

Gaps and Opportunities: The Rudimentary Protection to 'Data-Paying Consumers' under New EU Consumer Protection Law

Efroni, Zohar

Erstveröffentlichung / Primary Publication

Diese Arbeit wurde durch das Bundesministerium für Bildung und Forschung (BMBF) gefördert (Förderkennzeichen: 16DII111, 16DII112, 16DII113, 16DII114, 16DII115, 16DII116, 16DII117 - "Deutsches Internet-Institut"). / This work has been funded by the Federal Ministry of Education and Research of Germany (BMBF) (grant no.: 16DII111, 16DII112, 16DII113, 16DII114, 16DII115, 16DII116, 16DII117 - "Deutsches Internet-Institut").

Empfohlene Zitierung / Suggested Citation:

Efroni, Z. (2020). *Gaps and Opportunities: The Rudimentary Protection to 'Data-Paying Consumers' under New EU Consumer Protection Law*. (Weizenbaum Series, 4). Berlin: Weizenbaum Institute for the Networked Society - The German Internet Institute. <https://doi.org/10.34669/wi.ws/4>

Nutzungsbedingungen:

Dieser Text wird unter einer CC BY-NC-SA Lizenz (Namensnennung-Nicht-kommerziell-Weitergabe unter gleichen Bedingungen) zur Verfügung gestellt. Nähere Auskünfte zu den CC-Lizenzen finden Sie hier: <https://creativecommons.org/licenses/by-nc-sa/4.0/deed.de>

Terms of use:

This document is made available under a CC BY-NC-SA Licence (Attribution-NonCommercial-ShareAlike). For more information see: <https://creativecommons.org/licenses/by-nc-sa/4.0>

Weizenbaum Series #4

Working Paper

**Gaps and Opportunities:
The Rudimentary Protection to
‘Data-Paying Consumers’ under
New EU Consumer Protection Law**

Zohar Efroni

March 2020

Weizenbaum Series

Edited by

Weizenbaum Institute for the Networked Society -
The German Internet Institute

Project Coordination:

Wissenschaftszentrum Berlin für Sozialforschung
Reichpietschufer 50
10785 Berlin

Visiting Address:

Hardenbergstraße 32
10623 Berlin
Email: info@weizenbaum-institut.de
Web: www.weizenbaum-institut.de

Persistent long-term archiving of this series is ensured by the Social Science Open Access Repository and the DOI registration service in Germany for social science and economic data da|ra.

DOI [10.34669/wi.ws/4](https://doi.org/10.34669/wi.ws/4)

This series is available open access and is licensed under Creative Commons Attribution 4.0 (CC-BY-NC-SA 4.0):
<https://creativecommons.org/licenses/by-nc-sa/4.0/>

This work has been funded by the Federal Ministry of Education and Research of Germany (BMBF) (grant no.: 16DII111, 16DII112, 16DII113, 16DII114, 16DII115, 16DII116, 16DII117 - "Deutsches Internet-Institut").

Weizenbaum Series #4
Working Paper*

Gaps and Opportunities: The Rudimentary Protection to 'Data-Paying Consumers' under New EU Consumer Protection Law

Zohar Efroni**

March 2020

Keywords: Digital Content Directive; Data as counter-performance; contract law; consumer protection; data protection.

* Forthcoming in the Common Market Law Review. All websites were last accessed on 20 February 2020.

** Dr Zohar Efroni, LL.M., Weizenbaum Institute for the Networked Society in Berlin; Humboldt University Law Faculty, Berlin. This work was funded by the Federal Ministry of Education and Research of Germany (BMBF) under grant no 16DII111 („Deutsches Internet-Institut“). For correspondence: zohar.efroni@rewi.hu-berlin.de

Table of Contents

1. Introduction.....	5
2. Level of Harmonisation	7
3. Data as Counter-Performance	9
3.1. Data as Counter-Performance in Consumer Contracts	9
3.1.1. Recognition in the Final DCSD Text	
3.1.2. Normative Priority of EU Data Protection and Privacy Law	
3.1.3. Non-Personal Data	
3.1.4. Evaluation	
3.2. Coverage of Passively Provided Data	17
3.2.1. Should Passively Provided Data Qualify as Counter-Perfor-	
mance Under the DCSD?	
4. Digital Content and Services Connected to Physical Goods	22
4.1. How to Treat Physical Objects that are Bundled with Digital Content	
or Services?	22
4.2. The Solution: Excluding ‘Goods with Digital Elements’ from the DCSD ...	22
4.3. Evaluation	23
4.3.1. The General Approach	
4.3.2. Interface with the Consumer Rights Directive	
4.3.3. Application of the SGD to IoT Goods	
5. Data Portability	30
5.1. Data Portability Rights under the DCSD	30
5.2. Evaluation	31
6. Conformity and Non-Discrimination.....	32
7. Concluding Remarks.....	33

1. Introduction

Not all the ostensibly free contents, services and products offered in digital form over the internet are an expression of sheer gratuitousness. Very often, traders monetise data and contents that are being provided and generated over the course of using the content or service instead of charging money for that use. For instance, Google, with its extremely popular search engine and many useful web applications, does not charge its users a cent for taking advantage of its high-quality products, provided that Google is permitted to use and monetise the data, including personal data.¹

One key question is whether such arrangements constitute a valid contract where the user's counter-performance is reduced to merely providing data. Should that be the case, the next questions are what kind of a contract this is and whether the user may benefit from consumer protection law with respect to the digital contents or services even though she did not pay any price for it.

Against this backdrop and the unsuccessful attempt to harmonise European sales law more generally,² the European Commission published in December 2015 two proposals for directives that would regulate certain aspects concerning contracts for the supply of digital content ('COM-DCD')³ and for the online sale of goods.⁴ The proposals have triggered a lively debate that continued during the various phases of legislation,⁵ with the European Parliament and the Council of the EU proposing along

1 see <https://policies.google.com/privacy?hl=en-US>

2 see <https://www.europarl.europa.eu/legislative-train/theme-connected-digital-single-market/file-common-european-sales-law>

3 COM, 'Proposal for a Directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content', COM(2015) 634 final, 2015/0287 (COD), 09.12.2015 (hereinafter 'COM-DCD').

4 COM, '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', COM(2015) 635 final, 2015/0288 (COD) 09.12.2015.

5 See, e.g., Reiner Schulze, Dirk Staudenmayer and Sebastian Lohsse (eds), *Contracts for the Supply of Digital Content: Regulatory Challenges and Gaps*, Münster Colloquia on EU Law and the Digital Economy II (Nomos, 2017); European Law Institute (ELI), 'Statement on the European Commission's proposed directive on the supply of digital content to consumers' (ELI, 2016) https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Statement_on_DCD.pdf; Interventions submitted to the JURI Committee at the Workshop 'New rules for contracts in the digital environment' (Brussels, 17.02.2016) <http://www.europarl.europa.eu/committees/de/juri/events-workshops.html?id=20160217CHE00181>. For further literature (mostly in the German language), see Philipp Hacker, 'Daten als Gegenleistung: Rechtsgeschäfte im Spannungsfeld von DSGVO und allgemeinem Vertragsrecht', (2019) *Zeitschrift für die gesamte Privatrechtswissenschaft*, 148-197; Niko Härting, 'Digital Goods und Datenschutz – Daten sparen oder monetarisieren? Die Reichweite des vom DinHRL-E erfassten Geschäftsmodells', 11 *Computer und Recht* (2016) 735-740; Axel Metzger, 'Data as Counter-Performance - What Rights and Duties do Parties Have?', 8(1) *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* (2017) 2-8; Andreas Sattler, 'Personenbezogene Daten als Leistungsgegenstand - Die Einwilligung als Wegbereiter des Datenschuldrechts', 72(21) *JZ* (2017), 1036-1046; Martin Schmidt-Kessel et. al., 'Die

the way significant changes to the original proposals ('Council-DCD' and 'EP-DCD', respectively).⁶ At the conclusion of the trilogue negotiations in March 2019, the texts of Digital Content and Digital Services Directive and the Sale of Goods Directive received their final form⁷ and they were consequently published over the online portal of the EU Parliament.⁸ On the 22nd of May 2019, both directives (referred to hereinafter as 'DCSD' and 'SGD', respectively) were published in the Official Journal of the European Union.⁹

Some of the concerns addressed data-related aspects of the new instruments,¹⁰ including (1) coverage of situations, in which the consumer provides data as counter-performance instead of a price for digital content and services (referred to for convenience as 'data-paying consumers'); (2) the inclusion of embedded digital content (in the current texts of the directives: 'goods with digital elements') within the scope of the DCD

Richtlinienvorschläge der Kommission zu Digitalen Inhalten und Online-Handel - Teil 1', (2016) *European Union Private Law Review Fokus* 2-8; Martin Schmidt-Kessel et. al., 'Die Richtlinienvorschläge der Kommission zu Digitalen Inhalten und Online-Handel - Teil 2', (2016) *European Union Private Law Review Fokus* 54-70; Louisa Specht, 'Daten als Gegenleistung - Verlangt die Digitalisierung nach einem neuen Vertragstypus?', 72(15-16) *JZ* (2017), 763-770; Gerald Spindler, 'Verträge über digitale Inhalte – Anwendungsbereich und Ansätze Vorschlag der EU-Kommission zu einer Richtlinie über Verträge zur Bereitstellung digitaler Inhalte', 19(3) *MultiMedia und Recht. Zeitschrift für IT-Recht und Recht der Digitalisierung* (2016), 147-153; Gerald Spindler, 'Verträge über digitale Inhalte – Haftung, Gewährleistung und Portabilität Vorschlag der EU-Kommission zu einer Richtlinie über Verträge zur Bereitstellung digitaler Inhalte', 19(4) *MultiMedia und Recht. Zeitschrift für IT-Recht und Recht der Digitalisierung* (2016), 219-224; Friedrich Graf von Westphalen, 'Richtlinienentwurf der Kommission betreffend die Bereitstellung digitaler Inhalte und das Recht des Verbrauchers auf Schadensersatz', (2016) *Betriebs-Berater*, 1411-1418; Friedrich Graf von Westphalen and Cristiane Wendehorst, 'Hergabe personenbezogener Daten für digitale Inhalte - Gegenleistung, bereitzustellendes Material oder Zwangsbeitrag zum Datenbinnenmarkt?', (2016) *Betriebs-Berater* 2179-2187.

