Contract Law in the Age of Big Data

please cite to the final version forthcoming in:

2020 16(3) European Review of Contract Law

Author: Cemre Bedir

Abstract:
We are living in a data era where data drives everything we do, including businesses. In data-driven business models, users’ personal data is collected in order to determine consumer preferences and to tailor production and advertising to these preferences. In these new business models, consumers do not pay a price but provide their data, such as IP numbers, locations, and email addresses in order to benefit from digital service or digital content. Content or service providers and users have something in common in these “free” business models which is to benefit from each other. Users benefit from the content or service but they provide their personal data and/or they are exposed to advertisements in return.

This legal framework and trade cannot be made without taking contract law into consideration. Contracts naturally facilitate interactions between companies and users. Their transactions are regulated by contracts in which their agreement on data use and data processing are stipulated. In the last two to three decades, in particular, personal data has started to function similar to the functionality of money in synallagmatic transactions. In this vein, it goes without saying that the role of contract law is becoming more significant and complicated because it does not only concern the economic ordering and economic transactions anymore but also as it is personal data, data protection law comes into play which is considered a part of fundamental rights protection. Data is always collected and processed through a contractual relationship and in this paper, I will argue that there are problems arising from contracts involving data to which contract law applies and that contract law can map these problems and offer insights. The scope of this study will be limited to issues where data is provided as counter-performance and where data is provided in addition to a monetary payment.

1 Cemre Bedir, PhD Researcher at Tilburg University, The Private and Business Law Department, c.bedir@tilburguniversity.edu
1. Data-driven Business Models and Contract Law

We are living in an era where data drives everything we do, including businesses. In data-driven business models, users’ personal data is collected in order to determine the choices of consumers and adjust the production and advertisement of goods and services based on these preferences. Data is at the very heart of these business models. It is generally accepted that there are four main components of the personal data value chain: (1) the collection of data through devices such as mobile phones, smart appliances, sensors, (2) the storage and aggregation of data through browser histories and search service providers, (3) the analysis and distribution of data by data analysts, providers, and financial institutions, (4) and finally, the usage of data by businesses, government and public sector agencies.

In data-driven business models, consumers do not pay a price but provide their data, such as IP addresses, locations, and email addresses in order to benefit from digital service or content. In these business models, data can be necessary for the proper functioning of contracts or data can be generated through the use of digital service or content itself. Service or content providers either sell the data collected to advertisers or generally purchase space to place their advertisements where behavioural targeting plays a significant role as it is more efficient compared to previous simple marketing techniques.

The use of data has created its own economy and this development has grasped the attention of the EU legislator. In 2013, the European Commission

---

2 Viktor Mayer-Schönberger and Kenneth Cukier, *Big Data: A Revolution That Will Transform How We Live, Work, and Think* (Houghton Mifflin 2014) 104; Fabian Hunke & Thiemo Wanbsgasss, ‘Turning Data into Value: Towards an Ideation Tool for Key Activities of Data-Driven Business Models’ (3rd Karlsruhe Service Summit Research Workshop, Karlsruhe, Germany, 21st - 22nd September 2017); Vanessa Mak, ‘Contract and consumer law’ in Vanessa Mak and others (eds), *Research handbook in data science and law* (Edward Elgar Publishing 2018) 17.

3 OECD, ‘Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value’, *OECD Digital Economy Papers*, No. 220, OECD Publishing, 2013, 11-12 <http://dx.doi.org/10.1787/5k486qtxldmq-en> accessed 13 February 2020.; Pia Bublies, ‘Fuel of the Future - Data is giving rise to a new economy’ (*The Economist*, 6 May 2017) <https://www.economist.com/briefing/2017/05/06/data-is-giving-rise-to-a-new-economy> accessed 13 February 2020.
Communication on ‘Towards a thriving data-driven economy’ presented an action plan to introduce the data-driven economy in future applicable regulatory issues, such as the ownership and transfer of data. Following this initiative, in 2015, in the Digital Single Market for Europe, the Commission recognized the lack of legal clarity concerning big data, cloud services, and IoTs, and finally, in 2017, the European Data Economy initiative with the Communication Building a European Data Community was introduced where it was concluded that there is still a need for a legal framework to regulate the economic exploitation and tradability of data. On 20 May 2019, a new directive concerning contracts for the supply of digital content and digital services (DCD) was adopted, which aims at the full harmonization of certain key elements of digital content and digital service contracts concluded between businesses and consumers.

Consumer data is always collected and processed based on a contractual relationship. Because data has economic value, businesses have started to offer digital goods and services to consumers in exchange for data instead of a monetary payment. However, data protection law, in particular, the General Data Protection Regulation (GDPR), places restrictions on the way in which personal data can be used. As a result of this, data-driven technologies often do not fit into existing legal categories and create problems within certain legal regimes. In particular, contract law and data protection law are not fully aligned and the contractual consequences of exercising data protection rights are unclear.

