracts. Narciso (n 9) 202.

[126] Staudenmayer (n 79) 229. See also the Rec. 10 of the DCD: "Both the scope of this Directive and its substantive rules should be technologically neutral and future-proof."

DCD.[127] Apart from these examples, any electronic file that is produced and supplied by digital means should be considered as digital content "independently of the medium used for the transmission or for giving access to them" (Rec. 19). In case of 3D printing of goods, electronic files of them should be covered by the DCD to the extent that such files fall under the definition of digital content. However, goods manufactured with the use of such electronic files are not covered by the DCD (Rec. 26).

Similar to the definition of digital content, digital service is defined in a broad manner through dividing into two sub-categories. Accordingly, digital service is "(a) a service that allows the consumer to create, process, store or access data in digital form; *or* (b) a service that allows the sharing of or any other interaction with data in digital form uploaded or created by the consumer or other users of that service" according to the Art. 2(2) DCD. For instance, video sharing platforms, file hosting services, word processing applications or games offered in the cloud and social media are covered by this definition. Determination of whether particular cases fall into the scope of the definition is not made by access methods of digital services. All access methods are covered by the DCD in accordance with the aims of creating technologically neutral and future-proof rules (Rec. 10).

3.2.2.2. Providing personal data

As a result of contractual relationship, consumers have to perform their obligations in return for digital content or digital service. The DCD applies in cases where consumers are obligated with paying a price or providing personal data according to the Art. 3(1). In view of the legislator, there is no difference between the options of paying a price or providing personal data.[128] Consumers will have the same rights and obligations for both those options within the scope of the DCD.[129] Hence, traders cannot escape from the liability stipulated under the DCD by incentivising consumers to select the option of providing personal data.

Since the consumer has alternative payment methods like paying a price or providing personal data, the question should be whether and to what extent the consumer can combine the payment methods. For instance, can parties come to an agreement on combining the options as follows: 'the consumer will pay the discounted price of digital content and provide personal data'? It

[127] Rec. 19: "… this Directive should cover, inter alia, computer programmes, applications, video files, audio files, music files, digital games, e-books or other e-publications …"

[128] However, there is a differentiation between the possibilities of paying with price and providing personal data in terms of scope of the DCD. In cases where provision of personal data has two exclusions in the Art. 3(2) of the DCD. Accordingly, the scope of the former broader than the latter. Narciso (n 9) 205.

[129] Midorović and Sekulić (n 12) 1155; Metzger (n 117) 45.

can be inferred from the Rec. 67 of the DCD that it is possible to mix the payment methods of counter-performance.[130]

The consumer can provide his personal data in exchange for the supply of digital content and digital service as the DCD recognises the value of personal data with the Art. 3(1).[131] However, it is not stipulated any limitations regarding the categories of personal data to be provided and methods of providing personal data. Accordingly, all types of personal data might be considered as counter-performance in a contractual relationship. This might create a vague and difficult challenge regarding the protection of personal data, which is elaborated in the fourth chapter.

On the one hand, the DCD recognises the value of personal data with the Art. 3(1) as enabling consumers to trade their data in commercial transactions. [132] On the other hand, Rec. 24 states that personal data cannot be considered as a commodity. It might be argued that this conundrum stems from critiques by the EDPS. These critiques have steered the EU legislator to stipulate references to "the data protection as a fundamental right and legal instruments like the GDPR and the e-Privacy Directive" in recitals of the DCD. However, there is no consensus whether these references resolve the controversies in the interplay between the GDPR and the DCD. It is also uncertain whether and to what extend the trader can claim for the promised counter-performance against strict limitations of data protection law.[133]

As a result of the synallagmatic contractual relationship, the question should be how the trader can request the consumer's obligation regarding providing personal data. Since the DCD does not regulate the details of the consumer's obligation, the answer should be sought in the national laws. Correspondingly, the Art. 3(10) leaves the discretion to member states on issues related to contract law. Accordingly, the nature of the consumer's obligations and the non-performance should be reviewed under national contract rules. In this section, related provisions of the German Civil Code (*Bundesgesetzbuch*) and the Dutch Civil Code (*Burgerlijk Wetboek*) are reviewed in terms of these issues. Then, turning to the Directive, restrictions regarding the provision of personal data and debates over the two predecessor concepts are analysed.

---

[130] Rec. 67 of the DCD: "Where the digital content or digital service is supplied *in exchange for a price*, the consumer should be able to terminate the contract only if the lack of conformity is not minor. However, where the digital content or digital service is not supplied in exchange for a price but *personal data are provided by the consumer*, the consumer should be entitled to terminate the contract also in cases where the lack of conformity is minor, since the remedy of price reduction is not available to the consumer. In cases where the consumer *pays a price and provides personal data*, the consumer should be entitled to all available remedies in the event of a lack of conformity." (emphasize added)

[131] Jozefien Vanherpe, 'White Smoke, but Smoke Nonetheless: Some (Burning) Questions Regarding the Directives on Sale of Goods and Supply of Digital Content' [2020] European Review of Private Law 251, 256.

[132] Staudenmayer explains this situation as follows: "the DCD thereby recognizes that data is, if not already a form of 'currency' today, probably a de facto 'currency' of tomorrow." Staudenmayer (n 79) 226. For another explanation of value of data, see also Narciso (n 9) 200.

[133] Metzger (n 117) 45.

3.2.2.2.1. The nature of the consumer's obligation

According to the principle 'freedom of contract', parties can determine rights and obligations of them provided that complying compulsory legal rules of the national law. Moreover, parties have to comply contractual provisions when they are obligated themselves based upon the contractual freedom principle. So, in cases where they agreed on provision of personal data in return for supplying digital content and service, the consumer is bound by this obligation under the contract. If the consumer in default, consequences will be applied which are stipulated under the national law.

According to the German Civil Code (BGB) §241/I, the trader can claim enforced performance regarding the consumer's obligation of providing personal data in cases where the consumer is obligated with a contractual clause.[134] This is the primary right of the promisee in the contractual relationship.[135] Similarly, Dutch Civil Code acknowledges to claiming specific performance for the debtor's performance (BW Art. 3:296). The remedy of specific performance is granted primary position within the system of remedies.[136]

If the consumer does not provide his personal data although the request of specific performance through courts, the trader can claim for a compensation (BGB § 281 IV; BW Art. 6:74 and 75) or he may terminate the contract (BGB § 346; BW Art. 6:265) instead of the specific performance. The primary obligation of the consumer, which is provision of personal data, only moved away once the promisee appeals a claim for damages or terminates the contract.[137] It can be argued that German Law and Dutch Law do not push the consumer to the provision of personal data. Because though the court decision regarding specific enforcement, he may not provide personal data, therefore he can be convicted to indemnify, or the contract might be terminated.

3.2.2.2.2. Non-conforming performance of the consumer's obligation

The consumer may not perform his obligation to providing personal data or he can withdraw his data during the term of the contractual relationship. For those cases, German Contract Law and Dutch Contract Law establishes the breach of contract mechanism that includes various

[134] "It is referred to as the Primäranspruch (primary right) as opposed to Sekundäranspruch (secondary right) concerning substitutes for performance (eg, damages)." BS Markesinis, Hannes Unberath and Angus Charles Johnston, *The German Law of Contract: A Comparative Treatise* (2nd ed, Hart Publishing 2006) 398.

[135] The idea of enforced performance is derived from the idea of '*pacta sunt servanda*'. ibid 399.

[136] It could be ascribed to the maxim of pacta sunt servanda, one of the essential principles of Dutch contract law. Daniel Haas and Chris Jansen, 'Specific Performance in Dutch Law' in Jan Smits, Daniel Haas and Geerte Hesen (eds), *Specific Performance in Contract Law: National and Other Perspectives* (Intersentia 2008) 11.

[137] Markesinis, Unberath and Johnston (n 134) 400.

types of breach such as late performance, non-conforming performance, and performance being impossible.[138]

In cases of the non-conforming performance or the withdrawal of data by the consumer, the provisions related to non-conforming performance might be applicable. According to the German Civil Code (BG) §323, if the obligor does not render act of performance in conformity with the reciprocal contract, the obligee may revoke the contract.[139] Similar with the German Law, the remedy to revocation of contract is provided under Dutch Civil Code (BW Art. 6:265). Accordingly, every failure of a party in the performance of one of its obligations grants the other party the right to revocation of contract in whole or in part. Execution of this right is not possible under the conditions that the failure does not justify this remedy and the consequences, given its special nature or minor importance.

In terms of data as counter-performance contract, if the consumer does not perform his obligation or withdraw his consent in the period of contractual relationship, the trader may revoke the contract. In this case, the consumer will be in a harmful situation that contradicts to the GDPR Art. 7(4). Given provisions of the DCD regarding "no prejudice to the GDPR provisions" this situation led to create a sophisticated conflicting point.