6 For the draft of the Digital Content Directive, see Council, 'Proposal for a Directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content (First reading) – General approach', 9901/17 ADD 1, 2015/0287 (COD), 01.06.2017 (hereinafter 'Council-DCD'); European Parliament, 'Report 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 (COM(2015)0634 – C8-0394/2015 – 2015/0287(COD))', A8-0375/2017, 27.11.2017; (hereinafter referred to as 'EP-DCD').

7 Nikolina Sajn, 'Briefing, 'Contracts for the supply of digital content and digital services'', PE 635.601 – March 2019, [http://www.europarl.europa.eu/RegData/etudes/BRIE/2019/635601/EPRS_BRI\(2019\)635601_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/BRIE/2019/635601/EPRS_BRI(2019)635601_EN.pdf).

8 See <http://www.europarl.europa.eu/news/en/press-room/20190321IPR32116/parliament-boosts-consumer-rights-online-and-offline>.

9 DIRECTIVE (EU) 2019/770 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services, OJ L 136/1 (hereinafter 'DCSD'); DIRECTIVE (EU) 2019/771 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 20 May 2019 on certain aspects concerning contracts for the sale of goods, amending Regulation (EU) 2017/2394 and Directive 2009/22/EC, and repealing Directive 1999/44/EC, OJ L 136/28 (hereinafter 'SGD').

10 Axel Metzger et al. 'Data-Related Aspects of the Digital Content Directive', (2018) 9(1) *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, <https://www.jipitec.eu/issues/jipitec-9-1-2018/4682> at 90-109.

proposal; (3) data portability under the scheme of the DCD proposal and its relationship to the GDPR; and (4) aspects related to conformity, modification and termination. Within the emerging legal framework as applied to data-paying consumers, the explicit inclusion of (only) personal data (but possibly not any other data) as counter-performance under the DCSD and the simultaneous application of the GDPR to such situations have drawn much attention during the legislation phase.¹¹ Another important question focused on the application of the Commission's proposal only to data that are actively provided by the consumer rather also to data that are passively collected under the consumer's general permission to conduct such collection.¹²

With the entry into force in June 2019 of both directives under their amended titles (adding 'digital services' to the title of the Commission's proposal)¹³ it is a suitable time to revisit these issues while devoting special attention to the application of the DCSD – alongside other digital consumer protection instruments in the EU – to data-paying consumers.

2. Level of Harmonisation

The aim of the DCSD is to fully harmonise certain requirements concerning contracts between traders and consumers for the supply of digital content or services (Recital 11 DCSD). As stated there, the DCSD is explicitly designed to harmonise 'rules on the conformity of digital content or a digital service with the contract, remedies in the event of a lack of such conformity or a failure to supply and the modalities for the exercise of those remedies, as well as on the modification of digital content or a digital service'.

Article 4 prohibits Member States from introducing more or less stringent provisions concerning DCSD-regulated areas unless otherwise specially provided in the directive. Recitals 12 through 17 lay out a fairly long list of matters, in which Member States are not strictly bound by the DCSD. These matters include national rules on the formation, validity, nullity or effects of contracts, the legal nature or classification of the

11 See e.g., Fryderyk Zoll, 'Personal Data as Remuneration in the Proposal for a Directive on Supply of Digital Content' in Schulze, Staudenmayer and Lohsse (eds) (2017) n. 5 at 178.

12 Axel Metzger et al. (2018) n. 10 at 95-96.

13 The title of the directive concerning the sale of goods has been amended to cover 'certain aspects concerning contracts for the sale of goods' while changing the originally proposed title covering 'contracts for the online and other distance sales of goods' in order to include also goods that are being sold face-to-face by retailers. The intention was to avoid divergent regulation. See Recital 9 SGD. In addition, also the title of the DCD proposal has been amended to explicitly cover digital services alongside digital content.

contract, remedies for hidden defects and claims against any third party that is not the trader (Recitals 12-13).

For completing the picture, the Sale of Goods Directive has a similar maximum harmonisation agenda regarding that aspects its targets.¹⁴ The DCSD's definition of a 'trader' (Article 2(5) DCSD)¹⁵ is virtually identical to the definition of the SGD's definition of a 'seller' (Article 2(3) SGD).¹⁶ Member States enjoy a broad latitude to extend the application of the DCSD to parties that are not strictly 'consumers' in the meaning of the DCSD (Recital 16). There is a parallel statement in Recital 21 SGD. At the same time, Member States might be more restricted in expanding the general application scope of the directive to parties that are not strictly 'traders' in the meaning of the DCSD. This conclusion can be derived from Recital 18 DCSD, which allows to extend the scope of the directive specifically to platform providers that do not fulfil the requirements of a trader under the DCSD.¹⁷ There is a parallel provision in Recital 23 SGD. That said, it appears that Member States have a broader leeway in expanding the scope of liability to third parties that do not qualify as traders.¹⁸

The new DCSD harmonises the duty of the trader to supply (Article 5), which in the usual case should take place without undue delay after the conclusion of the contract. It further imposes on traders extensive duties of objective and subjective conformity in performing their part of the contract (Articles 6, 7, and 8). Among other things, the Directive contains burden of proof rules that benefit consumers (Article 12) and sets forth the rights to consumer remedy where the trader fails to supply (Article 13) or fails to comply with the conformity requirements. The remainder of this article focuses on the implication of the DCSD (and relevant legal instruments that apply in parallel)

14 Recital 10, SGD.

15 'trader' means any natural or legal person, irrespective of whether privately or publicly owned, that is acting, including through any other person acting in that natural or legal person's name or on that person's behalf, for purposes relating to that person's trade, business, craft, or profession, in relation to contracts covered by this Directive.'

16 'seller' means any natural person or any legal person, irrespective of whether privately or publicly owned, that is acting, including through any other person acting in that natural or legal person's name or on that person's behalf, for purposes relating to that person's trade, business, craft or profession, in relation to contracts covered by this Directive.'

17 See also, 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(3) *ERCL* 257, 261 (noting that the platform provider must in such case undertake the obligation to provide the digital content or service).

18 Recital 13 DCSD: 'Member States also remain free, for example, to regulate liability claims of a consumer against a third party other than a trader that supplies or undertakes to supply the digital content or digital service, such as a developer which is not at the same time the trader under this Directive.'

for data-paying consumers and highlights some gaps in the consumer protection scheme in this specific context.

3. Data as Counter-Performance

3.1. Data as Counter-Performance in Consumer Contracts

3.1.1. Recognition in the Final DCSD Text

The COM-DCD included a provision that extended the scope of the directive to cases where the consumer actively provides, in exchange for digital content, counter-performance other than money in the form of personal data or any other data.¹⁹

This language and the accompanying recitals triggered amendment proposals by the European Parliament and the Council, as well as an opinion by the European Data Protection Supervisor. The latter was quite critical toward the idea of personal data functioning as counter-performance in bargains that have a commercial context.²⁰ Several commentators recommended to explicitly regard data (including personal data) as counter-performance within the scope of the DCD in order to avoid unwarranted discriminatory treatment based on the type of counter-performance the consumer provides.²¹

The DCSD now clarifies this central question: Personal data that are provided by the consumer in exchange for digital content or digital services constitute a bargain that is in principle covered by the directive. This coverage rule is subject to two exceptions: (1) when the personal data is provided by the consumer is exclusively processed by the trader for the purpose of supplying the digital content or digital services, or (2) for allowing the trader to comply with legal requirements to which the trader is subject, - and in both cases, the trader does not process that data for any other propose.²² The two

¹⁹ Article 3(1) and Recital 13, 14 COM-DCD.

²⁰ EDPS, ‘Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content’ (EDPS, 14 March 2017), https://edps.europa.eu/sites/edp/files/publication/17-03-14_opinion_digital_content_en.pdf. The opinion noted that ‘[t]here might well be a market for personal data, just like there is, tragically, a market for live human organs, but that does not mean that we can or should give that market the blessing of legislation.’ *ibid* para. 17.

²¹ See e.g., Vanessa Mak, ‘The new proposal for harmonised rules on certain aspects concerning contracts for the supply of digital content – In-Depth Analysis’ in *The new proposal for harmonized rules on certain aspects concerning contracts for the supply of digital content*, Workshop for the JURI Committee, EP (2016) 10-11; Axel Metzger et al. (2018) n. 10 at 96.

²² Art. 3(1) DCSD.

exceptions address situations, in which the data users provide have a function other than as a contractual *quid pro quo*. Since questions of contractual formation and validity are left to be answered by domestic laws,²³ domestic classification of the exchange as a ‘contract’ remains a general threshold for the application of the DCSD.

At the same time, the DCSD (as opposed to the COM-DCD) no longer includes the phrase ‘counter-performance’ in connection with personal data provided by the consumer. It further omitted the phrase ‘in exchange’ which referred in the COM-DCD directly to the phrase ‘a consumer actively provid[ing] counter-performance other than money in the form of personal data or any other data.’