---

6 Commission, ‘Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Towards a thriving data-driven economy’ COM (2014) 0442 final.
7 Judita Dolzan, ‘Trading in Data: A Policy Perspective’ in Lohsse and others (eds), Trading Data in the Digital Economy: Legal Concepts and Tools, (Nomos 2017) 307.
8 Commission, ‘A Digital Single Market Strategy for Europe’, COM (2015) 192 final.
9 Commission, ‘Building a European Data Economy’ COM (2017) 9 final.
10 Dolzan (n 7) 307-308.
11 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.
12 Caroline Cauffman, ‘New EU Rules on Business-to-Consumer and Platform-to-Business Relationships' 2019 26(4) Maastricht Journal of European and Comparative Law 469, 471.
13 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1.
14 Natali Helberger, Frederik Zuiderveen Borgesius, Agustin Reyna, ‘The perfect match? A closer look at the relationship between EU consumer law and data protection law’ (2017) 54(5) Common Market Law Review, 1427; Alberto de Franceschi, ‘European Contract Law and the Digital Single Market: Current Issues and New Perspectives’ in Alberto de Franceschi (eds), European Contract Law and the
This paper focusses on the interplay between contract law and data protection law. Contract law concerns the economic ordering of society and if a new technological development impacts the society, which impacts this economic order as well, then contract law shall be triggered to provide workable frameworks for these new developments. Data protection law, on the other hand, concerns controlling the personal data of individuals by providing them with legal rights regarding the use of their personal data.

Analyses from the contract law perspective are necessary for transactions where personal data is provided in exchange for a good or service because data protection rules are not concerned with the fairness of bargains where consumers provide their personal data in exchange for a service or good. In this study, I will argue that contract law can provide mechanisms which can be tailored to individual situations to regulate contracts involving personal data. To that end, I will map a number of situations in which gaps exist with regard to the connection between contract law and data protection law. The scope of this study will be limited to issues where personal data is provided in exchange for a good or service. I will focus on European contract law but as not all aspects of contract law are regulated in EU law, I will refer to English and German law as the examples of national law of civil and common law systems.

The article is structured as follows. First, contract law and party autonomy will be briefly discussed in terms of personal data. Secondly, the contractual consequences of the use of data as an alternative currency in contracts will be scrutinized. As consent plays a significant role in contracts for the processing of personal data, thirdly, contractual problems with consent will be examined. In particular, the contractual consequences of the withdrawal of consent will be discussed. Finally, remedies and conformity problems regarding contracts that involve data will be investigated. The article wraps up with a brief conclusion. The practice of offering 'free services' in exchange for personal data poses a range of fundamental problems, not only in terms of data protection law but also contract law. The main

---

*Digital Single Market,* (Intersentia 2016) 4; Vanessa Mak, Eric Tjong Tjin Tai, and Anna Berlee, ‘Introduction’ in Vanessa Mak and other (eds), *Research handbook in data science and law,* (Edward Elgar Publishing 2018) 10.

Hein Kötz, *European Contract Law* (2nd edn, Oxford University Press, 2017) 5-6; Mak (n 2) 20.

Carmen Langhanke & Martin Schmidt-Kessel, ‘Consumer Data as Consideration’ (2015) 6 EuCML 219.
finding is that there is a gap between contract law and data protection law and contract law should be taken into consideration when creating an efficient environment for digital transactions between data subjects and good and service providers.

2. Contract Law and Party Autonomy

In the age of big data, data controllers have become more effective in influencing the actions and individual decisions of data subjects which questions the autonomy of data subjects in entering into privacy contracts.\textsuperscript{17} Although the GDPR, which superseded the Data Protection Directive 95/46/EC, seeks to enable data subjects with respect to monitoring and controlling their personal data, in the absence of a minimum level of privacy protection, avoiding privacy contracts is almost impossible for data subjects.\textsuperscript{18} This can be observed in digital content contracts in return for personal data where the principle of \textit{pacta sunt servanda} is not respected due to the fact that the single exchange of performance becomes more important instead of the continuity of performance in contracts where long-term developments play a role.\textsuperscript{19}

In fact, when personal data is used as a means of exchange in contracts, one of the issues to consider is the autonomy of parties. Data subjects often lack bargaining power, which reduces their party autonomy in the contracting phase.\textsuperscript{20} Autonomy is regarded as the fundamental right of individuals to take actions and freely enter into legal relationship regarding their own future through their own actions, which can be seen in private law as the principle of the freedom of contract.\textsuperscript{21} When the data subject’s right to privacy is infringed, this will influence the data subject’s freedom of

\textsuperscript{17} Michiel Rhoen, ‘Beyond consent: improving data protection through consumer protection law’ (2016) 5(1) Internet Policy Review < https://policyreview.info/articles/analysis/beyond-consent-improving-data-protection-through-consumer-protection-law > accessed 13 February 2020.
\textsuperscript{18} ibid.
\textsuperscript{19} De Franceschi (n 14) 9.
\textsuperscript{20} Rhoen (n 17); Also see Joined Cases C-240/98 and C-244/98 Océano Grupo Editorial SA v Rocío Marcial Quintero; Salvat Editores SA v Prades [2000] ECR I-4941.
\textsuperscript{21} Willem van Boom, & Antony Ogus, ‘Introducing, Defining, and Balancing ‘Autonomy v. Paternalism’ (2010) 1 Erasmus Law Review 1 < http://www.erasmuslawreview.nl/tijdschrift/ELR/2010/1/ELR_2210-2671_2010_003_001_001 > accessed 13 February 2020; Yvonne McDermott, ‘Conceptualising the right to data protection in an era of Big Data’ (2017) Big Data & Society 3 < https://doi.org/10.1177/2053951716686994 > accessed 13 February 2020; Stefan Grundmann, 'Information, Party Autonomy and Economic Agents in European Contract Law' (2002) 39(2) Common Market Law Review 269.
choice as to what contracts to conclude and on what terms, which ultimately undermines the autonomy of the party.\textsuperscript{22} Therefore, first of all, from a contractual point of view, the autonomy of data subjects is limited when it comes to drafting digital content or service contracts for data because they have limited bargaining power.