3.2.2.2.3. Restrictions regarding the provision of personal data

The DCD is not applicable for the two situations in relation to data as counter-performance contracts to protect traders from unjustified liability regime "in cases where the trader does not get any commercial gain from the data processing".[140] It seems that these restrictions also prevent the amorphous application of the DCD.[141] Furthermore, in cases which fall into the restrictions, the DCD's protection mechanism cannot be applied, thus, it constitutes a difference in the level of consumer protection in terms of application's scope.[142]

Firstly, it excludes a case "where the personal data provided by the consumer are exclusively processed by the trader for the purpose of supplying the digital content or digital service" (Art. 3(1) Par. 2 DCD) For instance, location data is exclusively processed by the trader in navigation apps, and therefore, is not covered. Contrarily, the DCD will be applicable if the consumer "opens a social media account and provides her name and email address that are used for purposes other than solely supplying digital content or digital service" (Rec. 24). However, it

[138] ibid 421 ff; Haas and Jansen (n 136) 11.

[139] Markesinis, Unberath and Johnston (n 134) 427.

[140] Sein and Spindler (n 19) 264.

[141] Narciso (n 9) 204.

[142] ibid 205.

is still unclear when personal data will be classified as necessary for the contract's performance.[143]

Secondly, the situation where the trader processes the consumer's data to comply with his legal requirements and does not process this data for any other purpose falls outside of the DCD. In both cases, the trader cannot be burdened with the liability arising from the DCD.[144] Considering a hypothetical example, one Member State's national law may require registration of consumers for specific digital services.[145] In case of this requirement, processing for the registration purpose is not covered by the DCD since it is a part of the trader's legal obligations.

These exclusions are not identified as acting upon the categories of personal data but on purposes of processing. Therefore, concrete cases should be interpreted with the purposes of processing by the trader. On the other side of the coin, it is not clear whether the GDPR is still applicable to the cases in which covered by the exceptions of the DCD. Because, it seems that there is a conflicting point between the wording of the exceptions and two legal grounds (the contract and the legal obligation) in the GDPR which is elaborated under the fourth chapter.

3.2.2.2.4. Debates over the two predecessor concepts

Notwithstanding it is expressly stated that the GDPR prevails in cases of conflict with the Directive, controversies have emerged regarding the relationship between the DCD and the GDPR. The EU attempted to reconcile two approaches, which are the human rights foundations of data protection and personal data as object of contracts, in preparatory phases of the Directive. In this regard, two phrases were removed from the proposal of the DCD.

Firstly, there was an indicator phrase which was 'actively provided' personal data to determine the scope of the DCD. In response to critiques from academics and the EDPB, this phrase was removed for the reasons that can be summarised as follows: (i) the distinction between actively and passively provided personal data was not grounded in any applicable legal instruments within the EU, (ii) there was no justification for excluding 'passively' provided personal data from the protection of the DCD mechanism. Accordingly, both passively and actively provided personal data are attempted to embracing by the official text of the DCD.

Seemingly, the problem related to the distinction between actively and passively provided personal data was not resolved. Many claim that the term 'provide' in the Art. 3(1) of the DCD

[143] ibid 204.

[144] Staudenmayer (n 79) 227.

[145] The aim of entailing the registration might be comply rules against money-laundering. Sein and Spindler (n 19) 264.

still implies the requirement of active provision by the consumer.[146] Since the information relating to the consumer's device or browsing history is considered as metadata which is passively collected, and this is excluded from the DCD in the Rec. 25, the idea of the distinction, indeed, is still reflected.[147] Another clue might be found in the Rec. 24 as implying the active manner of the consumer by "uploading or creating with the use of the digital content or digital service". Hence, it can be noted that the uncertainty related to the term 'provided actively' remains in the final text of the DCD.[148]

Secondly, the wording 'counter-performance' in exchange for receiving digital content and digital service was removed from the final text of the DCD after the notice from the EDPB. The aim of this alteration with more neutral wording was to prevent putting price tags on personal data and to "not encourage a further commercialisation of personal data" by traders in the market.[149] However, this did not affect the scope of the DCD, as many argue, since it was not affected to substance matter of the article, but rather form of statement.[150] Furthermore, the contractual relationship the consumer undertakes to provide personal data can still be considered as synallagmatic, which means that the consumer's obligation is the counter-performance for the trader's obligation.

Similarly, the EDPS shared its concerns regarding the introduction of the concept of 'pay with personal data' after the phrase of 'counter-performance' was removed. It emphasised that putting this phrase instead of "counter performance or making an analogy between the provision of personal data and the payment of a price would not solve problems regarding the commercialisation of personal data".[151] Accordingly, it recommended using the phrase "irrespective of whether a payment of the consumer is required" instead of provision of personal data by the consumer[152], which was not accepted in the legislation process. Overall, these

[146] Reiner Schulze and Dirk Staudenmayer (eds), *EU Digital Law* (Nomos 2020) Art. 3 para 57; Zohar Efroni, 'Gaps and Opportunities: The Rudimentary Protection for "Data-Paying Consumers" Under New EU Consumer Protection Law' [2020] Common Market Law Review 799, 813.

[147] Sein and Spindler (n 19) 263. If collecting metadata is leaded a formation of contract under national law, it will be covered by the DCD (Rec. 25, third sentence). But it is still uncertain to what extent usage metadata should be included. Anne Riechert, 'Data as a Counter-Performance' in Reiner Schulze and Dirk Staudenmayer (eds), *Data as Counter-Performance - Contract Law 2.0?: Münster Colloquia on EU Law and the Digital Economy V* (Nomos 2020) 274.

[148] In the case of C-49/11 Content Services ECLI:EU:C:2012:419, the CJEU dealt with the concept of consumers' 'active action', which is indirectly related to our case: 'actively provided'. See for details: Narciso (n 9) 204.

[149] Axel Metzger, 'A Market Model for Personal Data: State of Play under the New Directive on Digital Content and Digital Services' in Sebastian Lohsse, Reiner Schulze and Dirk Staudenmayer (eds), *Data as Counter-Performance - Contract Law 2.0?: Münster Colloquia on EU Law and the Digital Economy V* (Nomos 2020) 28; Reiner Schulze and Dirk Staudenmayer (eds), *EU Digital Law: Article-by-article commentary* (Nomos 2020) Art. 3, Par. 54.

[150] Efroni (n 23) 805.

[151] EDPS (n 115) 13.

[152] ibid 14.

debates to reconcile the DCD with the GDPR and its philosophy has shown that the EU attempted an appropriate way to acknowledge the value of personal data while simultaneously protecting its human right feature. Seemingly problems regarding the interplay have still ambiguities.

3.3. CONCLUDING REMARKS

This chapter is elaborated on the conditions of the data as counter-performance contracts according to the DCD, which is based on the freedom of contract principle. Since the requirement of a contractual relationship between the trader and the consumer, the DCD's scope is, inherently, restricted with the term 'contract'. On the contrary, the GDPR is applicable independently of the contractual relationship and other requirements provided in the DCD.

The removal of wordings 'personal data was provided actively' and 'counter-performance' from the DCD has not put an end to debates over the substantive meaning of those. Firstly, two recitals of the DCD (Recs. 24 and 25) which are regulating exclusion of metadata considering passively collected and the phrase 'uploading or creating' implying active provision, illustrated that final text of the DCD is still reflected with the idea of precedent wording 'provided actively'. Secondly, since changing the phrase from 'counter-performance' to 'providing personal data' did not change the possibility of providing personal data in return for supplying digital content or service, the contractual relationship might still be considered synallagmatic. As a result of that, contracting parties can request each other's performance of obligations.

Though it is possible to requesting performance of obligations related to the provision of personal data, the method of claiming does not expressly state in the DCD. The Directive leaves those methods to member states' discretion through the Art. 3(10). For instance, The German Civil Code and Dutch Civil Code does not push the consumer to the provision of personal data. If the consumer does not provide personal data, he can be convicted to indemnifying damages of the trader. Furthermore, in cases where the consumer does not render act of performance in conformity with the contract in a reciprocal contract, the trader may revoke the contract. Since the possibility of revoking contract is also applicable to the data as counter-performance contracts, the consumer as a data subject might be in a harmful situation, that contradicts to the Art. 7(4) GDPR.