The reason for this new wording seems to be the wish to avoid the impression that the directive encourages bargains in which consumers commercialise their personal data.²⁴ However, this attempt to downplay the commercial dimension obviously does not indicate that the DCSD in fact excludes situations where personal data replace other forms of contractual consideration (mainly, money paid by the consumer).²⁵ Rather, the provisions of Article 3(1) DCSD, which delineate the scope of the directive and the limitations thereto, are decisive on this matter. In light of the clear language of the second sentence of Article 3(1) DCSD, dropping the phrase ‘counter-performance’ turns out being rather a semantic, not a substantive, alteration.

3.1.2. Normative Priority of EU Data Protection and Privacy Law

Regarding the application of the EU General Data Protection Regulation (GDPR) to personal data that are provided as counter-performance, the DCSD now states that in the case of any conflict, the GDPR overrides provisions under the DCSD.²⁶ The same applies to conflicts with the e-Privacy directive (Directive 2002/58/EC).²⁷ The clear priority rule favouring EU data protection and privacy law is helpful at least on a formal-theoretical level for resolving questions of parallel application. The ‘consumer’ in terms of the DCSD and the ‘data subject’ in terms of data protection law are often one and the same person in a situation covered by both legal instruments. Similarly, a ‘con-

23 Recitals 12, 24 DCSD and Art. 3(10) DCSD.

24 cf. Recital 24 DCSD (‘While fully recognising that the protection of personal data is a fundamental right and that therefore personal data cannot be considered as a commodity [...]’).

25 Karin Sein and Gerald Spindler (2019) n. 17 at 263.

26 DCSD Art. 3(8).

27 *ibid.*

troller' in terms of data protection law often qualifies as a 'trader' under the DCSD. As the two regimes apply in parallel,²⁸ tension points will certainly emerge.

Essentially, data protection law provides instructions on the conditions under which personal data may be used. Those instructions continue to apply in consumer contracts scenarios, in which the parties regard the extension of personal data a central part of the bargain, and indeed, as a performance mandated by contract. As data protection law intervenes with the operation of contract law,²⁹ and essentially, in the ability of the parties to autonomously determine the terms of the bargain and the nature of their mutual obligations, it is important to understand how far this intervention reaches and what the consequences to the parties are.

The bright-line rule stated in the DCSD regarding the overriding normative power of data protection law should help domestic legislatures and courts that reach those tension points with the task of interpreting and applying the 'correct' legal regime if both do not lead to the same result. This rule represents the general understanding that neither contract law in general nor specific consumer protection provisions can derogate from the level of protection persons enjoy under data protection and privacy law. More precisely, consumer protection under the DCSD should be 'without prejudice' to the body of law covered under the mentioned EU data protection and privacy legislation. Indeed, according to Article 3(8) DCSD, data protection and privacy law prevails in the case of a conflict with the provisions of the DCSD. Following this instruction, a case in which data protection and privacy laws are more restrictive regarding the use of data as counter-performance would reflect the logic of the priority rule. Simply put, the parties cannot 'contract around' data protection and privacy law to the detriment of the data subject with regard to the conditions under which using personal data is permissible, and the DCSD can neither dictate nor underpin less stringent, private arrangements in this respect.

A prominent example for a tension point between the two regimes, which had been intensively discussed in the literature but not conclusively resolved yet, is the interplay between the 'personal data as counter performance' model supported by the DCSD and the restriction on coupling between consent to data processing and the provision of goods or services where the personal data is not necessary for the performance of

28 Carmen Langhanke and Martin Schmidt-Kessel, 'Consumer Data as Consideration', 6 *Journal of European Consumer and Market Law* (2015), 218-223, at 219 ff. (suggesting that two 'layers' of consumer protection apply in such cases).

29 One example of such explicit intervention concerns the obligation of the trader in the case of termination of a contract, in which the consumer has provided personal data as consideration, Article 16(2) DCSD states that '[i]n respect of personal data of the consumer, the trader shall comply with the obligations applicable under Regulation (EU) 2016/679'.

the contracts (Article 7(4)GDPR and Recital 43 GDPR). A strict interpretation to the GDPR on this point would invalidate consent in many cases the DCSD would cover, specifically, where personal data is not being exclusively processed by the trader for the purpose of supplying the digital content or digital service and where providing the data replaces payment of a price for those ‘free’ content and services provided online.³⁰ But such a strict interpretation appears to create a striking inconsistency between the GDPR and the DCSD, which has led some commentators to advocate for a more permissive interpretation of the GDPR’s prohibition on coupling to the effect that it does not outlaw what Article 3(1) DCSD permits and targets as an area in which consumer protection is warranted.³¹

The Court of Justice of the European Union (CJEU) had recently the opportunity to insert some clarity on this critical issue in its Planet49 decision (albeit considered under former EU law that preceded the enactment of the DCSD), but it preferred not to do so on procedural grounds.³² There is little doubt that the CJEU will have to revisit this matter soon.

The tension between the GDPR and the DCSD on the issue of coupling exemplifies a situation, in which data protection law would be more restrictive regarding the use of personal data in a scenario the DCSD explicitly intends to address. Consider, however, the opposite situation: What should be the implementation strategy if data protection law is more permissive about the use of personal data than contracts subject to the DCSD? One example that comes to mind is a termination situation, in which the trader invokes its legitimate interests as the legal ground for a continuous, post-termination use of personal data against the wish of the consumer.³³

30 Niko Härting (2016) n. 5 at 738-749.

31 Axel Metzger (2017) n. 5, under section 4.3. See also, Andreas Sattler, ‘Personenbezug als Hindernis des Datenhandels’, in Pertot and Schmidt-Kessel (eds), *Rechte an Daten* (forthcoming).

32 C-673/17, *Planet49 GmbH v. Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V.*, [2019] ECLI:EU:C:2019:801, para 64 (‘Lastly, it should be noted that the referring court has not referred to the Court the question whether it is compatible with the requirement that consent be ‘freely given’, within the meaning of Article 2(h) of Directive 95/46 and of Article 4(11) and Article 7(4) of Regulation 2016/679, for a user’s consent to the processing of his personal data for advertising purposes to be a prerequisite to that user’s participation in a promotional lottery, as appears to be the case in the main proceedings, according to the order for reference, at least as far as concerns the first checkbox. In those circumstances, it is not appropriate for the Court to consider that question.’).

33 Theoretically speaking, under certain interpretations of the GDPR, the legitimate interests of the controller might justify such continuous data processing irrespective of the wish of the data subject to discontinue such use. cf. Andreas Sattler, ‘Autonomie oder Determinismus – Welchen Weg geht das Datenschuldrecht?’ forthcoming in Friedewald, Lamla, Hess and Ochs (eds), *Forum Privatheit – Die Zukunft der Datenökonomie: Zwischen Geschäftsmodell, Kollektivgut und Verbraucherschutz* (Springer, 2019) at 15 ff. For discussion on the consumer’s termination rights under the DCSD and

Consider the following hypothetical: A music streaming services offers one month of free subscription under the condition that the service may collect personal data (such as regarding musical preferences of the user) and use this information for targeted marketing. Upon the expiry of the free trial, the user is obligated to pay a monthly subscription fee, and she has that option to deactivate the collection and use of personal data for targeted marketing. The user in this example decides to terminate the contract before the end of the free trial, and the trader claims to have the right to keep some personal data, as permitted under Article 6(1)(f) GDPR, based on its legitimate interest to prevent the same user from attempting another free trial of the same music service. Assume further that a domestic law generally provides that in case of a data-paying consumer, traders must, upon termination, permanently delete all the data that the consumer has provided as counter-performance.

Strictly applying Article 3(8) DCSD here would mean that such continuous use, as claimed by the trader to be legitimate under the GDPR, is permissible also under the DCSD, since it does not derogate from the rights of the data subject. In addition, the DCSD neither regulates the rights of traders to enforce contractual obligations against consumers to provide personal data nor the trader's entitlement to a continuous use of personal data after termination. It is an interesting question whether a consumer-friendly domestic rule that would flatly prohibit post-termination use of personal data in the case of legitimate interests of the trader under Article 6(1)(f) GDPR would contravene, or rather, reinforce the no-prejudice rule. A systematic reading of the DCSD would indicate that such a domestic regulation might breach the DCSD's no-prejudice rule – assuming that, in line with its Recital 4, the GDPR not only secures the rights of data subjects to exercise control over use of their data but also strikes a balance with the interests of others.

3.1.3. Non-Personal Data

Under the final text of the DCSD, some ambiguity remains regarding non-personal data that may function as counter-performance. The DCSD abandoned the phrase 'any other data' that had been included in the COM-DCD. Article 3(1) now speaks merely of cases where the 'consumer provides or undertakes to provide personal data to the

its intersection with trader's obligations under the GDPR, see Sein and Spindler, 'The new Directive on Contracts for Supply of Digital Content and Digital Services – Conformity Criteria, Remedies and Modifications – Part 2', (2019) 15(4) *ERCL* 365, 379 ff.

trader.’ The remaining question is whether data that do not qualify as personal data may also fall under this provision.