Secondly, the GDPR limits the autonomy of parties because data subject cannot oblige himself to provide personal data to an unlimited extent.\textsuperscript{23} In fact, data protection law limits the autonomy of digital service providers with regard to the use of data. If the digital service supplier prevents the data subject from using the right of withdrawal, the contract will be unenforceable.\textsuperscript{24}

Moreover, how the value of personal data will be determined also affects the autonomy of parties. Putting price tags on each individual’s data may sound like a rather utopian idea\textsuperscript{25} but at the same time, there are cases in which individuals fill out online surveys by sharing their personal data and earn money in return.\textsuperscript{26} Furthermore, personal data tend to have value when they are aggregated. When the data processor combines the data of many individual users, this makes it even much more challenging to allocate a separate price for the individual data in transactions. This also limits the autonomy of the data subject regarding the ‘price of the service’ as it is not possible for the data subject to know the value of his data. Thus, it needs to be examined whether the traditional understanding of party autonomy remains the same and to what extent personal data can be used in exchange for digital goods or

\begin{footnotes}
\textsuperscript{22} Horst Eidenmüller, ‘Party Autonomy, Distributive Justice and the Conclusion of Contracts in the DCFR’ 2009 5(2) European Review of Contract Law 109, 116-117; Joasia Luzak, ‘Is All Fair in War Against Unhealthy and Unsustainable Lifestyles? The Right to Privacy vs. Modern Technology in Consumer Contracts’ in Siliquini-Cinelli L., Hutchison A. (eds) The Constitutional Dimension of Contract Law (Springer 2017) 39, 46.
\textsuperscript{23} Langhanke & Schmidt-Kessel (n 16) 220; Pursuant to Article 7(4) of the GDPR, the data subject has the right to withdraw his consent at any time.
\textsuperscript{24} Langhanke & Schmidt-Kessel (n 16) 221.
\textsuperscript{25} A possible future scenario called ‘Datenmarkt’ can be given an example here as it is the first supermarket where customers pay with their personal Facebook data: <https://www.rlnord.de/nachrichten/datenmarkt.html> accessed 13 February 2020; Also see Datacoup consumers can receive brokering services to sell their data: <http://datacoup.com/> accessed 13 February 2020.
\textsuperscript{26} Natali Helberger, ‘Profiling and Targeting Consumers in the Internet of Things – A New Challenge for Consumer Law’ 14 <https://ssrn.com/abstract=2728717> accessed 13 February 2020; Sam Harrison, ‘Can you make money selling your data?’ \textit{BBC}, (2018) <http://www.bbc.com/capital/story/20180921-can-you-make-money-selling-your-data> accessed 13 February 2020.
\end{footnotes}
services by individuals. Contract law developed frameworks for balancing the rights of businesses and consumers, for instance, and these frameworks could provide guidance in determining the ways in which party autonomy should be handled in relation to contracts involving data.

3. Data as an Alternative Currency in Contracts

In the data economy, there is a tendency to treat data as a tool for paying a price in transactions where digital service or content is provided. It can be stated that currency usually has two functions that it can be ‘cashed out’ for good and services and also it can store value. For English law, for instance, since personal data provided in return for a digital service or digital content has economic value, it can be argued that there is consideration at the stage of contract formation.

Data as a currency will bring certain questions regarding fairness in its wake. Fairness requires that data is not collected in secret, which means data subjects need to have access to their data. It is generally accepted that contract law deals with and enforces the pre-conditions of the fairness of bargains. In the preamble of the EC Directive on Unfair Terms in Consumer Contracts, it is stated that ‘...the main subject matter of the contract and the price/quality ratio may nevertheless be taken into account in assessing the fairness of other term.’ By analogy, it can be argued that personal data can be considered as a price.

In such a case, if the personal data is collected on the ground of the necessity for the performance of the contract, how is it going to be established that only the

---

27 Mak (n 2) 23.
28 Reinhard Zimmermann, ‘Consumer Contract Law and General Contract Law: The German Experience’ (2005) 58(1) Current Legal Problems 415.
29 See page 8 for an example.
30 For the application of the rules of consumer law to free services, see Helberger and others (n 14) 12.
31 Viviane Reding, ‘The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age’ (Innovation Conference Digital, Life, Design, Munich, 22 January 2012) <http://europa.eu/rapid/press-release_SPEECH-12-26_en.htm> accessed 13 February 2020; the Preliminary Opinion of the EDPS (n 4) 10.
32 Also see, William Eggers, Rob Hamill, and Abed Ali, ‘Data as currency’ (Deloitte Review, 2013) <https://www2.deloitte.com/insights/us/en/deloitte-review/issue-13/data-as-the-new-currency.html> accessed 13 February 2020.
33 Currie v Misa [1875] LR 10 Ex 153, 162; Stone v Wythipol [1587] Croke, Elizabeth 126.
34 Rhoen (n 17).
35 Langhanke & Schmidt-Kessel (n 16) 219.
36 93/13/EEC OJ 1993 L 95/29.
necessary data is collected? When websites that are based on user-generated content such as Wikipedia are taken into consideration, although the users provide their personal data in exchange for using the digital content provided on the website, it can be argued that the digital content only needs the data in order to link it with the article’s version history and only for the purposes necessary to make the service function in conformity with the contract.\(^\text{37}\) In cases where data is provided in return for goods or services, as many factors play different roles, it is challenging to attach a single and characteristic purpose to the contract.\(^\text{38}\)