§ 4. RECONCILIATION OF THE GDPR'S AND THE DCD'S APPROACHES

The EU has a desire to unleash the value of personal data in the data-driven economy while it simultaneously seeks to protect personal data by strict rules. This is one of the major takeaways which can be inferred from the legislative process of the DCD (*Table 1*).[153] First of all, European Commission's proposal of the DCD has created a balance between the unleashing the value of personal data and protection of personal data in favour of the former. However, the EDPS and academics criticized that proposal with the argument that the possibility of using personal data as counter-performance should be expressed in an implicit and abstract way rather than explicit and concrete one.[154] The aim of those critiques was to re-establish the balance, which was not stable at that moment. Despite the critiques, the EU legislator persisted on recognising the value of personal data by an explicit wording,[155] and, this usage complicates to reconcile with data protection law.[156]

[153] Another sign which reflects the EU's purpose on utilising the value of personal data can be seen in the proposal of Proposal (EU) for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act), COM(2020) 767 final, 25.11.2020 ("DGA Proposal"). As it occurred in the legislative process of the DCD, the EDPB and the EDPS raised their concerns regarding the significant inconsistencies between the DGA Proposal and the GDPR, qq.v., 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)' (2021) para 25; EDPB, 'Statement 05/2021 on the Data Governance Act in Light of the Legislative Developments' (2021) 2. In addition, CITIP researchers have agreed that this approach might be clashed with the GDPR's approach: "Such an approach endorses the *commodification of data*, namely the process by which data is increasingly viewed as a tradeable commodity. (…) Such a new approach in EU legislation is worth observing, as it departs quite significantly from previous regulation of 'data'." (emphasize added) Julie Baloup and others, 'White Paper on the Data Governance Act (CiTiP Working Paper Series)' [2021] SSRN Electronic Journal 54 <https://www.ssrn.com/abstract=3872703> accessed 16 July 2021.

[154] EDPS (n 16); EDPS (n 115); Giliker (n 16); Midorović and Sekulić (n 12); Versaci (n 14); Efroni (n 23).

[155] Lewinski explains the situation that "market privacy is the deliberate blind spot of the European Data Protection Law". Von Kai v. Lewinski, 'Wert von Personenbezogenen Daten', *DatenDebatten: Band 3* (Erich Schmidt 2019) 211. The European Parliament Research Service warned the co-legislators that they were encountered a challenging task "to reconcile the fundamental rights approach with the requirements of economic reality, including the need to grant legal protection for consumers who provide their personal data in order to access digital content or services". Mańko and Monteleone (n 54) 11.

[156] Vanherpe (n 131) 257.

Table 1: Legislation process of the data as counter-performance contracts in the DCD.

European Commission Proposal 09.12.2015	EESC* Opinion 20.07.2016	EDPS* Opinion 4/2017 14.03.2017
Art. 3(1) of the Proposal: "This Directive shall apply to any contract where the supplier supplies digital content to the consumer or undertakes to do so and, in exchange, a price is to be paid or the consumer **actively provides counter-performance** other than money in the form of personal data or any other data."	The EESC can accept that payments be made in kind (against 'counter-performance other than money') as long as this is defined in a precise manner in terms of content; where personal or other data is provided it will be **necessary to specify which data and under what conditions and in what circumstances.** *European Economic and Social Committee	The EDPS recommends avoiding referring to **data (actively) provided** by the consumer since it contradicts the (existing and future) rules on data protection. The EDPS considers that the term **"data as a counter-performance"** should be avoided. *European Data Protection Supervisor

Official Text 22.05.2019	European Parliament's Position 26.03.2019	EDPS Opinion 5/2018 05.10.2018	European Parliament's Joint Committee Report 27.11.2017
Art. 3(1)2 of the DCD: "This Directive 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, except where the personal data provided by the consumer are exclusively processed by the trader for the purpose of supplying the digital content or digital service in accordance with this Directive or for allowing the trader to comply with legal requirements to which the trader is subject, and the trader does not process those data for any other purpose."	The wording of "consumer provides or undertakes to provide personal data to the trader" is retained. Two exceptions for the scope regarding the contracts are added which can also be seen in the official text.	The EDPS welcomes to refraining from certain terms in the article. However, the EDPS retains his concerns regarding the new approach which contains that consumer can **"pay" with their personal data.** The EDPS therefore recommends refraining from any reference to personal data and suggests to using the phrase **"irrespective of whether a payment of the consumer is required"** to addressing personal data.	The report includes an amendment regarding the Art. 3(1) of the Proposal. Accordingly, instead of the wording "actively provided", "is provided by the consumer" is used. In addition to that the term "counter-performance" is removed.

Considering the matters addressed by data protection authorities and academics, a fair balance should be struck between the approaches of the GDPR and of the DCD. This leads us to the question of how we can reconcile these approaches. In order to provide rational resolutions, this chapter is divided into four sections. To begin with, it is provided a brief overview of connecting points between the legal instruments and the philosophy behind them. The second section presents the conflicting points amongst them (*the third sub-question*). In the third section, ways to reconcile the conflicting points are analysed (*the fourth sub-question*). Finally, the question of how these ways can be integrated into the current EU legal landscape is answered.

4.1. OVERVIEW OF THE APPROACHES

The GDPR and the DCD evaluates the status of the personal data with different mindsets as elaborated in the second and third chapter of this thesis. The GDPR, mainly, approaches personal data from the human rights perspective by advocating inalienable and non-waivable features of personal data. By doing so, it also aims to ensure the free movement of personal data (e.g., with several provisions like Art. 18 – right to data portability) and does not prohibit contractual practices on exchanging them as consideration. Hence, it can be concluded that personal data can be transferred to the controller in return for digital content and digital service

by complying with the requirements of the GDPR. On the other side of the coin, the DCD is established on the contractual freedom principle. Accordingly, the DCD identifies the possibility of providing personal data in return for receiving digital content or digital service. Prior to the enactment of the DCD, consumers could also be the party of the contract which contained the provision of consumer's personal data by fulfilling the GDPR's conditions. The DCD, solely, regulated the de facto reality of the value of personal data in contractual relations and envisaged the legal protection mechanism for consumers via its provisions.

As mentioned by many, the GDPR and the DCD are parallel legal regimes, which means that they can be simultaneously applied to a specific case, rather than in a way that they are applied as *lex specialis* and *lex generalis*.[157] Although the same points are touched to some extent by both of them, aims and subject matters of those legal instruments are completely different. References regarding the implementation of the Directive without prejudice to the GDPR and e-Privacy Directive also prove that the two legal instruments can be applied in parallel.[158]

As regards the essential features of these legal instruments, while the GDPR is a public law instrument which primarily comprises mandatory rules about data protection, the DCD is a private law instrument which aims at harmonisation of rights and obligations arising from private law relations. As another connection point, the terms data subject and controller in the GDPR might be equivalent, respectively, to the terms consumer and trader in the DCD.[159] Last but not the least, the GDPR does not require a pre-condition for the applicability, unlike the DCD. The GDPR is applied to all kinds of cases regardless of causality of action such as tort, contract, and unjust enrichment. However, an existing contractual relationship between the trader and the consumer is a pre-condition for the applicability of the DCD, which is stipulated under the Art. 3(1).

4.2. CONFLICTING POINTS

4.2.1. The Tension between the Contractual Freedom Principle in the DCD and Human Rights Foundations of the GDPR

All types of personal data can be regarded as consideration in a contractual relationship according to the wording of the DCD and its main principle which is freedom of contract. I.e.,

[157] Mańko and Monteleone (n 54) 5; Cemre Bedir, 'Data as Counter-Performance: Yet Another Point Where Digital Content Contracts and the GDPR Conflict' (Leiden University 2018) 10 <https://www.ssrn.com/abstract=3648092> accessed 8 November 2020.

[158] Art. 3(8) of the DCD: "(…) In particular, this Directive shall be without prejudice to Regulation (EU) 2016/679 and Directive 2002/58/EC. In the event of conflict between the provisions of this Directive and Union law on the protection of personal data, the latter prevails."

[159] Reiner Schulze and Dirk Staudenmayer (eds), *EU Digital Law: Article-by-article commentary* (Nomos 2020) Art. 3 Para 139; Zohar Efroni, 'Gaps and Opportunities: The Rudimentary Protection for "Data-Paying Consumers" Under New EU Consumer Protection Law' [2020] Common Market Law Review 799, 805.

the consumer and trader can reach an agreement on the exchange of personal data without any limitations except for the conditions stipulated in the GDPR. This is the basic result of the pure application of the freedom of contract principle. The European Parliament's Economic and Social Committee has criticized it, arguing that it is necessary to specify which data are provided and under what conditions data are processed.[160] Accordingly, as long as categories of personal data and specific conditions for monetisation of personal data are defined in a precise manner, personal data, thus, might be considered as consideration in contracts. Otherwise, the freedom of contract principle might compromise the GDPR's human rights approach by creating contradictions. Since the EU legislator did not consider this concern in the final text of the Directive, a tension between the DCD and the GDPR, inevitably, emerged. Put differently, monetisation of personal data without specifying any further conditions creates a conflicting point with the GDPR's human rights approach.