The DCSD draws systematic distinctions between personal and non-persona data – but in a different context. Such a distinction can be observed in the regulation of user-generated content under Article 16(3)-(4) DCSD. These provisions address termination and traders’ obligations generally to ‘refrain from using any content [...] which was provided or created by the consumer when using the digital content or digital service supplied by the trader’ after termination,³⁴ and also to make available to the consumer any such content at the request of the consumer.³⁵

Also regarding conformity obligations, so it appears according to the context, Recital 50 DCSD provides that ‘traders should make use of standards, open technical specifications, good practices and codes of conduct, including in relation to the commonly used and machine-readable format for retrieving the content other than personal data, which was provided or created by the consumer when using the digital content or digital service’ (emphasis added). These examples demonstrate that the drafters of the DCSD use a specific wording when they want to refer to non-personal data (‘content other than personal data’) similar to the why in which the drafters of the COM-DCD used a specific wording to achieve the same purpose (‘any other data’).

Under the final DCSD text, user-generated content is such that was generated (that is, ‘provided or created’ in the wording of Article 16(3)-(4) DCSD) by the consumer in the course of using the digital good or service. At the same time, that content by definition does not qualify as ‘personal data.’³⁶ Further, it is important to mention that references to user-generated content do not appear in the context of data as counter-performance under the DCSD, and indeed, it does not function as such in that specific context. User-generated content is typically content that is being uploaded as consumers are using the digital good or service - almost as a by-product of already ongoing relationships or relationships that have been terminated, but not necessarily as a contractual condition or obligation imposed on the consumer.³⁷ This is not to say,

³⁴ Article 16(3) DCSD.

³⁵ Article 16(4) DCSD.

³⁶ It has been observed that that likelihood of user-generated content not qualifying as personal data is quite low. See Karin Sein and Gerald Spindler (2019) n. 33 at 382; Mischau, ‘Daten als „Gegenleistung“ im neuen Verbrauchervertragsrecht’ (forthcoming 2020 in *Zeitschrift für die gesamte Privatrechtswissenschaft*) at *5.

³⁷ In practice, traders can draft the contract in such a way that secures for them the entitlement to commercially exploit user-generated content beyond what is necessary to fulfil the contract - as part of the bargain. But failing to provide such content would likely not breach any contractual obligation of the consumer. For instance, Facebook’s Terms and Condition currently include the following: ‘**Information and content you provide.** We collect the content, communications and other infor-

of course, that user-generated content does not have a commercial value³⁸ nor that such content cannot be the subject matter of contractual obligations per se.³⁹

There is no clear explanation in the Recitals or elsewhere for the removal of the phrase ‘any other data’ from Article 3(1). The plain language of this provision now mentions only ‘personal data’ as something that consumers can provide or undertake to provide alternatively to price for receiving digital goods or services. The central coverage question is whether the general conclusion that non-personal data is categorially excluded from the type of data that can function as counter-performance is mandatory.

It remains unclear which public policy would support this outcome. Indeed, in light of the GDPR’s broad concept of personal data⁴⁰ and the corresponding interpretation by the Court of Justice of the European Union,⁴¹ the practical relevance of the question might remain quite marginal. In some particular situations, however, this distinction could raise interesting queries.

Consider the following hypothetical scenario: The trader is manufacturing pet feeders. It launches a promotional campaign promising each customer who goes to a post office branch, fills out an anonymous questionnaire about the nutrition habits of her pet and anonymously sends it back to the trader via a prepaid envelope, may immediately collect at the post office, free of charge, a card containing a subscription code to a music streaming service that guarantees three months of free use of the streaming service without a requirement to abide by any additional contract with that service provider.

mation you provide when you use our Products, including when you sign up for an account, create or share content, and message or communicate with others. This can include information in or about the content you provide (like metadata), such as the location of a photo or the date a file was created [...] Our systems automatically process content and communications you and others provide to analyze context and what’s in them for the purposes described below [...] We use the information we have (including your activity off our Products, such as the websites you visit and ads you see) to help advertisers and other partners measure the effectiveness and distribution of their ads and services, understand the types of and people who use their services and how people interact with their websites, apps, and services.’ <https://www.facebook.com/about/privacy/update>. (links removed, bold letters in original).

38 See e.g., Top Examples of Successful User Generated Content Campaigns Worldwide, <https://wedevs.com/141859/user-generated-content-campaigns>.

39 It has been inquired, for instance, whether a user transferring copyrights in the content she generates and provides over a digital platform as a condition for taking advantage of the platform’s services can represent a contractual counter-performance situation. see Vanessa Mak (2016) n. 21 at 10.

40 Art. 4(1) GDPR (“personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person”).

41 Case C582/14, *Patrick Breyer v. Bundesrepublik Deutschland*, [2016] ECLI:EU:C:2016:779 (discussing the definition of ‘personal data’ under Art. 2(a) of Directive 95/46, which is considered equivalent to the definition of the same concept under the GDPR).

Assume further that it remains impossible both for the trader and for the music streaming service to know who sends which questionnaire or to link between a specific code and a specific questionnaire/user. It is further impossible to distinguish codes that are distributed as part of the promotional program from voucher codes that are unrelatedly purchased for money. The consumer later discovers to her agony that the free subscription lasts only for one month, not three, as promised by the trader. Should the consumer be prevented from bringing claims against the trader⁴² under the DCSD for lack of conformity only because the counter-performance does not qualify as a commitment to deliver personal information? The common interpretation of Article 3(1)⁴³ would leave the consumer in such cases without redress mandated by the DCSD. Another question pertains to a situation, in which the trader sufficiently anonymises the personal data to the effect that it loses its character as ‘personal data’ under the GDPR⁴⁴ and continues to monetise the data in this form. It would seem unjustified to uphold the claim of the trader that the DCSD protections cannot apply because the counter-performance (i.e., the anonymised data) no longer falls under the scope of the directive.

42 The manufacturer of the feeders should be liable as ‘trader’ under the DCSD even though the performance is being carried out on its behalf by the music service. cf. Recital 41 DCSD (‘There are various ways for the trader to supply digital content or digital services to consumers ... The digital content or digital service should be considered to be made available or accessible to the consumer *when the digital content or digital service, or any means suitable for accessing or downloading it, has reached the sphere of the consumer and no further action is required by the trader* in order to enable the consumer to use the digital content or digital service in accordance with the contract. Considering that the trader is not in principle responsible for acts or omissions of a third party which operates a physical or virtual facility, for instance an electronic platform or a cloud storage facility, that the consumer selects for receiving or storing the digital content or digital service, it should be sufficient for the trader to supply the digital content or digital service to that third party. *However, the physical or virtual facility cannot be considered to be chosen by the consumer if it is under the trader’s control or is contractually linked to the trader, or where the consumer selected that physical or virtual facility for receipt of the digital content or digital service but that choice was the only one offered by the trader to receive or access the digital content or digital service.*’ (emphasis added). In the current example, the trader chooses to perform *via* a third party under a contract between that trader and that third party. The consumer cannot select the platform and the trader remains principally responsible vis-à-vis the consumer.

43 Lena Mischau (2020) n. 36 at *5 (concluding that non-personal data are excluded from the scope of the DCSD and criticising this legislative outcome).

44 On the requisite standard for such anonymisation and doubts regarding the feasibility of complete anonymisation, see Michèle Finck and Frank Pallas, ‘They who must not be Identified – Distinguishing Personal from Non-Personal Data under the GDPR’ (2019) Max Planck Institute for Innovation and Competition Research Paper No. 19-14 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3462948.

3.1.4. Evaluation

Overall, the inclusion of (personal) data as counter-performance under the regime of the DCSD – although the explicit terms counter-performance and exchange are missing – is a welcome upshot. It contributes to aligning the level of consumer protection regardless of the question of whether the consumer pays money or provides (personal) data. This regulative approach reduces the danger of incentivising traders to prefer personal data over money as counter-performance in order to escape responsibilities under the DCSD while operating under the assumption that non-conformity vis-a-vis a data-paying consumer bears no (or fewer) legal consequences for them.⁴⁵

Some differentiations between the two consumer categories will persist, however. Different treatment may emanate from the ontology of data as informational subject-matter that carries value but is at the same time nonexcludable and its use is not rivalrous. In addition, the legal typology of personal data as being subject to data protection and privacy norms, and the intervention of such norms, might affect the legal analysis and the end-result for the consumer.⁴⁶ Such built-in and structural differences cannot be undone completely, and it is clear that equal treatment at all times cannot be attained. Examples that illustrate this proposition are reimbursement of the consumer after termination⁴⁷ or certain remedies for lack of conformity.⁴⁸

3.2. Coverage of Passively Provided Data

3.2.1. Should Passively Provided Data Qualify as Counter-Performance Under the DCSD?

Early draft proposals highlighted a distinction between actively and passively provided data in connection with the ‘data as counter-performance’ quandary. Whereas the Commission’s proposal referred only to data that is actively provided by the consu-

⁴⁵ Karin Sein and Gerald Spindler argue that the main effect of the directive on the position of data-paying consumers would mostly be limited to post termination damages under national law. See citation in n. 17 at 265. Yet, also before termination and damages, such consumers should be able to demand bringing the contract into conformity during its life by invoking important remedies, e.g., demanding updates under Sec. 8(2) DCSD.

⁴⁶ Axel Metzger et al. (2018) n. 10 at 108-109.

⁴⁷ Art. 16(1) DCSD (the remedy of reimbursement, in whole or in part, is not available for data-paying consumers).