If the necessary data for the performance of the contract is not revealed to the data subject or data that is collected is more than necessary for the performance of the service, then fairness discussions will arise. A disproportionate consideration, which is the collected data that is more than necessary for the performance of the contract, is nothing different from an unfair price and therefore the doctrine of unconscionability in German law can be triggered.\(^\text{39}\) However, by taking discussions regarding the *iustum pretium* (just price) doctrine into account\(^\text{40}\), it can be stated that unless there is an extreme case, the doctrine should not apply and national law should determine the limit of application.\(^\text{41}\)

It is also worth noticing that there are mobile applications called free, such as ‘imo free video calls and chat’\(^\text{42}\) downloaded by more than 500 million people. Even though it is called free, they collect an enormous amount of personal data of users.\(^\text{43}\) Here one might ask whether the simple existence of the word ‘free’ in these kinds of apps creates unfairness, at least in the context of the Unfair Commercial Practices Directive 2005/29/EC where it is stated that

\(^{37}\) Gerald Spindler, ‘Proposal for a Directive on Supply of Digital Content’ in Stefan Grundmann (eds) *European Contract Law and the Digital Single Market*, (Intersentia, 2018) 290.

\(^{38}\) Stefan Grundmann & Philipp Hacker, ‘The Digital Dimension as a Challenge to European Contract Law – The Architecture’ in Stefan Grundmann (ed), *European Contract Law in the Digital Age*, (Intersentia 2018) 44.

\(^{39}\) Florian Rödl, ‘Contractual Freedom, Contractual Justice, and Contract Law (Theory)’, (2013) 76 Law and Contemporary Problems 57, 61, 66.

\(^{40}\) Stefan Grundmann, *Constitutional Values and European Contract Law*, (Kluwer Law International 2008) 258; Ewoud Hondius, ‘Unfair Contract Terms and the Consumer: ECJ Case Law, Foreign Literature, and Their Impact on Dutch Law’ (2016) (24) ¾ European Review of Private Law, 457, 469.

\(^{41}\) Philipp Hacker, ‘Regulating the Economic Impact of Data as Counter-Performance: From the Illegality Doctrine to the Unfair Contract Terms Directive’ in Sebastian Lohsse, Reiner Schulze and Dirk Staudenmayer (eds.), *Data as Counter-Performance: Contract Law 2.0?* (Hart/Nomos 2019) 16 <https://ssrn.com/abstract=3391772> accessed 13 February 2020.

\(^{42}\) <https://play.google.com/store/apps/details?id=hssb.android.free.app&hl=en > accessed 13 February 2020.

\(^{43}\) <https://imo.im/policies/privacy_policy.html > accessed 13 February 2020.

Electronic copy available at: https://ssrn.com/abstract=3631023
‘This provision (No: 20 of the Annex I to the Unfair Commercial Practice Directive) is based on the idea that consumers expect a free claim to be exactly that, meaning they receive something for ‘nothing’, that is, no money or other consideration has to be given in exchange.’

If the statement above is interpreted broadly, the data itself can be thought of as consideration in which the unfair practice can be observed. Although there is a rule of the freedom of contract that allows parties to decide with whom they want to make contracts and on what terms, contract law doctrines still do not permit the strong party to exploit the weaker party ‘in the name of freedom of contract’. It can be argued here that the fair procedure of contract formation is not followed.

Another issue concerns the substance of the data provided by individuals. Although it is argued that commercialization turns consumers’ personal data into consideration which brings new risks and requires new rules, it is still a problem whether inaccurate data can be considered as consideration as well. Even though in civil law, for instance in German law, there are no consideration requirements for contracts, in common law jurisdictions, such as in English law, there needs to be a consideration in order to legally enforce contracts. Consideration is usually defined as ‘something of value in the eye of law’, which must be given by the promisee to make the promise enforceable. If the inaccurate data is actually related to an existing third party, will the condition of the provision of the consideration be met? Apparently, this can lead to problems as there is no standard accepted in the EU when it comes to the quality of data that is provided in return for digital content or service.

---

44 European Commission, Commission Staff Working Document Guidance on the Implementation/Application of Directive 2005/29/EC on Unfair Commercial Practices, 2009, 86 <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016SC0163&from=EN> accessed 13 February 2020; Helberger (n 26) 146-147.
45 Chris Willett, Fairness in Consumer Contracts: The Case of Unfair Terms (Routledge, 2007) 37; Helberger (n 26) 147.
46 Alan Schwartz, ‘Justice and the Law of Contracts: A Case for the Traditional Approach’ (1986) 1122 Faculty Scholarship Series 108 <https://digitalcommons.law.yale.edu/fss_papers/1122> accessed 13 February 2020.
47 Langhanke & Schmidt-Kessel (n 16) 218.
48 Ruth Janal, ‘Fishing for an Agreement: Data Access and the Notion of Contract’ in Sebastian Lohsse (eds) Trading Data in the Digital Economy: Legal Concepts and Tools (Hart, 2017) 275.
49 Guenter Treitel, ‘Consideration’ in Joseph Chitty, Hugh Beale & Andrew S Burrows, Chitty on Contracts, Volume I, General Principles, (31st edn, Sweet & Maxwell, 2012) 1693 293, 294.
50 Mak (n 2) 26.
The question regarding the classification of contracts where personal data is used as a payment method also becomes important because most of the EU members currently hold the view that payment in contracts can only be made with money. The classification matters in terms of the rules applicable to these contracts, in particular, the rights of the data subject regarding termination and conformity with the contract. Rules that are applicable to these new types of contracts for data resemble not only contracts for sale but also contracts for services although do not fully match with them. In the EU, as for contracts for sales and services, many national contract laws accept that the payment can be made with money and the seller pays the agreed price. However, there is no regulation that states whether data can constitute the price. It is likely that all EU member states prefer a sui generis regime and apply specific rules for these new type of contracts for data, which can impede the cross-border supply and harmonization of digital content within the EU. Yet contract law can provide more adequate solutions if ‘payment with money’ can also include ‘payment with data’.