Indeed, many pointed out that there is a conflicting point between the freedom of contract principle and the right to data protection. *Hacker* argues that "tying the quality of data as counter-performance to its status under data protection law would inject an unwelcome dose of legal uncertainty into general contract law."[161] A similar argumentation can be seen in *Sattler*'s and *Versaci*'s papers respectively as follows: "there is an obvious tension stemming from the freedom of contract and the approach taken by the GDPR."[162] and "privacy law has an unclear relationship with contract".[163] However, this so-called uncertainty, tension or unclear situation has not still been elaborated. Arguably, the GDPR's human rights foundations might be challenged by monetisation of personal data, as human rights foundations of the GDPR include "minimum and non-negotiable level of privacy and data protection", which is elaborated under the second chapter. Monetisation of personal data through contracts might lead to losing that level of privacy and data protection.

As a matter of fact, personal data in any category (sensitive or not) may be sold and bought within the European Union by respecting the legislative sources. Theoretically, it is possible under the GDPR, and that is increasingly being common practice all around the world as well

[160] Opinion of the European Economic and Social Committee on the "Proposal for a directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content" and the "Proposal for a directive of the European Parliament and of the Council on certain aspects concerning contracts for the online and other distance sales of goods", Rapporteur: Mr Jorge Pegado Liz, OJ 20.07.2016, 4.3.2.3 Article 3 – Scope: "The EESC can accept that payments be made in kind (against 'counter-performance other than money') as long as this is defined in a precise manner in terms of content; where personal or other data is provided it will be necessary to specify which data and under what conditions and in what circumstances." Riechert has also stated that "we have an unclear legal situation concerning the exploitation of data." Riechert (n 147) 268.

[161] Hacker (n 36) 60.

[162] Andreas Sattler, 'Autonomy or Heteronomy – Proposal for a Two-Tier Interpretation of Art 6 GDPR' in Reiner Schulze and Dirk Staudenmayer (eds), *Data as Counter-Performance - Contract Law 2.0?: Münster Colloquia on EU Law and the Digital Economy V* (Nomos 2020) 234.

[163] Versaci (n 14) 385.

as in the EU. Although data subjects have rights and remedies in theory against the abusement of their personal data after the monetisation, it should be considered that we live in an age of massive data breaches that occur at every single day, and that millions of personal data has stolen from the most protective databases thus far. Following a data breach, data subjects inherently lose their control over their personal data as opposed to their theoretical rights and remedies. At that point, limits of freedom of contract might be considered again. Though data subjects have freedom of contract that enables them to contract over privacy within the certain limits,[164] these existing limits (*status quo*) might not be sufficient in terms of data as counter-performance contracts. Therefore, it can be argued that freedom of contract should be limited with some additional measures to ensure minimum level of protection. Otherwise, this principle might lead undesired results, such as exploitation of consumers in contractual relations, rather than be a tool that serves the will of parties. This thesis argues that limitation of the freedom of contract principle should be based on the risk in which consumers may lose their control over their personal data.

4.2.2. Validity of Consent according to the Art. 7(4) GDPR in Data as Counter-Performance Contracts

This thesis focuses on three possible legal grounds for processing consumers personal data in DACP contracts. The contract in Art. 6(1)(b) and the legitimate interest Art. in 6(1)(f) have controversial issues and practical challenges which are elaborated under the second chapter. Seemingly, consent is one of the most appropriate valid legal ground for processing data in DACP contracts, which also has certain requirements. Apart from the discussions related to the Art. 7 GDPR, elucidated in the second chapter, the Art. 7(4) GDPR prohibits the conditionality on consent to the processing of personal data that is not necessary for the performance of that contract. [165] If the Art. 7(4) GDPR is interpreted strictly, consent will be invalidated in many cases. [166] Invalidation of consent renders the processing of personal data illegal in certain cases, and this constitutes a conflicting point between the Art. 7(4) GDPR and the DCD.[167]

4.2.3. The Interplay between Exceptions in the DCD and Legal Grounds for Processing of Personal Data in the GDPR

The DCD envisages two exceptions regarding the scope of the DCD's legal protection mechanism on DACP contracts. The Art. 3(1) mandates that the following cases shall not be

[164] "… the analysis of the relevant CJEU case law has been useful insofar as it showed that the data protection right can impose limits on economic rights, but it usually does not exclude them altogether." ibid.

[165] "If a controller seeks to process personal data that are in fact necessary for the performance of a contract, then consent is not the appropriate lawful basis." See, EDPB, 'Guidelines 05/2020 on Consent under Regulation 2016/679 (v1.1)' (n 64) para 31. "Article 7(4) is only relevant where the requested data are not necessary for the performance of the contract" ibid 32.

[166] Efroni (n 23) 806.

[167] ibid.

within the scope of the Directive where (i) "the consumer's personal data are exclusively processed by the trader for the purpose of supplying the digital content or digital service in accordance with this Directive" or (ii) "the consumer's personal data is processed for the compliance of the legal requirements of the trader, and the trader does not process those data for any other purpose". Choice of wording in the Directive might lead to a confusion in relation to legal grounds of processing of personal data since it connotates the contract in Art. 6(1)(b) and legal obligation in Art. 6(1)(c) within the GDPR respectively. This confusion will highly likely cause a conflict between the GDPR and the DCD since it includes a possibility of an exact overlap between the exceptions and the legal grounds. Put differently, if the exceptions of the DCD are interpreted in the exactly same way as the legal grounds, consumers' rights and remedies envisaged by the DCD will be under risk. Because, the safeguards of the Directive cannot be applicable in cases where Art. 6(1)(b) or Art. 6(1)(c) are legal grounds of the processing of personal data. Therefore, traders may be able to avoid the scope and consumer-friendly provisions of the DCD by relying on the legal grounds in question. As a consequence of this, the conflicting point stems from the question of whether these exceptions exactly overlap with the two specific legal grounds in the GDPR.[168]

4.3. RECONCILIATION OF CONFLICTING POINTS

4.3.1. Limiting Contractual Freedom by Determination of the Risks for Processing Personal Data in Data as Counter Performance Contracts

The best starting point for the reconciliation of two approaches is to acknowledge the current EU's policy regarding utilisation of personal data which can be seen in the DCD.[169] Since the prospect of the revision of the DCD's wording is pretty low for the chosen path by the EU, the existing limits of the freedom of contract principle, which is mentioned in the sub-section 4.3.1, might be adjusted with other appropriate means such as guidelines and court practice. In that way, the reconciliation between the contractual freedom principle and the human rights foundations of the GDPR could be materialised.

Janeček and *Malgieri* developed the *dynamically limited alienability rule* to establish a link between data protection laws and contract law rules and principles.[170] This rule is based on two-step test: (i) Are data personal or non-personal, and, if they are personal data, are they sensitive

[168] A possible overlap might lead an unintended consequence which is the interpretation of the Art. 6(1)(b) will also impact the Art. 3 DCD. Durovic and Montanaro (n 93) 30. Furthermore, *Weiß* highlights that differences between 'necessary for the performance' [GDPR] and 'exclusively processed for supplying content' [DCD] will be discussed by courts and data protection officers. Weiß (n 10) 281.

[169] For the details of the DGA Proposal, see the footnote 153.

[170] Janeček and Malgieri (n 25).

or non-sensitive? (ii) What is the legal basis for trading data?[171] As stated in this approach, if they are non-personal data, they might be traded by contractual transactions without the limitations of the GDPR. If they are personal data, the controller should consider the necessary conditions of the GDPR. Furthermore, if they also have sensitive feature, related provisions of the GDPR should be considered. Indeed, this perspective has not formed a new interpretation for the decent application of the DCD but systematized the conditions regarding processing of personal data in the GDPR. Therefore, the question should be which novel tools or interpretations can be developed to propose a way of reconciliation between the approaches of the GDPR and of the DCD.

Both legal instruments have a spirit being on the data subject or consumer's side and protecting them. Accordingly, the criteria which will be developed should be consumer-sided and create clear distinctions on the risks related to the human rights character of right to data protection. Put simply, high risks regarding right to data protection in data as counter-performance contracts should be determined, and accordingly pertinent measures should be developed.[172]

The risks can be determined based on the quite simple questions like from which sources are the personal data is processed (*source*), whose personal data is processed (*data subject*), and which categories of personal data is processed (*types of personal data*). These questions can create the main structure of the resolution, which will be completed after the identification of risks regarding the loss of right to data protection. Hence, this approach focuses on, at least, three topics, which are external sources of personal data, risky categories of personal data, and vulnerable data subjects. Therefore, it can be determined whether and to which extent the freedom of contract should be further limited within data as counter-performance contracts.