⁴⁸ A proportionate price reduction under Art. 14 DCSD cannot be applied when no price has ever been paid. Data-paying consumers may therefore terminate faster than price-paying consumers. Recital 67 DCSD.

mer,⁴⁹ The Council draft would have allowed member states to extend the application of the directive also to passively provided data.⁵⁰ Both the Council and the EU Parliament refrained from using the term ‘actively’ within their respective amendments to Article 3 of the draft directive. The Council’s draft kept the emphasis on actively provided data, while excluding collected metadata (such as IP addresses) or automatically generated content (such as information collected and transmitted by cookies).⁵¹ By comparison, the EP-DCD would allow for the inclusion of data that is provided passively (e.g., personal data collected by the trader such as IP address).⁵²

It should be noted that the term ‘actively provides’ was not defined in the Commission’s proposal, though some clues to the situations it covered could be found in Recital 14 COM-DCD. The lack of clarity there rendered the distinction of ‘actively’ from ‘passively’ provided data blurry and the debate on the topic somewhat fuzzy. Several commentators argued that the DCSD should cover in principle both actively and passively provided data;⁵³ depriving data-paying consumers of remedies simply due to the passive manner in which data is being collected appeared neither justified nor compatible with the objectives of the directive.⁵⁴ Furthermore, the distinction between actively and passively provided data might turn ambiguous in certain situations, for instance, in case that the continuous collection of data over time is being performed after having the consumer once agreeing to such collection by the trader, but the consumer never actually provides data to the trader in an active manner (e.g., uploading, sending an email, filling out online forms or any other engagement).⁵⁵ More generally, strictly applying the directive to data that has been actively provided to the trader in exchange for digital goods/services might exclude situations, in which the trader already has the

49 COM-DCD, Recital 14 (‘As regards digital content supplied not in exchange for a price but against counter-performance other than money, this Directive *should apply only* to contracts where the supplier requests and the consumer *actively* provides data) (emphasis added).

50 Council-DCD, Article 3(1) at n. 15.

51 *ibid* at n. 15.

52 EP-DCD, Recital 14. The Recital also mentioned as covered by the directive ‘the name and e-mail address or photos, provided directly or indirectly to the trader, for example through individual registration or on the basis of a contract which allows access to consumers’ photos.’ *ibid*.

53 See e.g., Axel Metzger et al., (2018) n. 10 at 96, paras 26-28; Schmidt-Kessel et. al., ‘Die Richtlinienenvorschläge der Kommission zu Digitalen Inhalten und Online-Handel - Teil 2’, (2016) n. 5 at 59.

54 Gerald Spindler, ‘Verträge über digitale Inhalte – Anwendungsbereich und Ansätze Vorschlag der EU-Kommission zu einer Richtlinie über Verträge zur Bereitstellung digitaler Inhalte’ (2016) n. 5 at 149-159; Hacker (2019) n. 5 at 166.

55 cf. Friedrich Graf von Westphalen and Cristiane Wendehorst (2016) n. 5 at 2180-2181 (recommended to delete the adjective ‘active’ from the text of the COM-DCD).

data but wishes now to use it for a certain, new purpose (e.g., share with a third party for marketing purposes).⁵⁶

The DCSD Approach

The solution reflected in the DCSD is not entirely clear of any ambiguity. The phrase ‘actively provide[s]’ has been removed. This choice supports an interpretation that embraces both actively and passively provided data. Upon a closer inspection, however, it might also support the opposite conclusion. One clue can be found in Recital 25 DCSD, which states as follows:

‘This Directive should also not apply to situations where the trader only collects metadata, such as information concerning the consumer’s device or browsing history, except where this situation is considered to be a contract under national law. It should also not apply to situations where the consumer, without having concluded a contract with the trader, is exposed to advertisements exclusively in order to gain access to digital content or a digital service. However, Member States should remain free to extend the application of this Directive to such situations, or to otherwise regulate such situations, which are excluded from the scope of this Directive.’ (emphasis added).

The structure of this Recital is somewhat confusing. The first sentence begins with an exclusion clause (‘should also not apply’) regarding the collection of metadata, and it ends with an ‘exception’ to this exclusion, namely, ‘where this situation is considered to be a contract under national law.’ But this exception is identical to the coverage threshold of the DCSD in general, namely, that there must be a contract recognised under national law for the directive to apply. It follows that passively provided data that falls under the ‘metadata’ concept will trigger DCSD protection only then.⁵⁷ Note that the directive does not provide a definition to the term ‘metadata’, and the examples it mentioned, namely, ‘information concerning the consumer’s device or browsing history’ does not offer a conclusive answer to the coverage issue.

Another clue can be found in Recital 24 DCSD:

‘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.’

⁵⁶ A possible (not entirely satisfactory) answer to this situation might be that an additional, specific consent of the data subject is required for using the personal data for new purposes, and granting this consent qualifies as ‘providing’ the data, although the trader already ‘possesses’ them.

⁵⁷ cf. Axel Metzger, ‘A Market Model for Personal Data: State of the Play under the New Directive on Digital Content and Digital Services’ in Lohsse, Schulze and Staudenmayer (eds), *Data as CounterPerformance – Contract Law 2.0? Münster Colloquia on EU Law and the Digital Economy V* (2020), at *3 (forthcoming 2020).

This recital clarifies that providing the data and the conclusion of the contract do not have to happen simultaneously or in any specific time proximity, which leads to a related question of whether the phrase ‘personal data that the consumer might upload or create’ supports the conclusion that passive data provision is excluded. At first glance, these verbs resound active performance of providing or creating the data. At the same time, including in the concept of counter-performance data that are being created after the conclusion of the contract points in the opposite direction: whereas creating the data is a result of an active action, the provision of the data can occur passively (from the standpoint of the consumer) during the life of the contract.

This ambiguity turns relevant *inter alia* in the case of cookies. Cookies typically collect and transfer to the websites various kinds of information that help them to ‘remember’ users, including device information and browsing history. Reading Recital 24 and 25 together can lead to the conclusion that, for instance, the case of a cookie which tracks, say, browsing history – hence ‘metadata’ that the consumer, strictly speaking, neither uploads nor creates, - falls outside the scope of the directive.⁵⁸

The case of cookies is particularly interesting in light of the recent decision of the CJEU in the Planet49 case.⁵⁹ The Advocate General of the EU published an opinion according to which the active and informed consent of the person is required in the case of placing cookies that collect information covered by the Article 5(3) of Directive 2002/58/EC (the ‘e-Privacy Directive’) as amended by Directive 2009/136/EC (the ‘cookie Directive’).⁶⁰

The CJEU followed this opinion and ruled that a pre-selected checkbox does not fulfil the requirements of consent.⁶¹ Active, informed and specific consent is required for using both personal and non-personal data covered under the e-Privacy Directive,⁶² and the user should have a viable option to refuse the implementation of cookies as ‘user consent may no longer be presumed but must be the result of active behaviour

58 See Gerald Spindler and Karin Sein, ‘Die Endgültige Richtlinie über digitale Inhalte und Dienstleistungen’, *MultiMedia und Recht. Zeitschrift für IT-Recht und Recht der Digitalisierung* (2019), 415-420, at 418 (reading Recital 25 DCSD as excluding cookies information generally, and cookies information that qualifies as personal data specifically).

59 C-673/17, *Planet49* n. 32.

60 OPINION OF ADVOCATE GENERAL SZPUNAR, delivered on 21 March 2019, Case C673/17, ECLI:EU:C:2019:246. Specifically, ‘requiring a user to positively untick a box and therefore become active if he does *not* consent to the installation of cookies does not satisfy the criterion of active consent. In such a situation, it is virtually impossible to determine objectively whether or not a user has given his consent on the basis of a freely given and informed decision. By contrast, requiring a user to tick a box makes such an assertion far more probable.’ *ibid* para 88 (emphasis in original).

61 C-673/17, *Planet49* n. 32 at paras 49-65.

62 *ibid* paras 70-71.

on the part of the user.⁶³ The situation is not expected to change under the anticipated e-Privacy Regulation that would replace the e-Privacy Directive and repeal the cookie Directive.⁶⁴

The examples for ‘metadata’ provided in the DCSD could certainly qualify as confidential ‘electronic communications data’ covered under the e-Privacy Directive and proposed e-Privacy Regulation.⁶⁵ Although the act of granting consent to data collection via cookies needs to be affirmative, it does not necessarily coincide with an affirmative act of providing data (‘upload or create’) that manifests a counter-performance. In the case of cookies, then, data collection is a continuous, ongoing process that seamlessly occurs at the background without any action of users to ‘hand over’ their data. Under the jurisprudence of the CJEU in the Planet49 case, the action that is necessary for legitimising data collection through cookies under the e-Privacy Directive is the manifestation of an affirmative consent. Obviously, an affirmative act of providing the data is not required. Returning to the DCSD, the fear that including cookies situations under the directive would lead to regulating the entire Internet⁶⁶ appears a little overstated in light of the fact that these situations are already regulated (under privacy and data protection law) and since tentative recognition under national law provides an additional buffer.

Normatively, the argument for excluding such situations from the scope of the directive are not convincing, especially if its application operates to protect the weaker party in the bargain – the consumer. Domestic laws diversifying on this essential point would be detrimental to legal certainty and to the harmonisation cause behind the DCSD. But some aspects will need to be observed uniformly nonetheless: Domestically upholding such contracts should in any case be applied without prejudice to the e-Privacy Directive⁶⁷ and to the anticipated e-Privacy Regulations, and clearly, the DCSD’s transposition cannot derogate from the consent requirements established therein.

63 *ibid* para 56.

64 The Draft e-Privacy Regulation would adopt the definition of consent as stated in GDPR. See, Art. 9(1) to the EC’s Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), COM(2017) 10 final, 2017/0003 (COD), 10.01.2017.

65 Under the proposed e-Privacy Regulation, ‘‘electronic communications data’ means electronic communications content and electronic communications metadata’. Art. 4(3)(a) Draft e-Privacy Regulation, COM(2017) 10 final 2017/0003 (COD) (10.1.2017).