4. Consent

4.1 Contract formation

Excluding English law, as it necessitates consideration for the existence of a valid contract, when the Principles of European Contract Law are taken into account, which are common principles that underline the creation of a contract in many different legal systems in the EU, it can be observed that in order to have a valid contract, two main requirements need to be satisfied: an agreement and the intention of the parties to be legally bound. In order to reach an agreement, there needs to be an offer and acceptance.

According to the GDPR, consent is a legal ground for processing personal data and it does not always correspond to the offer and acceptance procedure in contract law. Indeed, these two concepts, namely, giving consent for processing data within the meaning of Article 6(1)(a) and entering into a contract are not the same but have

51 Mak (n 2) 33; Stefanos Mouzas & Michael Furmston, ‘A proposed taxonomy of contracts’ (2013) Journal of Contract Law 3.
52 Mak (n 2) 33.
53 ibid 34.
54 Hugh Beale (eds), Cases, Materials and Text on Contract Law (Hart, 2010) 44.
different consequences regarding the data subjects' rights and expectations.\textsuperscript{55} Even though consent to process personal data and a contract can separately be a legal ground for processing personal data, they cannot be merged and blurred.\textsuperscript{56} For instance, when a consumer buys an online product, he provides his credit card details and home address to the retailer to make the payment and to fulfil the contract, and the retailer must process the data subject’s credit card and home address for the delivery.\textsuperscript{57} Even though this provision of data can be found in the terms of service, this in itself does not lead to the conclusion of a contract. In these kinds of cases, consent to process data is necessary for the performance of the contract and Article 6(1)(b) of the GDPR is applicable for the processing of the data.

In Article 6 of the GDPR, the lawfulness of processing is regulated and consent is only one of the grounds. Pursuant to Article 6(1)(f) of the GDPR, if the processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party (…), the processing will still be lawful. Here the problem arises when it comes to the definition of legitimate interests. Pursuant to recital 47 of the GDPR, the legitimate interest could exist, for example, where ‘there is a relevant and appropriate relationship between the data subject and the controller in situations such as where the data subject is a client or in the service of the controller.’ From a contractual point of view, it can be argued that the legitimate interest test may not simply be justified on a commercial basis.\textsuperscript{58}

Another problem regarding the use of personal data as counter-performance is the specific purpose for the collection and use of personal data. Contracts through which data collection and processing takes place need to have a specific purpose in the very beginning of the contractual relationship which covers the entire relationship between contractors. In the GDPR it is required that at the time of the collection of the personal data, the specific purposes for which personal data are collected and processed should be explicit, legitimate, and determined.\textsuperscript{59} Technology changes and is

\textsuperscript{55} Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, (adopted on 9 April 2019) 6.
\textsuperscript{56} Article 29 Working Party Guidelines on consent under Regulation 2016/679, (adopted 10 April 2018) 8.
\textsuperscript{57} ibid 9.
\textsuperscript{58} Mak (n 2) 28.
\textsuperscript{59} Recital 39 of the GDPR.
outdated by the minute and new uses for the data collected show up. This makes it cumbersome to limit the use of the data still for presupposed purposes.

Although the consent that parties grant is static, the practice itself calls for, in a way, a sort of dynamic consent which can serve the purpose of the parties in a better way. Similar to the processing of personal data in return for a service, in the field of biobank research, for instance, it is rarely possible to identify all potential future applications of tissue samples, which often requires reliance on broad consent to the identification of appropriate uses of the tissue sample.\textsuperscript{60} Data protection law can benefit from contract law in this sense, in particular, medical treatment contracts. In the field of medical treatment, there is already the concept of dynamic consent that is still being developed, especially in biobanking research, which can provide fine level control over the use of biobank donors’ sample and data.\textsuperscript{61} Therefore, in the long term, developments that arise through the interaction between contract law and data protection should be closely observed.

\subsection*{4.2 Withdrawal of Consent}

Another contractual consequence of consent concerns the right of withdrawal.\textsuperscript{62} If an individual provides his personal data in return for the supply of digital content or service, pursuant to Article 7(3) of the GDPR, he also has the right to withdraw his consent at any time. However, if there are no other grounds for the collecting and processing of the personal data of the individual in question, the processing and collecting will have to stop. Therefore, the data subject may not be prevented from withdrawing his consent as it is his fundamental right, which does not give rights to the digital content or service provider to claim damages on the basis of breach of contract.\textsuperscript{63} The Article 29 Working Party\textsuperscript{64} states that the withdrawal is

\textsuperscript{60} Edgar Whitley, ‘Towards effective, consent based control of personal data’ in Mireille Hildebrandt, Kieron O’Hara, and Michael Waidner (eds) Digital Enlightenment Yearbook (IOS Press, 2013) 165, 174, 175.

\textsuperscript{61} Isabelle Budin-Ljøsne et al. ‘Dynamic Consent: A potential solution to some of the challenges of modern biomedical research’ (2017) 18(4) BMC Med Ethics <https://doi.org/10.1186/s12910-016-0162-9> accessed 13 February 2020.