The first distinction can be established by considering the source of personal data. In a hypothetical case, it is assumed that Netflix presents subscription packages including an option of provision of personal data as well as option of paying with a price. Accordingly, Netflix processes its consumers' personal data such as watch history, search queries, time spent watching a show and other several data points. By implementing data analytics models through sophisticated techniques, Netflix should be able to monetise those data through creating a detailed profile of its subscribers and monetising those data instead of receiving a price. In this case, user-generated personal data in the digital service (internal source) are monetised as a matter of course.

[171] They accept here that "trading data means *obtaining personal data in exchange for money or for other valuable assets*" (emphasize added). ibid 933.
[172] *Wendehorst* argues that the notion 'data commerce' should be introduced to determining conditions of onward transfer of personal data to another controller for commercial purposes within the risk-based approach. Wendehorst (n 10) 217.

Contrarily, the source of personal data might also be *external* within the context of DACP contracts. To continue with the example, Netflix might request accessing users' social media accounts to retrieve their data to monetise them in contractual relations. Utilising personal data that are retrieved from external sources have a greater risk since they can be easily utilized unfairly, when compared to internal sources of data. In today's big data environment, data analytics models may be used for correlating the user-generated data (*internal*) with the data from external sources and creating several new data points related to consumer. As stated by the Information Commissioner's Office,[173]

> "if a company is analysing its own customer database, even if that database is particularly large, it may not necessarily raise any novel issues in terms of either analytics or data protection. However, when it combines its own information with data sourced externally (whether that be from a publicly accessible source or not), then it is doing something qualitatively different that can be called big data."

Therefore, Netflix will have personal data records that include user-generated data, external data, and new data points earned from the matching and can easily monetise these records in an unfair way which might be challenged with data protection principles. Contrarily, if only the user-generated data in a certain digital service is processed by the trader, the possibility of unfair utilization is decreased. Therefore, it can be argued that traders should be sceptical about external data sources to ensure their compliance with the data protection rules and principles.

The GDPR creates a clear distinction between sensitive and non-sensitive personal data. Sensitive data categories are determined by the legislator in terms of their risks of processing activity.[174] I.e., risks in processing sensitive data are much higher than those in non-sensitive data. Accordingly, sensitive data are protected by stricter rules than the rules for non-sensitive data. For example, processing of sensitive data is prohibited in principle pursuant to the Art. 9(1) GDPR. Due to having high risks regarding the human rights approach in the contractual relationship that involves trading sensitive data, which might be considered that they are at the closest place to the core of the safeguarded area, such processing should be welcomed with a sceptical manner. Moreover, the Art. 9(4) GDPR lets the member states specify further conditions with regard to the processing of genetic, biometric or health data. As a consequence, the member states should introduce more protective conditions and raise the level of protection for the environment of DACP contracts.

[173] ICO, 'Big Data and Data Protection (v1.0)' (2014) para 88.

[174] Rec. 51 of the GDPR: "Personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms. (…)"

Processing of vulnerable persons' data, in particular children's data, has also a noteworthy risk regardless of whether their data are sensitive or not. Generally, legislators consider this risk and separate the conditions for children's data from the general conditions on processing of personal data. Correspondingly, the GDPR stipulates the conditions of processing personal data of children in the Art. 8 which is as an example of the practice of the aim of protecting vulnerable persons. It can be claimed that the utmost importance regarding vulnerable persons' data should also be given in the context of DACP contracts.

4.3.2. Distinguishing Data as Counter-Performance Contracts from Traditional Ones

The second conflicting point is related to the validity of consent according to the Art. 7(4) GDPR in DACP contracts. Some commentators have proposed to advocate a more permissive interpretation of the Art. 7(4)'s prohibition on coupling pursuant.[175] However, general permissive interpretation might lead to the conclusion that the protection mechanism of the Art. 7(4) GDPR will not be effective anymore for "coupling between consent to data processing and the provision of goods or services where the personal data is not necessary for the performance of the contracts".[176]

Therefore, it can be argued that a certain interpretation might be developed according to the whether the contract is data as counter-performance contract, or not. I.e., contracts that include the main obligation to supplying digital content and digital services might be distinguished from traditional contracts where the supplier provides traditional goods or services. As a basis of that distinction, two significant factors can be put forward. First of all, the subject of a DACP contract is digital content or digital service, and that contract inherently requires processing more data than traditional contracts do. Because these contracts are generally concluded in digital platforms such as Netflix, Google Drive or Steam as opposed to traditional contracts. Furthermore, digital content and digital services have already distinguished from traditional goods and services within the DCD in terms of consumer protection law. This can be seen in Articles 7 and 8 of the DCD, which regulates the conformity requirements that are different from those for traditional goods and services.[177] Accordingly, this distinction should be reflected into data protection rules with an appropriate interpretation.

Considering these factors, contracts containing the obligation of supplying digital content and digital services should be distinguished from traditional contracts by developing a certain interpretation of the Art. 7(4). A key element to assess whether a situation of bundling or tying occurs is the determination of "what the scope of the contract is and which data would be

[175] Efroni (n 23) 806–807.

[176] ibid 806.

[177] Compatibility, interoperability, being updated, accessibility, continuity and security are prominent examples of the requirements. They are novel concepts that were not envisaged for traditional goods and services.

necessary for the performance of that contract."[178] I.e., the boundaries of the phrase "necessary for the performance" determine whether there is a bundling or tying issue. Accordingly, this phrase should not be interpreted in a broad manner in traditional contracts.[179] Otherwise, the controller can easily rely on consent as a legal valid ground for legitimating the processing of irrelevant categories of personal data. For example, processing of personal data basing on marketing purposes should be illegal in a typical sales contract if the processing depends on the consent of the consumer. Contrarily, it can be argued that these and purposes alike might be interpreted broadly in data as counter-performance contracts.[180] Because, without marketing or similar purposes, the supplier no longer achieves its aim, which is monetising the consumer's data instead of receiving a price from the consumer.

4.3.3. Formulating an Interpretation on the Exceptions of the DCD

The relationship between the exceptions regarding the scope of the DCD and two legal grounds for processing of personal data in the GDPR must be explained in a clear way to prevent the confliction. *Schulze* and *Staudenmayer* claims that there is no room to establish a link between the exceptions and the legal grounds.[181] Accordingly, the Directive's application is not determined on whether or which of legal grounds under the GDPR apply for the processing of data since the lawfulness of processing personal data is exclusively dealt with by the GDPR.[182] Contrarily, some advocate that the Directive implicitly refers to the Art. 6(1)(b) concerning the

[178] "To assess whether such a situation of bundling or tying occurs, it is important to determine what the scope of the contract is and what data would be *necessary for the performance* of that contract." (emphasize added) EDPB, 'Guidelines 05/2020 on Consent under Regulation 2016/679 (v1.1)' (n 64) para 29.

[179] The Article 29 Working Party has explained the issue without touching upon the distinction on traditional contracts and data as counter-performance contracts. A29WP, 'Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC' (n 94) 16.

[180] What is my personal data worth? – Commoditised data as "counter performance", <https://www.bristows.com/news/what-is-my-personal-data-worth-commoditised-data-as-counter-performance/> accessed 16 July 2021.

[181] Reiner Schulze and Dirk Staudenmayer (eds), *EU Digital Law* (Nomos 2020) Art. 3 Para. 61: "The similarities of the references to 'exclusively processed by the trader for the purpose of supplying' and 'comply with legal requirements' to Art. 6(1)(b) and (c) GDPR are not to be interpreted as references to the legal grounds for processing personal data under this provision."

[182] "The similarities of the references to 'exclusively processed by the trader for the purpose of supplying' and 'comply with legal requirements' to Art. 6(1)(b) and (c) GDPR are not to be interpreted as references to the legal grounds for processing personal data under this provision." Reiner Schulze and Dirk Staudenmayer (eds), *EU Digital Law: Article-by-article commentary* (Nomos 2020) Art. 3, Par. 61. "(...) the legislator inserted the second subparagraph of Art. 3 and respective explanations in Recitals 24, 37–40. This clarifies that the lawfulness of processing personal data is exclusively dealt with by GDPR. (…) It is also clarified that the list of legal bases in Art. 6(1) GDPR for processing personal data is exhaustive and that the Digital Content Directive does not add to, or interfere with, those legal grounds for lawfully processing data." Reiner Schulze and Dirk Staudenmayer (eds), *EU Digital Law: Article-by-article commentary* (Nomos 2020) Art. 3, Par. 140.

contractual necessity and Art. 6(1)(c) concerning the compliance with legal obligations.[183] However, it is difficult to see how these conclusions could be reached.