66 cf Dirk Staudenmayer, ‘Verträge über digitalen Inhalt’ (2016) *Neue Juristische Wochenschrift*, 2719, 2720.

67 Art. 3(8) and Recital 37 DCSD.

4. Digital Content and Services Connected to Physical Goods

4.1. How to Treat Physical Objects that are Bundled with Digital Content or Services?

The COM-DCD excluded from its scope ‘digital content which is embedded in goods in such a way that it operates as an integral part of the goods and its functions are subordinate to the main functionalities of the goods.’⁶⁸ The Council added a definition to ‘embedded digital content’ in its proposed formulation to Article 2(12), which excluded such content under the proposed Article 3(3a). By contrast, the EU Parliament would explicitly include pre-installed embedded digital content within the regulative scope of the DCD.⁶⁹

Including embedded digital content and related services within the DCD proposal seemed preferable against the alternative of covering such content and services exclusively under the proposed sale of goods directive.⁷⁰ One reason was the wish to avoid coverage gaps in situations of rental, lending and IoT products that are provided gratis (i.e., there is no sales contract) and where the trader receives data instead of money in exchange for providing those products and related services to the consumer.⁷¹

4.2. The Solution: Excluding ‘Goods with Digital Elements’ from the DCSD

Ultimately, the DCSD adopted a new definition to what is now called ‘goods with digital elements’, meaning ‘any tangible movable items that incorporate, or are inter-connected with, digital content or a digital service in such a way that the absence of that digital content or digital service would prevent the goods from performing their functions.’⁷² It explicitly excludes goods with digital elements from the coverage of the DCSD, while making such good subject to the SGD.⁷³ Since the SGD applies only

⁶⁸ COM-DCD, Recital 11.

⁶⁹ EP-DCD, Article 2(1)(1b) (defining ‘embedded digital content or digital service’); EP-DCD, Art. 3(3).

⁷⁰ cf Mak (2016) n. 21 at 8-9 (highlighting demarcation problems under the COM-DCD).

⁷¹ Axel Metzger et. al. (2018) n. 10 at 98-101.

⁷² Art. 2(3) DCSD.

⁷³ Recital 21 DCSD. (‘Directive (EU) 2019/771 [SGD] should apply to contracts for the sale of goods, including goods with digital elements. The notion of goods with digital elements should refer to goods that incorporate or are inter-connected with digital content or a digital service in such a way

to sales contracts,⁷⁴ and since the definition of sales contract found therein does not entertain the concept of data as counter-performance,⁷⁵ goods with digital elements for which the consumer provides data instead of a price are covered neither by the DCSD nor by the SGD.

It follows that transactions involving a smart device that do not constitute – or are not underpinned by – a sales contract, fall outside the scope of both the DCSD and the SGD, including cases where the consumer provides data in exchange for obtaining a good and related services. For instance, renting, lending and gratis distribution of goods with digital elements remain outside of the regulative scope the directives,⁷⁶ unless the transaction for the supply of digital elements can be severed from the transaction conserving the physical good and be treated separately and independently.⁷⁷

4.3. Evaluation

4.3.1. The General Approach

The solution described above creates a certain ‘division of labour’ between the DCSD and the SGD: Unless the physical component serves merely as data carrier of digital content, the SGD applies exclusively to sales contracts of goods that include digital elements, and the question whether the digital element in a given case is essential for the good to perform its functions is to be answered, to a large extent, by the terms of the contract itself and the surrounding circumstances. SGD-covered contracts include ‘those sales contracts which can be understood as covering the supply of specific digital content or a specific digital service because they are normal for goods of the same type and the consumer could reasonably expect them given the nature of the goods.’⁷⁸

that the absence of that digital content or digital service would prevent the goods from performing their functions. Digital content or a digital service that is incorporated in or inter-connected with goods in that manner should fall within the scope of Directive (EU) 2019/771 if it is provided with the goods under a sales contract concerning those goods. Whether the supply of the incorporated or inter-connected digital content or digital service forms part of the sales contract with the seller should depend on the content of this contract.’)

74 Art. 3.1 SGD.

75 Art. 2(1) SGD (‘sales contract’ means any contract under which the seller transfers or undertakes to transfer ownership of goods to a consumer, and the consumer pays or undertakes to pay the price thereof’).

76 cf Jorge Morais Carvalho, ‘Sale of Goods and Supply of Digital Content and Digital Services – Overview of Directives 2019/770 and 2019/771’ (2019) 5 *EuCML* 194, 198 (arguing that Member States can extend the scope of the SGD to leasing contracts).

77 Recital 21 DCSD.

78 *ibid.*

In case of doubt regarding the digital component being part of a sales contract of the physical article or not, the SGD applies.⁷⁹

The notion of good with digital elements covering products which incorporate or are inter-connected with digital content/service in such a way that the absence of that digital content/digital service would prevent the good from performing its functions reflects a simple reality in which IoT devices without the digital content/service are pretty much useless.⁸⁰ It follows that, from a consumer protection perspective, the guarantees the law provides concerning the digital content/service in principle should not fall short of the guarantees that apply to the physical good.⁸¹ As we shall see, this is not always the case.

4.3.2. Interface with the Consumer Rights Directive

In order to appreciate the consequences of this regulative choice to consumer protection more broadly, it is helpful to zoom out and take a look at the larger EU legal scheme and the interrelations with other consumer protection instruments. Perhaps most relevant in the present context is the Consumer Rights Directive (CRD) (2011/83/EU) and the changes introduced to it under the recently enacted, so-called ‘Omnibus Directive’ (Directive (EU) 2019/2161).⁸²

Like the DCSD, the CRD in its version already before the Omnibus Directive applied, *inter alia*, to digital content.⁸³ For the purpose of the CRD, contracts for digital content not supplied on a tangible medium are classified neither as sales contracts nor as services contract.⁸⁴ They are rather treated as a special contract species (similar to contracts for the supply of water, gas or electricity), with digital content being defined

⁷⁹ *ibid.*

⁸⁰ For an overview on IoT and consumer contracts, see Katarzyna Kryla-Cudna, ‘Consumer contracts and the Internet of Things’ in MaK, Tjong Tjin Tai and Berlee (eds.), *Data Science and Law* (Edward Elgar, 2018), at pp. 83-107. See also, Christiane Wendehorst, ‘Sale of goods and supply of digital content – two worlds apart? Why the law on sale of goods needs to respond better to the challenges of the digital age – In-Depth Analysis’, Study for the JURI Committee, EP (2016).

⁸¹ For a pre-DCSD/SGD discussion on the regulative options in the case of smart goods, see Sein ‘What Rules Should Apply to Smart Consumer Goods? Goods with Embedded Digital Content in the Borderland Between the Digital Content Directive and “Normal” Contract Law’ (2017) 8(2) *JIPITEC* 96.

⁸² DIRECTIVE (EU) 2019/2161 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council as regards the better enforcement and modernisation of Union consumer protection rules, OJ L 328/7 (18.12.2019).

⁸³ Recital 19 CRD. For further analysis on the interrelations between the CRD and the COM-DCD, see Martin Schmidt-Kessel et. al., ‘Die Richtlinien vorschläge der Kommission zu Digitalen Inhalten und Online-Handel - Teil 2’, n. 5 at 54-55.

⁸⁴ Recital 19 CRD.

simply as ‘data which are produced and supplied in digital form.’⁸⁵ The CRD secures some rights of consumers with respect to digital content, for instance, requirements concerning pre-contractual information duties,⁸⁶ or the rights of consumers in the case of withdrawal.⁸⁷ One inconsistency that has been identified is the lack of systematic treatment under the CRD to digital services and the fact that digital services which are provided ‘for free’ (namely, the consumer does not pay a price, but instead, provides personal data) are not covered under that directive.⁸⁸

The aim of the Omnibus Directive’s amendments to the CRD is to align the scope of application of the CRD with that of the DCSD in respect of the definitions of ‘digital content’ and ‘digital services’.⁸⁹ Recital 31 Omnibus Directive explains that the CRD already applies to contracts for the supply of digital content, which is not supplied on a tangible medium, regardless of whether the consumer pays a price in money or provides personal data. To close the gap, Recital 33 Omnibus Directive states that the scope of the amended CRD should be extended to cover also contracts under which the trader supplies or undertakes to supply a digital service to the consumer, and the consumer provides or undertakes to provide personal data.

Following this alignment agenda, the Omnibus Directive adopted the SGD’s definition of ‘goods’ to include also ‘goods with digital elements’.⁹⁰ It further amended the CRD’s definitions to ‘sales contract’⁹¹ and ‘service contract’ - with the latter bringing digital services under the definition of a service contract.⁹² Under the revision, the CRD will henceforth cover digital content which is not supplied on a tangible medium or a digital service to the consumer and the consumer provides or undertakes to provi-

85 Art. 2(11) CRD.

86 Art. 5(1)(g)-(h) CRD (referring specifically to ‘digital content’).

87 Art. 9(1), 9(2)(c) CRD.

88 Nikolina Šajn, ‘Briefing, EU Legislation in Progress, ‘Modernisation of EU consumer protection rules: A new deal for consumers’ PE 623.547 (European Parliament, April 2019) at 3, [https://www.europarl.europa.eu/RegData/etudes/BRIE/2018/623547/EPRS_BRI\(2018\)623547_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2018/623547/EPRS_BRI(2018)623547_EN.pdf).

89 See ‘Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Council Directive 93/13/EEC of 5 April 1993, Directive 98/6/EC of the European Parliament and of the Council, Directive 2005/29/EC of the European Parliament and of the Council and Directive 2011/83/EU of the European Parliament and of the Council as regards better enforcement and modernisation of EU consumer protection rules’, COM(2018) 185 final, 2018/0090(COD), 11.04.2018, <https://eur-lex.europa.eu/legal-content/EN/TEXT/?qid=1523880940100&uri=COM:2018:185:FIN> para 1.3.