\textsuperscript{62} Reiner Schulze & Jonathan Morgan, ‘The Right of Withdrawal’ in Gerhard Dannemann / Stefan Vogenhauer (eds) The Common European Sales Law in context: Interactions with English and German law (Oxford 2013) 294, 331.

\textsuperscript{63} Langhanke & Schmidt-Kessel (n 16) 222.

\textsuperscript{64} Article 29 Data Protection Working Party, ‘Opinion 15/2011 on the definition of consent’ WP 187, <http://www.pdpjournals.com/docs/88081.pdf> accessed 13 February 2020.
exercised for the future which means the processing that took place in the past is not affected by the withdrawal but if there are no other legal grounds in order to justify the further use and storage of the data in question, it has to be deleted by the data controller.  

The fact that the data subject is entitled to withdraw his consent seems to be in contradiction with the binding nature of an obligation. However, certain service contracts entail similar rules and can at least offer legal frames for service contracts for data. In medical treatment contracts, for instance, which interact with public law regulation and fundamental rights, patients are allowed to retract their consent in every stage of the medical treatment because it is a fundamental right. Unlike contracts in which personal data is processed, the patient is informed about all stages of the treatment and observes the treatment which makes it easy for the patient to retract. One the other hand, one could argue that it is a general issue of contract law that blanket consent can cover all future purposes. However, in case of any possible violation of the fundamental right of data subjects consent needs to be obtained every time and the processing of personal data by the operator of a search engine ‘cannot be justified by merely the economic interest which the operator of such an engine has in that processing.’ It is argued that when data subjects provide their personal data in return for digital goods or services, they still want to benefit from the application of data protection rules. However, Article 8 of the CFREU and Article 7(3) of the GDPR give the right to the data subject to withdraw his consent at any moment which also creates problems as the contract obliges him to continue supplying the data. For

---

65 Eugenia Politou, Efthimios Alepis, Constantinos Patsakis, ‘Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solution’ (2018) 4(1) Journal of Cybersecurity https://doi.org/10.1093/cybsec/tyy001 accessed 13 February 2020.
66 Langhanke & Schmidt-Kessel (n 16) 221.
67 Stewart C, Aparicio L, Lipworth W, Kerridge I, ‘Public Umbilical Cord Blood Banking and Charitable Trusts’ in: Goold et al (eds), Persons, Parts, and Property: How Should we Regulate Human Tissue in the 21st Century? (Hart, 2014) 53, 59; Mark Sheehan, ‘Can Broad Consent be Informed Consent?’ (2011) 4(3) Public health ethics, 226; Margaret Otlowski, ‘Developing an Appropriate Consent Model for Biobanks: in Defence of “Broad” Consent’ in J. Kaye and M. Stranger (eds.) Principles and Practice in Biobank Governance (Ashgate 2009) 79.
68 Case C-131/12 Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, [2014] EU:C:2014:317; Giuseppe Versaci, ‘Personal Data and Contract Law: Challenges and Concerns about the Economic Exploitation of the Right to Data Protection’, 2018 14(4) European Review of Contract Law 374, 385.
69 Versaci (n 68) 391.
70 Laura Drechsler, ‘Data as Counter-performance: A New Way Forward or a Step Back for the Fundamental Right of Data Protection?’ (2018) Jusletter IT 5 <https://cris.vub.be/files/36462976/IRIS2017_DRAFT_Drechsler_V3.pdf> accessed 13 February 2020; Langhanke & Schmidt-Kessel (n 16) 221.

Electronic copy available at: https://ssrn.com/abstract=3631023
those cases, the parties can always specify in their contract what the consequences of the withdrawal of consent will be and what happens with regard to the future use of data.

In the absence of this specification, it is ambiguous in the GDPR whether the withdrawal of consent means termination in the contractual sense. One of the feasible contractual approaches considers data provided by the data subject as consideration and treats it as a license to use the data for the service or digital content; so, when the data subject withdraws his consent, for instance, then the use of his data and provision of the digital service or content are terminated.\textsuperscript{71} It can be argued that every contract where personal data is provided by data subjects in return for a digital service or digital content can be regarded as a long-term contract due to the fact that the consent requirement does not form the subject matter of the contract but it is rather the duty of the consumer to tolerate the processing thereof.\textsuperscript{72} In this vein, the result of the withdrawal of consent would be the termination of the contract in question. Indeed, Article 7(3) of the GDPR can also be interpreted within the concept of long-term contracts as it produces only effects for the future without affecting the lawfulness of the past processing of data subject’s data.\textsuperscript{73}

Yet this provision still does not make it clear whether partial termination is possible. If this partial termination is possible, it is necessary to discuss what parts of the services or content will not be provided anymore and on what grounds. Indeed, when the right to terminate the contract is used by the data subjects in cases where due to the abuse of personal data, breach or non-performance, for instance, will the agreement continue to operate with regards to the benefits received before the date of the termination? In such a case, is the data subject entitled to be granted compensation for not being able to receive the digital service or content, and if so, how will the compensation be calculated?

Further questions arise where there is a contract that needs to be performed in instalments. Here contracts that involve personal data can be regarded as anomalies.