Turning back to the former question which is whether these exceptions exactly overlap with the two specific legal grounds in the GDPR, if it is answered positively, the consumer who needs to be protected by law due to her weak position cannot be safeguarded by the DCD in cases where these two legal grounds are applicable. Furthermore, this way of approach also contradicts the first two sentences of Recital 38, which clarifies that the DCD does not in any way tamper with the legal grounds of processing personal data under the GDPR.[184] On the other side of the coin, consumers can still bind themselves to provide personal data in return for digital content or service with contracts even in cases which are not covered by the DCD. In other words, the fact that the DCD does not cover a case will not cause the invalidity of the contract: it only leads to the loss of the consumer's legal remedies stipulated under the DCD.

Considering the necessity of consumer protection in the digital environment, an interpretation should be formulated which aims to maintain the protection of consumers as much as possible within the current legal framework, which embodies the DCD and the GDPR in our case. Put differently, a resolution regarding the issue should be developed in such a way that it will not lead to the loss of the safeguards of the consumer. Therefore, the resolution will serve to secure the consumer. In light of this "safeguarding" factor, the exceptions in the Art. 3(1) DCD should be understood narrowly while two specific legal grounds in the GDPR should be interpreted broadly as stated by *Efroni*.[185] This way of interpretation would also be consistent with the Roman Law principle "*singularia non sunt extendenda*" (exceptions should be construed narrowly), which is also adopted by the CJEU in many of its judgments.[186] By concluding that the exceptions are narrower than the legal grounds, consumer's protection area will be expanded

[183] Juliette Sénéchal, 'Article 16(2) of the "Digital Content and Digital Services" Directive on the Consequences of Termination of Contract, or the Difficult Articulation between Union Law on Consumer Contract and Union Law on the Protection of Personal Data' in Reiner Schulze and Dirk Staudenmayer (eds), *Data as Counter-Performance - Contract Law 2.0?: Münster Colloquia on EU Law and the Digital Economy V* (Nomos 2020) 155–156; Sattler (n 162) 242.

[184] Reiner Schulze and Dirk Staudenmayer (eds), *EU Digital Law: Article-by-article commentary* (Nomos 2020), Art. 3, Par. 61.

[185] In his conference talk, Zohar Efroni, who has, explained his opinions regarding the interplay between the legal grounds of the GDPR and exceptions of the DCD as follows: *"… I think that the language is not exactly identical. I think there are different ways to interpret it. In my reading, the GDPR grounds are broader than the exceptions of the DCD. Therefore, we might have situations in which the processing is legitimate either under 6(1)b or 6(1)c and the DCD applies, because exceptions are narrower than the legal grounds.*" Efroni Z, 'Data Protection Aspects of the Digital Content Directive' (Conference on Data Protection in Digital Era, Istanbul (Zoom), 16 April 2021) <https://youtu.be/YvRipkWV8uA?t=4280> accessed 10 June 2021

[186] Nial Fennelly, 'Legal Interpretation at the European Court of Justice' (1996) 20 Fordham International Law Journal 26, 674.

in line with the aim of the DCD. Therefore, the provisions of the DCD will be simultaneously applicable with the legal grounds under the Art. 6(1)(b) and Art. 6(1)(c) of the GDPR.

4.4. ADOPTING RECONCILIATIONS TO THE LEGAL FRAMEWORK

The EDPS issued two different opinions regarding the notion of data as counter performance contracts during the legislation process of the DCD. These opinions criticized by many in relation to the wording of the DACPC-related provisions in the DCD. Although some of those were taken into account in the legislation process, there are still hidden gaps in the interplay between the GDPR and the DCD, which might arise when the DCD begins to be applied in the member states (July 2022). At the time of legislation process, one argued that the determination whether the contractualisation of personal data should be prohibited is a policy issue which must be decided by the European legislator.[187] Since the EU did not prefer the prohibition of commercialisation, it could be argued that the European Data Protection Board can lead the way for controllers to provide them for awareness of the human rights foundations of the GDPR. This would be *ex-ante* and non-binding way of reconciliation of the approaches. In addition to that, the frontiers of the contractualisation might be determined by the CJEU by its binding decisions (*ex-post*). [188]

In order to fill hidden gaps, the EDPB as a competent authority which is established by the GDPR, should issue guidelines regarding the notion of data as counter-performance contracts. The aim of these guidelines should be to reconcile two different approaches. This thesis argues that these guidelines, at least, should touch upon the foregoing conflicting points. Beside the EDPB, controversies arising in the interplay between two approaches are portent of the prospective judgments that will be made by the CJEU as the highest judicial authority of the EU.

Indeed, the CJEU will shed light on the interaction between the legal grounds of consent (Art. 6-1-a) and performance of contract (Art. 6-1-b) with the pending Schrems-Facebook case before the court. [189] Facebook is a prominent example of gratuitous digital service provider whereby users' personal data are processed. Due to having a contractual duty to provide personalized advertisement to users, Facebook believes that they do not need to obtain consent of users. Accordingly, they rely on the Art. 6(1)(b) for the processing of personal data. Following earlier judgments in Vienna, the Austrian Supreme Court has referred the case to the CJEU with four questions. The core question is related to the legal basis of Facebook uses for

[187] Versaci (n 14) 392. Furthermore, Wendehorst argues that the prospect of the revision of the GDPR's wording is pretty low for political reasons. Wendehorst (n 10) 218.

[188] Sattler (n 162) 250.

[189] Facebook's GDPR bypass reaches Austrian Supreme Court <https://noyb.eu/en/facebooks-gdpr-bypass-reaches-austrian-supreme-court> accessed 9 April 2021.

processing of user data. Accordingly, it is asked whether Facebook can avoid strict requirements of consent that provides significant protection for consumers, by relying on the contract within the context of personalized advertisements.[190]

As elaborated under the second chapter, the controller cannot rely on the Art. 6(1)(b) GDPR for every type of processing activity that occurs in the contractual relationship. Relying on the contract requires more than just adding a clause to the contract.[191] Therefore, Facebook's contractual duty - argument regarding the personalised advertisement might not be sufficient, as the EDPB adopts the idea that "as a general rule, processing of personal data for behavioural advertising is not necessary for the performance of a contract for online services".[192] Furthermore, Facebook unilaterally drafts the terms and conditions, and its users do not have a chance to have a say in the contractual provisions. That take-it or leave-it approach might also affect the decision to be provided by the CJEU. Last but not least, Facebook's duty of providing personalised advertisement to data subjects is a revenue-generating activity purely in favour of Facebook rather than its users. Ironically, Facebook, in this case, advocates an argument that serves to avoid the requirements of the consent, with another argument that involves the aim of increasing its revenue.

Building on these reflections, the CJEU will make a binding interpretation regarding the interplay between the consent and the contract. Although this case is not directly related to DACP contracts, it is highly likely that the Court's interpretation will have certain implications for these contracts, especially for gratuitous ones. Accordingly, the CJEU will have identified the criteria for the term "necessity" in data as counter-performance contracts. Furthermore, the prospective judgment will also affect the interpretation of consent in terms of the Art. 7(4) GDPR, since the term "necessity" in this provision is closely connected to the term "necessity" in the Art. 6(1)(b).[193]

4.5. CONCLUDING REMARKS

This chapter is elaborated on the ways of reconciliation between the GDPR's and the DCD's approaches. Conflicting points are, generally, stemmed from chosen path by the EU which is unleashing the value of personal data in data-driven economy. Since this chapter is an analytical

[190] Austrian OGH asks CJEU if Facebook "undermines" GDPR since 2018 <https://noyb.eu/en/breaking-austrian-ogh-asks-cjeu-if-facebook-undermines-gdpr-2018> accessed 23 July 2021.

[191] 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 (v 2.0)' (n 61) para 27. According to EDPB, mentioning to profiling in contracts alone does not make it 'necessary' for the performance of the contract (ibid 35.).

[192]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 (v 2.0)' (n 61) para 52.

[193] Bühler (n 58) 28.

summary of the thesis and to avoid repetition in the thesis, conclusions drawn from the conflicting points and their reconciliation are moved to the conclusion chapter which is the next one.

§ 5. CONCLUSION

Prior to the DCD, monetisation of personal data was not discussed in the EU at legislation level. The enactment of the DCD has opened the Pandora's Box that involves conflicting points between the monetisation of personal data and its human rights foundations. Although the references regarding the implementation of the Directive without prejudice to the GDPR and e-Privacy Directive, reconciliation of them is a simple necessity due to existing ambiguities.