90 Art. 4(1)(a) Omnibus Directive.

91 Art. 4(1)(c)(5) Omnibus Directive (‘sales contract’ means any contract under which the trader transfers or undertakes to transfer ownership of goods to the consumer, including any contract having as its object both goods and services’).

92 Art. 4(1)(c)(6) Omnibus Directive (‘service contract’ means any contract other than a sales contract under which the trader supplies or undertakes to supply a service, including a digital service to the consumer’).

de personal data to the trader, while importing verbatim the two exceptions from the DCSD concerning personal data that is exclusively provided for supplying the digital content/service or for complying with legal obligations of the trader.⁹³

The Commission's proposed definition for a 'contract for the supply of digital content which is not supplied on tangible medium' that would include digital goods provided in exchange for personal data has been deleted⁹⁴ apparently based on the understanding that such contracts are already covered under the CRD. In addition, the Omnibus Directive imported into the CRD consumer protection provisions regarding user-generated content that is not personal information, which are virtually identical to the DCSD's provisions on the subject.⁹⁵

On the whole, one important aspect of the Omnibus Directive is the explicit recognition by yet an additional EU directive (namely, the CRD) in the market phenomenon of contractual payment with personal data instead of money and the desire to extend consumer protection in such cases. But what are the implications to IoT products (or generally, 'goods with digital elements') that are provided in exchange for data instead of a price?

Indeed, Omnibus Directive amended Article 5 CRD (pre-contractual information requirements for contracts other than distance or off-premises contracts) to include goods with digital elements under the information duties to consumers regarding functionality (subsection (1)(g)) and interoperability (subsection (1)(h)). Article 6 CRD (information requirements for distance and off-premises contracts) will include similar information requirements that are generally applicable regarding digital goods and service contracts also regarding goods with digital elements.⁹⁶

Under the revised Article 3(b)(1a), in case the consumer provides personal data in exchange for the digital content/services, the CRD would cover only such content that is not provided on a tangible medium.⁹⁷ This leaves outside of the CRD's scope IoT goods and other smart devices that are supplied with pre-installed software and other digital content in case they were provided in exchange for data, only. As noted, such devices are principally covered under the SGD and the CRD as 'goods', but the

93 Art. 4(2)(b) (amending Art. 3 CRD to cover data-paying consumers 'except where the personal data provided by the consumer are exclusively processed by the trader for the purpose of supplying the digital content which is not supplied on a tangible medium 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').

94 Art. 2(1)(d), COM(2018) 185 final n. 89

95 Art. 4(10) Omnibus Directive. cf Art. 16(3) ff. DCSD.

96 Art. 4(4)(a)(iv) Omnibus Directive.

97 Art. 4(2)(b) Omnibus Directive.

definition of a ‘sales contract’ to which the SGD applies requires the transfer of ownership and the payment of price, whereas the parallel definition of ‘sales contract’ in the revised CRD does not require payment of price.

The applicability of the various DCSD-SGD-CRD provisions to goods with digital elements – and specifically, to the digital content (and in most cases, to related post-purchase digital services as well) involved in the transaction, as distinguished from the physical good – can be arranged in the following metrics:

IoT Product (‘products with digital elements’)	Ownership transfer for money, pre-in- stalled digital content	Ownership transfer for money, post-installed digital content	Ownership transfer for personal data, pre-installed digital content	Ownership transfer for personal data, post-installed digital content	No transfer of ownership (lending, rental etc.)
DCSD	X (products w/ digital elements excluded)	X (unless the post-installed digital content can be severed from the sales contract, Recitals 21-22 DCSD)	X (products w/ digital elements excluded)	X (unless the post-installed digital content can be severed from the sales contract, Recitals 21-22 DCSD)	X (products w/ digital elements excluded)
SGD	✓ (SGD ‘sales contract’ for goods with digital elements)	✓ (Recial 14 SGD, the digital content can be installed subsequently)	X (data as counter-performance not covered)	X (data as counter-performance not covered)	X (no SGD ‘sales contract’)
Revised CRD	✓ (CRD ‘sales contract’ for the device + some coverage of the digital elements)	✓ (CRD ‘sales contract’ for the device + CRD’s coverage of ‘digital content’ contracts)	X (digital content not covered under amended Art. 3 since provided on a tangible medium)	✓ (digital content covered under amended Art. 3, since not provided on a tangible medium + device covered under ‘sales contract’ since payment of price is not required)	X / ✓ (no CRD ‘sales contract’ for the device, but possibly separate recognition in a contract for digital content/services provided online)

One important upshot is that digital content for consumer IoT devices that are provided in exchange for data are only covered by the CRD, and even then – under the condition that the digital content is not provided on a tangible medium. Typically, this would mean that the content should not be embedded in the device as initially delivered to the consumer but rather be available through another (most likely online) source. Although the definition of ‘goods’ under the SGD and the CRD includes the concept of ‘goods with digital elements’, digital content that is embedded in a physical IoT

product which is not sold for money remains entirely outside this new EU consumer protection scheme. This result is curious.

Interestingly, as shown in the table above, the CRD's new definition of a 'sales contract' – unlike the definition of a 'sales contract' under the SDG – does not require that the ownership of goods is transferred to the consumer for a price.⁹⁸ Therefore, the CRD will potentially cover instances where smart goods are sold (but not lent or rented) in exchange for data, but the digital content that is necessary for the proper functioning of the device must not be provided on a tangible medium. This result is curious as well. The emerging kaleidoscopic landscape is inexplicable and largely unwarranted. Especially remarkable is the inferior status of smart devices with pre-installed digital elements that are provided in exchange for personal data. Probably, excluding from the DCSD/SGD scheme IoT goods that are not sold for money was not required and not even intended.

For consumer IoT devices with digital elements covered by the revised CRD but excluded from the DCD/SGD scheme, (i.e., ownership transfer of devices with post-installed digital content in exchange for personal data), the level of consumer protection is clearly inferior to the DCSD/SGD consumer, including the lack of the detailed conformity requirements regarding the digital elements as laid out in the two aforementioned directives.

An additional implication to the coverage of digital content/services provided in exchange for personal data (with and without connection to an IoT device) under the CRD concerns the trader's duty therein to provide information about the price. Namely, Article 5(c) CRD requires the trader to provide clear and comprehensible information concerning the total price of the goods/services in the case of contract other than a distance or an off-premises contract. A similar information obligation exists regarding distance and off-premises contracts under Article 6(1)(e) CRD. Also Article 8(4) CRD includes a pre-contractual information duty as part of the formal requirements for distance contracts.

The question discussed in the literature is whether such provisions that obligate traders to provide to consumers information about the price change where the payment is not (entirely) in the form of money but (in whole or in part) in the form of data.⁹⁹ The argument is that traders must be transparent about the fact that data, especially such data that are collected via smart devices, is being monetised. Data monetisation opportunities might indeed constitute an essential element of the total price. It has been

⁹⁸ Art. 4(1)(c) Omnibus Directive.

⁹⁹ For analysis and further sources, see Katarzyna Kryla-Cudna, n. 80 at 90-94.

argued on the one hand, that hiding this fact might violate the CRD, and possibly, also consumer protection under Directive 2005/29/EC on unfair commercial practices.¹⁰⁰ On the other hand, the term ‘price’ is being consistently used in the DCSD to indicate a situation of money payment, in contrast to payment via data.¹⁰¹ Assuming a uniform terminology, the CRD provisions that impose price transparency duties possibly do not apply to data-paying consumers. As a partial alternative (or supplement), the data paying-consumer, now in her role as a data subject, should benefit from quite extensive transparency obligations already imposed on the data processor, e.g. under Articles 12-14 GDPR.

4.3.3. Application of the SGD to IoT Goods

Regarding goods with digital elements that do fall under the SGD, the directive’s protection scheme covers the digital components alongside the physical elements.¹⁰² It sets forth specific objective requirements for conformity that are typical to digital content and services, such as the duty to inform the consumer and to supply updates, including security updates that are necessary to keep those goods in conformity.¹⁰³

At the same time, some of the protections embodied in the DCSD are lacking in the SGD, such as the obligations of the trader regarding user-generated content in the case of termination. In addition, the SGD does not include a detailed provision comparable to Article 19 of the DCSD regarding modifications in the digital content or services and the consumer protection safeguards therein (e.g., the requirements that unilateral modifications in the digital components initiated by the trader should be made without additional cost to the consumer).¹⁰⁴ It has been argued that on the matter of remedies for lack of conformity, the SGD is expected to effectively reduce the level of consumer protection in some Member States due to the hierarchical structure of remedies that bars immediate termination by the consumer (with some exceptions).¹⁰⁵ As a consequence of bringing all goods with digital elements under the wings of the SGD, both price and data-paying consumers will suffer from these gaps.

¹⁰⁰ *ibid* at 92-94.

¹⁰¹ Art. 2(7) DCSD (“price” means money or a digital representation of value that is due in exchange for the supply of digital content or a digital service”).

¹⁰² Recitals 14-15 SGD.

¹⁰³ Art. 7(3) SGD.

¹⁰⁴ Axel Metzger, ‘Verträge über digitale Inhalte und digitale Dienstleistungen: Neuer BGB-Vertragstypus oder punktuelle Reform?’, 12 JZ (2019), 577-586, at 578.

¹⁰⁵ Carvalho (2019) n. 76 at 201.