\textsuperscript{71} Christian Twigg-Flesner, ‘Disruptive technology - disrupted Law? How the digital revolution affects (Contract) Law’ in Alberto De Franceschi (ed), European Contract Law and the Digital Single Market (Intersentia 2016) 19, 41.
\textsuperscript{72} Fryderyk Zoll, ‘Personal Data as Remuneration’ in Reiner Schulze (eds), Contracts for the Supply of Digital Content: Regulatory Challenges and Gaps (Hart 2017) 184.
\textsuperscript{73} ibid 184.
This is so because in such a contract in many jurisdictions the aggrieved party not only has the right to refuse to accept and refuse to render its counter-performance for the defective instalment or part but also it may be entitled to reject any further performance if the non-performance affects the whole contract.\textsuperscript{74} Applying this to the contract where data is provided as counter-performance, it can be argued that the partial termination will also be prospective.

Moreover, it is significant to realize whether the withdrawal of consent \textit{per se} leads to the breach or results in the termination of the contract \textit{ipso jure}. As the GDPR requires a freely given consent to process the personal data of data subjects, if consent becomes part of the contract, it turns out to be a contractual obligation which will face the obstacle of the legality of the contract due to Article 5 of the GDPR. It is argued that as it is provided by the law, the application of the right of withdrawal by the data subject may not be qualified \textit{per se} as the breach of contract and does not provide the other party with a claim for damages.\textsuperscript{75} However, it is also claimed that withdrawal of consent should give a right to the digital content or service provider to terminate the contract unilaterally as it may become burdensome to the latter to provide his service or content.\textsuperscript{76} However, it is ambiguous at what moment the service or content provider can consider the performance of his obligation burdensome for him in the lack of the collection of personal data. Similarly, it needs to be considered whether he still owes any responsibility to the data subject in the first place in cases where the former does not terminate the contract.

In conclusion, there is a need to reconsider the way consent is conceptualized in law, its application, and consequences in the digital world. There is a better and more specific understanding that can encompass, at least, the abovementioned problems. It needs to be kept in mind that many transactions unavoidably take place with some sort of inequality in knowledge and power, which is more frequently observed in the ‘information era’.\textsuperscript{77} The problem comes into existence when the law perceives consent as a simple condition, instead of taking into the details account as to whether consent can be far more nuanced and more workable methods can be

\textsuperscript{74} Ole Lando, Hugh Beale, Martinus Nijhoff, \textit{The Principles of European Contract Law: Part I and II} (Kluwer 200) 411.
\textsuperscript{75} Langhanke & Schmidt-Kessel (n 16) 222.
\textsuperscript{76} ibid 222.
\textsuperscript{77} Daniel Solove, ‘Introduction: Privacy Self-Management and the Consent Dilemma’ (2013) 126 Harvard Law Review 1899, 1901
developed within the existing rules. Yet contract law can identify these problems through general contract law and provide tailored insights through the application of certain general and specific contract law rules, which are analyzed above.

5. Remedies and Conformity

Data subjects provide their personal data to digital content or digital service providers. This so-called ‘freemium model’ becomes the premium model when data subjects pay a price. Contracts for the supply of digital content and services is one of the examples for this where one of the parties supplies the digital content or service to another by himself or through a third party. In cases where the other party’s performance does not conform to the contract, consumers are vested in certain contractual remedies.

The provision of personal data by individuals in contracts brings about questions about conformity. The first question is about the quality of the digital content or digital service that is provided in return for the provision of personal data. In other words, it is a question whether those who provide data instead of paying a price can obtain the same rights when it comes to the conformity with the contract. It is argued that consumers who do not pay a price but provide data instead do not expect the same quality compared to those who pay a price. However, this distinction is becoming blurred, if not completely gone away, when it comes to mobile apps that can be downloaded on Google Pay for €1 or less. Indeed, it is not clear-cut whether the data provided, such as names and email addresses in return for

---

78 ibid 1901.
79 Reiner Schulze, Dirk Staudenmayer, Sebastian Lohsse, ‘Regulatory Challenges and Gaps: An Introduction’ in Reiner Schulze (eds), Contracts for the Supply of Digital Content: Regulatory Challenges and Gaps (Hart 2017) 16.
80 Michael Lehmann, ‘A European Market for Digital Goods’ in Alberto de Franceschi (eds), European Contract Law and the Digital Single Market, (Intersentia 2016) 119.
81 Marco Loos, et al, Analysis of the applicable legal frameworks and suggestions for the contours of a model system of consumer protection in relation to digital content contracts. - Final report: Comparative analysis, law & economics analysis, assessment and development of recommendations for possible future rules on digital content contracts, (2011) Centre for the Study of European Contract Law 180 < http://dare.uva.nl/search?identifier=7d3d806d-8315-4aa6-8fb6-1fc565d2b557 > accessed 13 February 2020.
82 Aurelia Ciacchi & Esther van Schagen, ‘Conformity under the Draft Digital Content Directive’ in Reiner Schulze (eds), Contracts for the Supply of Digital Content: Regulatory Challenges and Gaps (Hart 2017) 119.
the mobile application can replace the actual payment of a price in order to enable the data subject to be subject to the same conformity standards.

With regards to conformity and fitness for the purpose of digital content, the application of traditional contractual law tools, in particular, those that apply to the sale of goods might be considered. Certain jurisdictions, such as New Zealand, simply extend the definition of goods in their national law in order to include digital content yet there might be a risk that rules regarding tangible items might not fit for intangible items.\textsuperscript{83} For instance, unlike property law rules regarding tangibles, the fate of people’s digital assets is ambiguous.