The main criticism for the DCD is that it diverges from the human rights approach reflected in the GDPR. Although alterations of wording during the legislation process were made in line with the critiques, many scholars were not persuaded that the conflicting points were resolved they have proposed resolutions on two divergent perspectives. One of the resolutions is that the DCD should be applied only provided that the consumer "actively imparted his personal data" to the supplier. However, this approach is not intended for analysing the relationship between the DCD and the GDPR. Another proposal is put forward by *Janecek and Malgieri,* who developed the dynamically limited alienability rule to establish a link between data protection law and contract law rules and principles. It is based upon systematising the conditions regarding processing of personal data in the GDPR and does not formulate a novel interpretation for the decent application of the DCD. *Sattler* states that the incompatibilities in question should be resolved by courts –especially by the CJEU- as the bridge builder. However, this proposal is not related to the content of the resolution but meaning of it. Consequently, the question of the how the two divergent approaches can be reconciled in a coherent way is still unanswered.

This research aims to fill the gap by developing an interpretation to propose a way of reconciliation between the approaches of the GDPR and of the DCD. Accordingly, this thesis provides an answer for the following research question:

> Is there a conflict between the DCD's regime of regulating personal data as an object of commercial transaction and the GDPR's approach where personal data must be protected based on human rights foundations? If yes, how can this conflict be reconciled?

While seeking the answer to that question, the research is limited with the concept "data as counter-performance contracts" including paid and gratuitous ones. The perspective taken by this thesis is essentially data protection law rather than contract law rules. Furthermore, this thesis focuses on the GDPR and the DCD as the legal framework. On the GDPR side, principles and legal grounds, especially consent, relating to processing of personal data are considered as a principal focal point. On the other side, the DCD is considered within its data-related provisions. In relation to the legal framework, this thesis focuses on the human rights foundations of the GDPR and the contractual freedom principle behind the DCD.

Within determined limitations, this thesis claims that the reconciliation should be made on at least three topics as follows: determination of the risks for processing of personal data to be provided by the consumer, distinguishing data as counter-performance contracts from traditional ones to manage the "necessity" problem in the Art. 7(4) GDPR and formulation of an interpretation on the exceptions in the Art. 3(1) DCD.

First of all, there is a tension between the contractual freedom approach that is taken by the DCD and human rights foundations of the GDPR. It is because, monetisation of personal data without any further limitations on freedom of contract principle may lead to losing the consumer's control over their personal data. Accordingly, the GDPR's human rights foundations might be challenged by monetisation of personal data, as they include "minimum and non-negotiable level of privacy and data protection". This thesis argues that limitation of the freedom of contract principle should be based on the risk in which consumers may lose the control over their personal data. Accordingly, it could be focused on three risky categories, which are external sources of personal data, sensitive data, and vulnerable persons' data. As a result, these categories of personal data should be confronted with scepticism by traders to ensure compliance with the data protection rules and principles.

As regards to consent, which is one of the most appropriate legal ground for processing, requirements of the Art. 7(4) might create a conflicting point. Because, if the Art. 7(4) GDPR is interpreted strictly, consent will be invalidated in many cases. Invalidation of the consent renders the processing of personal data illegal in certain cases, and this constitutes a conflicting point between the Art. 7(4) GDPR and the DCD. Accordingly, it is arguable that data as counter-performance contracts might be distinguished from traditional contracts where the supplier provides traditional goods and services to developing an interpretation. In line with this distinction, the phrase "necessary for the performance" should be interpreted broadly in DACP contracts since it inherently requires processing more data than traditional contracts do and digital content and digital services are distinguished from traditional goods and services by specific conformity criteria stipulated under the articles 7 and 8 DCD.

Finally, choice of wording in the exceptions in the Art. 3(1) DCD might lead to a confusion in relation to two legal grounds of the GDPR, since they connotate the contract in Art. 6(1)(b) and legal obligation in Art. 6(1)(c). If these exceptions exactly overlap with the two legal grounds, the consumer cannot be safeguarded by the DCD in cases where these two legal grounds are applicable. Given the consumer-safeguarding aims of the DCD and the GDPR, this thesis proposes that the exceptions in the Art. 3(1) DCD should be interpreted narrowly while two specific legal grounds -Art. 6(1)(b) and Art. 6(1)(c) of the GDPR- should be construed broadly. Therefore, the consumer's protection area will be expanded in line with the aim of the DCD.

This thesis' resolution proposals are not based on the idea of necessity for new legislation package but primarily aim to establish a new mindset for traders via adopting soft law instruments. The reason for this choice is that the prospect for the revision of the DCD's wording is pretty low given the chosen path by the EU, which is recognition of de facto value of personal data. Accordingly, the reconciliation should initially be performed by the European Data Protection Board, and data protection authorities through their prospective and non-binding guidances (*ex-ante*). Apart from the soft law instruments, a merely consistent CJEU practice will be able to remove the blurry points in terms of the interplay between the DCD and the GDPR. So, the CJEU will play a key role in forming a binding interpretation regarding the controversies arising in the interplay between two approaches (*ex-post*). However, this might take a fairly long time when considered the fully effective date of the DCD (July 2022), and a legal dispute might arise after that time.

By proposing flexible resolutions, it should be acknowledged that conflicting points and their resolutions in this thesis, which seeks to fill the gap in the literature, are open-ended for possible developments. Especially interpretations developed regarding the separation of data as counter-performance contracts from traditional ones is not perfectly clear since such an approach is unfounded in the literature. Therefore, the resolutions might be considered as a departure point for further interpretations by data protection advocates, authorities and European courts.

As concluding remarks, the EU was at a fork in the road to data-driven economy on the question whether de facto value of personal data should be identified, and the option of the recognition was chosen with the enactment of the DCD in 2019. Shortly afterwards, the EU once again showed its desire to unleash the value of personal data in data-driven economy by proposing the Digital Governance Act that included indirect references to utilizing the value of personal data. It is highly likely that the EU will widen the path regarding the utilisation of personal data in near future. Therefore, it certainly requires that a fair balance should be struck between the human rights character of the right to data protection and trading them in commercial transactions with appropriate legal tools. And this necessity is not merely related to the DCD but to prospective EU acts on the commodification of personal data.

BIBLIOGRAPHY

Primary Sources

Efroni Z, 'Gaps and Opportunities: The Rudimentary Protection for "Data-Paying Consumers" Under New EU Consumer Protection Law' [2020] Common Market Law Review 799

Janeček V and Malgieri G, 'Commerce in Data and the Dynamically Limited Alienability Rule' (2020) 21 German Law Journal 924

Kuner C, Bygrave LA and Docksey C (eds), The EU General Data Protection Regulation (GDPR): A Commentary (Oxford University Press 2020)

Midorović S and Sekulić M, 'A New Function of Personal Data in the Light of the Contract for the Supply of Digital Content and Digital Services' (2019) 53 Zbornik radova Pravnog fakulteta, Novi Sad 1145

Narciso M, '"Gratuitous" Digital Content Contracts in EU Consumer Law' [2017] EuCML 9

Schulze R and Staudenmayer D (eds), EU Digital Law: Article-by-article commentary (Nomos 2020)

Secondary Sources

A29WP, 'Opinion 1/98: Platform for Privacy Preferences (P3P) and the Open Profiling Standard (OPS)' (1998)

——, 'Opinion 03/2013 on Purpose Limitation' (2013)

——, 'Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC' (2014)

——, 'Guidelines on Consent under Regulation 2016/679' (2018)

Alan Schwartz, 'Justice and the Law of Contracts: A Case for the Traditional Approach' <https://digitalcommons.law.yale.edu/fss_papers/1122> accessed 22 June 2021

Baloup J and others, 'White Paper on the Data Governance Act (CiTiP Working Paper Series)' [2021] SSRN Electronic Journal <https://www.ssrn.com/abstract=3872703> accessed 16 July 2021

Bedir C, 'Data as Counter-Performance: Yet Another Point Where Digital Content Contracts and the GDPR Conflict' (Leiden University 2018) <https://www.ssrn.com/abstract=3648092> accessed 8 November 2020

——, 'Contract Law in the Age of Big Data' (2020) 16 European Review of Contract Law 347

Bergkamp L, 'EU Data Protection Policy' (2002) 18 Computer Law & Security Review 31

Bühler S, 'Conditional Consent as a Valid Legal Ground for Data Processing - a Misbelief?' 8

Durovic M and Montanaro M, 'Data Protection and Data Commerce: Friends or Foes?' (2021) 17 European Review of Contract Law 1

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 (v 2.0)' (2019)

——, 'Guidelines 05/2020 on Consent under Regulation 2016/679 (v1.1)' (2020)

——, 'Statement 05/2021 on the Data Governance Act in Light of the Legislative Developments' (2021)

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)' (2021)

EDPS, 'Opinion 4/2017 on the Proposal for a Directive on Certain Aspects Concerning Contracts for the Supply of Digital Content' (2017)

——, 'Opinion 8/2018 on the Legislative Package "A New Deal for Consumers"' (2018)

European Union Agency for Fundamental Rights and Council of Europe, *Handbook on European Data Protection Law* (2018)