5. Data Portability

5.1. Data Portability Rights under the DCSD

Do data-paying consumers have a ‘right to data portability’ styled in the shape of the GDPR model? Already on the basis of earlier DCD drafts it was observed that the GDPR rights are more vigorous than the slightly comparable arrangement the DCD had proposed.¹⁰⁶ It therefore seemed preferable to subject personal data directly and exclusively to the GDPR regime when such personal data was the means of consumer counter-performance.¹⁰⁷

In the end, the DCSD adopted a clear GDPR-priority rule for personal data concerning the obligations of the trader in case of termination.¹⁰⁸ As indicated above, the DCSD more generally cannot derogate from the rights of the data subject under the GDPR (the ‘no prejudice’ rule), which covers, among other things, the rights to withdraw consent to data collection and processing anytime at will, to demand deletion of data collected based on withdrawn consent, and to require the retrieval and transfer of personal data to another entity.¹⁰⁹

If, for instance, a data-paying consumer withdraws consent for processing of personal data she has provided as counter-performance, Article 20 GDPR governs the data portability rights with respect to that personal data. It is debatable whether this act of withdrawal constitutes also (consequential) termination of the contract by the consumer,¹¹⁰ which would trigger Article 16 DCSD and its more limited portability rights concerning ‘any content other than personal data’ which was ‘provided or created’ by the consumer when using the digital service. Alternatively, the consumer must separately terminate the contract according to the modalities and for grounds recognised under domestic contract law in order to benefit from those rights. Either way, it seems reasonable to allow termination by the trader once consent is withdrawn, which essentially leads to the same result.

¹⁰⁶ Axel Metzger et al. (2018), n. 10 at 103-105.

¹⁰⁷ *ibid* at 105. cf Janal, ‘Data Portability - A Tale of Two Concepts’, 8 (2017) JIPITEC 59, 68 (proposed a consumer right of choice regarding data portability in case of parallel application of the DCD draft and Art. 20 GDPR).

¹⁰⁸ Art. 16(2) DCSD.

¹⁰⁹ See above III.A.2.

¹¹⁰ Vanessa Mak (2016) n. 21 at 9 (discussing the tension between withdrawal of consent and its consequences under data protection law and the contractual consequences of such withdrawal); Schmidt-Kessel et. al., ‘Die Richtlinien-vorschläge der Kommission zu Digitalen Inhalten und Online-Handel - Teil 2’, (2016) n. 5 at 60.

5.2. Evaluation

It is interesting to pause and observe the slight formulation difference between the phrase ‘provided or created when using the digital content or digital service’ in the context of Article 16 DCSD (obligations of the trader in the case of termination regarding user-generated content) as compared to the phrase ‘upload or create with the use of the digital content or digital service’ in the context of the coverage rule of Article 3 as explained in Recital 24 DCSD.

In the former case, the language of the provision indicates an affirmative conduct by the consumer. Such a conclusion is supported by the examples listed in Recital 69, which mentions ‘digital images, video and audio files and content created on mobile devices.’ At the same time, passively provided non-personal data is not explicitly excluded from the scope of the DCSD’s data portability right. The debate described in the context of Article 3 DCD (see above Section 3.2) might assume similar counters also when data portability under Article 16 DCD is at focus, namely, whether consumers who provide non-personal data in a passive manner are entitled to the rights under Article 16(3)-(4) DCSD. The practical implications will be less dramatic, though, as reality scenarios - specifically involving user-generated content, which the directive explicitly targets - are less likely raise many doubts as under Article 3.

As indicated, the newly available data portability rights, such as regarding the traders’ obligation to discontinue use or the right of data retrieval, are limited to termination situations. They are further subject to broad exceptions under Article 16(3) DCSD, as it has been the case under previous versions of the DCD draft. Commentators criticised this situation, but the flaw was not mended in the final DCSD text.¹¹¹

Unlike the position of a data subject under Article 20 GDPR, the DCSD consumer does not have a right to demand data to be transferred directly to a third party.¹¹² In this sense, the DCSD does not contain fully-fledged portability rights in the meaning of the term under the GDPR. Further, as the DCSD generally does not regulate relationships between consumers and third parties (such as a service provider that contracts with the trader to provide certain digital content or perform digital services), the consumer has no retrieval rights against third parties under the DCSD. Instead, Recital 13 DCSD provides generally that regulating liability claims of a consumer against a third party

¹¹¹ See e.g., Axel Metzger (2019) n. 104 at 583.

¹¹² cf. Art. 20(2) GDPR (‘In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible’).

other than a trader that supplies or undertakes to supply the digital content or digital service remains permissive.

6. Conformity and Non-Discrimination

The Commission's draft proposed a structural hierarchy between subjective and objective conformity criteria. Namely, objective conformity criteria should be taken into consideration only to the extent that important aspects of the transaction are not stipulated in the contract in a clear and comprehensive manner (Article 6(2) COM-DCD). That draft suggested to take into consideration - while applying objective conformity criteria - the question whether digital content is supplied in exchange for a price or other counter performance than money.¹¹³

By comparison, the Parliament's draft suggested to introduce more elaborate objective conformity requirements, and importantly, to remove the hierarchy between subjective and objective conformity factors. It also removed the objective conformity criterion taking into account the type of counter-performance (money versus other types of counter-performance, such as data). In the end, the argument for eliminating from the draft, to the extent possible, provisions that discriminated between money-paying consumers and data-paying consumers gained a small victory on this point.

In line with the Parliament's approach, also the argument for putting subjective and objective conformity criteria on equal footing in order to achieve a higher level of consumer protection is now anchored in the DCSD. Both objective and subjective conformity criteria must be considered, and there is no priority to subjective criteria.¹¹⁴ Protection is essentially independent of the type of counter-performance, and Article 8 now stipulates a fairly detailed scheme of objective conformity requirements that importantly includes the obligation to provide updates (including security updates) as well as any accessories and instructions which the consumer may reasonably expect to receive.

In the final analysis, many coverage and discrimination concerns against data-paying consumers have been resolved. DCSD essentially provides similar conformity protection to consumers irrespective of the type of counter-performance, which can be

¹¹³ Art. 6.2(a) COM-DCD.

¹¹⁴ Art. 6 DCSD; Art. 8(1) DCSD (listing objective requirements for conformity '[i]n addition to complying with any subjective requirement for conformity...').

observed also in some other important areas such as the trader duty to supply (Article 5), burden of proof (Article 12), and the rights of consumers in case of modifications of the digital content or service (Article 19).¹¹⁵ Yet, especially in the area of conformity obligations, it is interesting to follow whether these will become in the future a meaningful instrument in the hands of data-paying consumers, or rather, they will predominantly prefer the remedy of termination.

7. Concluding Remarks

Discussions surrounding the DCSD kept EU legislatures and legal experts in the area of consumer protection, contracts and data protection quite busy in recent years. The centre of gravity shifts now to national legislatures. After all, central elements affecting inter alia data-paying consumers, such as of contract formation and validity, remained unharmonised. Particularly on the issue of data as counter-performance, denying or limiting protection on national contract law level might pinch large holes in the harmonisation agenda envisioned by the directive.

A heterogeneous landscape remains in the case of multiparty scenarios. Participants in the chain of transaction alongside direct vendors, such as providers of technical support, security and/or maintenance services, third party suppliers of content or services, storage or data processors of any kind (especially, but not exclusively, in the context of IoT), are not affected by the directive.¹¹⁶ Despite admonitions by legal experts, the DCSD did to introduce more uniformity in this area. Another ‘blind spot’ in the DCSD/SGD structure is its silence on potential legal obligations of data-paying consumers with respect to the data they provide, e.g., duty to provide, commitments regarding data quality, authenticity and accuracy.¹¹⁷ This domain is entirely left to domestic law. Courts, as well, will have to weight in, specifically as regards areas to which the harmonised scheme does apply but leaves room for interpretation. The DCSD indeed has resolved many discussions on key elements raised during the legislative process.

115 For more discussion on the consumer’s rights, see Dirk Staudenmayer, ‘Auf dem Weg zum digitalen Privatrecht – Verträge über digitale Inhalte’, 35 *Neue Juristische Wochenschrift* (2019), 2497-2501, at 2498 ff.

116 See e.g., discussion under Section 2 (level of harmonisation) and section 5.2 (data portability) above. See also, Karin Sein & Gerald Spindler (2019) n. 17 at 275 (‘if the seller has made it sufficiently clear that the consumer has to acquire the “digital elements” from a third party, then the seller himself only remains liable for the “plastic and metal” part of the good.’).

117 cf. Louisa Specht, ‘Datenverwertungsverträge zwischen Datenschutz und Vertragsfreiheit – Eckpfeiler eines neuen Datenschuldrechts’ in Briner and Funk (eds.), *DGRI Jahrbuch 2017* (Dr. Otto Schmidt, 2018); Axel Metzger, ‘Dienst gegen Daten: Ein synallagmatischer Vertrag’, (2016) *Archiv für die civilistische Praxis*, 817-856, at 851 ff.; Philipp Hacker (2019) n. 5 at 180 ff.

It is still early, however, to assess its consolidated effect on consumer protection and commerce at large throughout the EU. One of the main reasons is the open interpretation questions regarding its scope and interplay with other consumer protection instruments as well as with privacy and data protection law.

Not before national legislatures and courts have reached these junctions, will it be possible to make a more precise assessment regarding the implications of the directive for data-paying consumers, and for consumers and traders more generally. Nonetheless, the directive sends out a clear message about the need to provide viable and adequate protection to consumer of digital content and digital services, which cannot turn a blind eye to the very significant and growing consumers category that pays with data instead of money.