Furthermore, pursuant to Article 14(6) of the DCD, the consumer may terminate the contract only if the lack of conformity with the contract is not minor. The question here is whether there can be more suitable alternatives when the nonconformity is minor and not sufficient to terminate the contract. In circumstances where in addition to the provision of personal data a monetary payment is made, the price reduction on the digital service/content can be a solution. However, if the digital content or service does not work at all, then the price reduction would not be an appropriate remedy. The same is also true for transactions where only personal data is provided as counter-performance because in such a case price reduction would not be possible. One potential solution would be to provide the digital content or digital service for the data subject in question without collecting his data for a period equaling the period during which the digital content or digital service was not in conformity with the contract.

So far my assumptions and examples have been based on those contracts that are made in return for the provision of data instead of payment of a price. However, in practice, there are many digital contracts concluded not only in return for the user’s data but also monetary payment. In these type of mixed contracts, it is not clear-cut what specific digital service and digital content are provided in return for the data provided and a monetary payment. This assessment is also required when it comes to the application of the rules concerning data protection. In fact, in these cases, there is not a clear answer in the DCD for the assessment of to what extent the withdrawal of

\textsuperscript{83} See, Article 2(1) of the Consumer Guarantees Act 1993 (New Zealand): ‘In this Act, unless the context otherwise requires, goods means personal property of every kind (whether tangible or intangible) (…) and includes computer software….’; Twigg-Flesner (n 71) 33.
the data subject’s consent can influence the supplier’s performance in the form of the digital content or digital service. It can be argued that as it is rather impossible to distinguish the part of the digital content or service, the withdrawal of the consent to process the data should conclude the termination of the long-term contract as a whole.

Finally, it needs to be underlined how the service provider can comply with the result of the termination. Pursuant to the DCD, if the consumer provided personal data as a counter-performance instead of a monetary payment, then the trader has to take any necessary actions to refrain from using that data. Yet, the data which is provided by the data subject can easily be copied, pseudonymised, and might be used elsewhere by the processor or collector itself or sub-contractors. If the data has already been passed on to third parties, it may not be possible to have them deleted the data. It is suggested that as the analytical findings are beyond the reach of the individual’s consent, i.e., it is highly likely that the data subject’s data can potentially be used by unknown third parties, the data subject should also be allowed to continue to use the service although the consent has been withdrawn. However, in either case, this termination in practice may not bring about the same conclusion compared to contracts that are made in the non-digital world. In such cases, specific performance, which is a discretionary remedy in English law, can be used as a remedy to receive the data back from those parties that are involved in the collection and processing procedures.

6. Conclusions
As has been demonstrated, there are certain problems arising from contracts involving data. In this study, an analysis has been made by taking two main arguments, namely, whenever data is collected and processed, contract law applies

84 Zoll (n 72) 186.
85 ibid 187.
86 Nikolina Šajn ‘Contracts for the Supply of Digital Content and Digital Services’ (2019) European Parliamentary Research Service 3 <http://www.europarl.europa.eu/RegData/etudes/BRIE/2019/635601/EPRS_BRI(2019)635601_EN.pdf> accessed 13 February 2020.
87 Twigg-Flesner (n 71) 41.
and when problems relating to the GDPR arise from those contracts, contract law can function as a potential solution mechanism to map the issues and provide certain solutions, not only through general contract law but also the tools of specific contracts, such as medical treatment and consumer sales contracts.

Firstly, as has been noted, consent comes with a cost, as there are technical and legal ambiguities when it comes to its scope. The observation of data flow and control of personal data seem to be challenging to follow by the data subject or the controller. When one looks at what takes place in practice, it can be seen that the requirement of consent in the GDPR needs to be more elaborated and cover the data subject’s further consent. Data subjects generally give blanket consent and this blanket consent does not have the details and long-term consequences, which contract law can provide. The GDPR did consider certain parts of consent but again in practice, it leaves open quite a lot of questions, in particular, related to the control of data and further agreements about the processing of data. Consent does not cover the spectrum of what is happening with the personal data at stake and what businesses want to use the data for. In other words, the GDPR is still somewhat ineffective. Contracts involving personal data can benefit from the notion of dynamic consent that is being developed in certain kinds of contracts, such as contracts concerning medical treatment, which eventually can provide data subjects with a better environment in participating in the digital economy.

What also requires further research is whether contracts that involve personal data made in the digital environment of the big data era, - in particular, those in which consumers pay with their personal data - need to be considered the same as traditional contracts where consumers pay a price. This is also closely related to conformity because if the data subject pays with his data, the question is whether he can have the same expectations as he would have in the case of a monetary payment. Besides, the traditional application of contractual concepts of termination to the contracts that are made in return for data raises questions regarding both contractual remedies and consequences.

Furthermore, within the EU, certain legal instruments, such as the GDPR try to create a balance when it comes to the collection of personal data and the fair processing thereof. However, in certain aforementioned points, they fail to do so as
they miss the connection with contract law. Similarly, although the DCD, in many aspects in line with the GDPR, attempts to mitigate the negative consequences of data-driven business models, it also has ambiguities when it comes to contracts for the supply of digital services or digital content that are made through the provision of personal data. Even though the main concepts of contract law, such as offer, acceptance, and consideration requirements, remain the same, new challenges have been observed due to the digital revolution.

Last but certainly not least, it is worth pointing out that data has no borders, and thus, instead of focusing on only one or two national laws to find out how those laws deal with the problems, I believe that the solutions should be searched for in the common tools of contract law in certain jurisdictions to give a clear picture of international practice. In this context, what needs to be examined is the connection and correlation between data protection law, rules that are applicable to digital content and services, and contract law. Contract law needs to be taken into consideration as well regarding achieving the goals that are set out in the GDPR.