Fennelly N, 'Legal Interpretation at the European Court of Justice' (1996) 20 Fordham International Law Journal 26

Garner BA (ed), *Black's Law Dictionary* (8th edn, 2004)

Giliker P, 'Adopting a Smart Approach to EU Legislation: Why Has It Proven So Difficult to Introduce a Directive on Contracts for the Supply of Digital Content?' in Tatiana-Eleni Synodinou and others (eds), *EU Internet Law in the Digital Era: Regulation and Enforcement* (Springer International Publishing 2020)

Haas D and Jansen C, 'Specific Performance in Dutch Law' in Jan Smits, Daniel Haas and Geerte Hesen (eds), *Specific Performance in Contract Law: National and Other Perspectives* (Intersentia 2008)

Hacker P, 'Regulating the Economic Impact of Data as Counter-Performance: From the Illegality Doctrine to the Unfair Contract Terms Directive' in Sebastian Lohsse, Reiner Schulze and Dirk Staudenmayer (eds), *Data as Counter-Performance Contract Law 2.0?* (2019)

ICO, 'Big Data and Data Protection (v1.0)' (2014)

Kemppainen L and others, 'Emerging Revenue Models for Personal Data Platform Operators: When Individuals Are in Control of Their Data' (2018) 6 27

Korff D, *EC Study on Implementation of Data Protection Directive, Comparative Summary of National Laws* (2002) <http://194.242.234.211/documents/10160/10704/Stato+di+attuazione+della+Direttiva+95-46-CE> accessed 11 June 2016

Lapuente SC, 'Termination of the Contract for the Supply of Digital Content and Services, and Availability of Data: Rights of Retrieval, Portability and Erasure in EU Law and Practice' in Sebastian Lohsse, Reiner Schulze and Dirk Staudenmayer (eds), *Data as Counter-Performance - Contract Law 2.0?: Münster Colloquia on EU Law and the Digital Economy V* (Nomos 2020)

Laudon KC, 'Markets and Privacy' (1996) 39 Communications of the ACM 92

Lewinski VK v., 'Wert von Personenbezogenen Daten', *DatenDebatten: Band 3* (Erich Schmidt 2019)

Li C and others, 'A Theory of Pricing Private Data' (2017) 60 Communications of the ACM <https://dl.acm.org/doi/10.1145/3139457> accessed 26 February 2021

Lynskey O, *The Foundations of EU Data Protection Law* (First edition, Oxford University Press 2015)

Malgieri G, 'The Concept of Fairness in the GDPR: A Linguistic and Contextual Interpretation' (ACM 2020)

Malgieri G and Custers B, 'Pricing Privacy – the Right to Know the Value of Your Personal Data' (2018) 34 Computer Law & Security Review 289

Mańko R and Monteleone S, 'Contracts for the Supply of Digital Content and Personal Data Protection (European Parliament Research Service, Briefing)' (2017)

Markesinis BS, Unberath H and Johnston AC, *The German Law of Contract: A Comparative Treatise* (2nd ed, Hart Publishing 2006)

Metzger A, 'Data as Counter-Performance' [2017] Journal of Intellectual Property, Information Technology and Electronic Commerce Law 1

——, 'A Market Model for Personal Data: State of Play under the New Directive on Digital Content and Digital Services' in Sebastian Lohsse, Reiner Schulze and Dirk Staudenmayer (eds), *Data as Counter-Performance - Contract Law 2.0?: Münster Colloquia on EU Law and the Digital Economy V* (Nomos 2020)

Prins JEJ, 'The Propertization of Personal Data and Identities' (2004) 8 Electronic Journal of Comparative Law 1

Purtova N, 'Private Law Solutions in European Data Protection: Relationship to Privacy, and Waiver of Data Protection Rights' (2010) 28 Neth. Q. Hum. Rts. 179

Riechert A, 'Data as a Counter-Performance' in Reiner Schulze and Dirk Staudenmayer (eds), *Data as Counter-Performance - Contract Law 2.0?: Münster Colloquia on EU Law and the Digital Economy V* (Nomos 2020)

Robert R and Smit L, 'The Proposal for a Directive on Digital Content: A Complex Relationship with Data Protection Law' (2018) 19 ERA Forum 159

Sattler A, 'Autonomy or Heteronomy – Proposal for a Two-Tier Interpretation of Art 6 GDPR' in Reiner Schulze and Dirk Staudenmayer (eds), *Data as Counter-Performance - Contract Law 2.0?: Münster Colloquia on EU Law and the Digital Economy V* (Nomos 2020)

——, 'Neues EU-Vertragsrecht für digitale Güter' [2020] Computer und Recht 145

Schmidt-Kessel M, 'Right to Withdraw Consent to Data Processing The Effect on the Contract' in Reiner Schulze and Dirk Staudenmayer (eds), *Data as Counter-Performance - Contract Law 2.0?: Münster Colloquia on EU Law and the Digital Economy V* (Nomos 2020)

Sein K and Spindler G, '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' (2019) 15 European Review of Contract Law 257

Sénéchal J, 'Article 16(2) of the "Digital Content and Digital Services" Directive on the Consequences of Termination of Contract, or the Difficult Articulation between Union Law on Consumer Contract and Union Law on the Protection of Personal Data' in Reiner Schulze and Dirk Staudenmayer (eds), *Data as Counter-Performance - Contract Law 2.0?: Münster Colloquia on EU Law and the Digital Economy V* (Nomos 2020)

Staudenmayer D, 'The Directives on Digital Contracts: First Steps Towards the Private Law of the Digital Economy' 32

Vanherpe J, 'White Smoke, but Smoke Nonetheless: Some (Burning) Questions Regarding the Directives on Sale of Goods and Supply of Digital Content' [2020] European Review of Private Law 251

Versaci G, 'Personal Data and Contract Law: Challenges and Concerns about the Economic Exploitation of the Right to Data Protection' (2018) 14 European Review of Contract Law 374

Weiß R, 'Data as Counter-Performance & the Digital Content Directive – The End of a Debate?' in Reiner Schulze and Dirk Staudenmayer (eds), *Data as Counter-Performance - Contract Law 2.0?: Münster Colloquia on EU Law and the Digital Economy V* (Nomos 2020)

Wendehorst C, 'Personal Data in Data Value Chains – Is Data Protection Law Fit for the Data Economy?' in Reiner Schulze and Dirk Staudenmayer (eds), *Data as Counter-Performance - Contract Law 2.0?: Münster Colloquia on EU Law and the Digital Economy V* (Nomos 2020)

Zoll F, 'Personal Data as Remuneration in the Proposal for a Directive on Supply of Digital Content' in Reiner Schulze, Sebastian Lohsse and Dirk Staudenmayer (eds), *Contracts for the Supply of Digital Content: Regulatory Challenges and Gaps* (2017)

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

Case-law

CJEU, Case C-139/01 Österreichischer Rundfunk and Others [2003].

CJEU, Case C-131/12 Google Spain, [2014].

CJEU, Joined cases C-293/12 and C-594/12, Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others [2014].

CJEU, C-149/15 Sabrina Wathelet v Garage Bietheres & Fils SPRL [2016]

Internet Sources

Austrian OGH asks CJEU if Facebook "undermines" GDPR since 2018 < https://noyb.eu/en/breaking-austrian-ogh-asks-cjeu-if-facebook-undermines-gdpr-2018> accessed 23 July 2021.

Cirillo, G, 'Data as Counter-Performance and Transformative Contract Law', <https://transformativeprivatelaw.com/data-as-counter-performance-and-transformative-contract-law/> accessed 16 July 2021.

Efroni Z, 'Data Protection Aspects of the Digital Content Directive' (Conference on Data Protection in Digital Era, Istanbul (Zoom), 16 April 2021) <https://youtu.be/YvRipkWV8uA?t=4280> accessed 10 June 2021

Facebook's GDPR bypass reaches Austrian Supreme Court, <https://noyb.eu/en/facebooks-gdpr-bypass-reaches-austrian-supreme-court> accessed 9 April 2021.

Management Study Guide, Consumer Modeling - Meaning and its Different Aspects, <https://www.managementstudyguide.com/consumer-modeling.htm> accessed 6 March 2021.

University of Cambridge, Centre for Intellectual Property and Information Law, 'European Data Protection - National Laws: Current and Historic' <https://www.cipil.law.cam.ac.uk/resources/european-data-protection-national-laws-current-and-historic> accessed 10 March 2021.

What is my personal data worth? – Commoditised data as "counter performance", <https://www.bristows.com/news/what-is-my-personal-data-worth-commoditised-data-as-counter-performance/> accessed 16 July 2021.

Is sharing personal data for free java worth the risk?, <https://blog.avast.com/shiru-cafe-offers-free-coffee-for-personal-data > accessed 20 July 2021.