https://doi.org/10.22364/jull.13.03

Withdrawal from the Consent to Process Personal Data Provided as Counter-Performance: Contractual Consequences

Dr. iur. **Irene Kull**
Faculty of Law, University of Tartu
Professor of Civil Law
E-mail: *irene.kull@ut.ee*

This article deals with the 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. The Directive says that Member States are free regarding the question of the legal nature of contracts for the supply of digital content or digital services. The Directive must be transposed into national law by 1 July 2021 and the date of entry into force of the transposition rules shall be 1 January 2022. As contracts for the supply of digital content and digital services were not previously regulated, the major challenges for Member States are the contractual meaning of personal data and categorisation of these contracts. The article explores the link between consumer consent to process personal data and the contractual consequences of withdrawal from such consent, specifically the trader's right to terminate the contract. The author supports the need to grant traders the right to terminate the contract in order to provide balance between the rights and obligations of the parties in accordance with the existing national law.

Keywords: digital content and services, contract law, DCDS Directive, personal data as counter-performance.

Contents

Introduction

Technological developments have made it possible to develop different business models based on the supply of digital content and digital services. Business models where digital content or digital services are supplied not for payment but for the personal data of the consumer are used in a considerable part of the market. In order to harmonise the rules governing the supply of digital content and digital services, DCDS Directive (EU) 2019/770 on certain aspects concerning contracts for the supply of digital content and digital services (hereinafter DCDS Directive)[1] was extended to cover 'free contracts'. The processing of personal data must comply with the General Data Protection Regulation (EU) 2016/679 [GDPR][2] and Directive 2002/58/EC[3] on privacy and electronic communications, which, in turn, raises the question of whether compliance with data protection requirements affects the contractual rights and obligations of the parties.

The same set of rules, provided for in the DCDS Directive, apply to both gratuitous and remunerated digital content and services. The purpose of this article is to examine the conditions under which the consumer may withdraw from the consent to process personal data, and the provider in turn use contractual remedies based on processing personal data. In order to answer the question, the article examines the use of personal data as a form of counter-performance in different business models, the consent to process the data under Directive (EU) 2019/770 and GDPR, requirements applying to the submission of personal data and finally the consumer's right to withdraw from the consent and the provider's right to terminate the contract and claim damages under Estonian law. As the DCDS Directive does not regulate the consequences of the consumer's withdrawal from the consent, the consequences of such a withdrawal should remain a matter for national law (Estonian law is analysed as an applicable national legal system).

[1] 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 (Text with EEA relevance). 22/5/2019, OJ L 136, 22/5/2019, pp. 1–27.

[2] 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) (Text with EEA relevance). OJ L 119, 4/5/2016, pp. 1–88.

[3] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). OJ L 201, 31/7/2002, pp. 37–47.

1. Personal Data as a Form of Consideration

1.1. Free Digital Content and Services as a Business Model

According to Article 3 (1) of DCDS Directive (EU) 2019/770, the DCDS Directive applies to remunerated contracts and contracts where the trader supplies or undertakes to supply digital content or a digital service to the consumer, and the consumer provides or undertakes to provide personal data to the trader instead of paying. Sharing digital content or services against personal data, i.e. contracting 'free of charge' is a widely used business model.[4] There are several ways to use personal data provided by consumers, such as transmitting the data to advertising companies or data collection platforms[5], or indirectly generating revenue from advertising aimed at using data sets or providing co-financing services.[6] Social media platforms and software hosting providers also use the supply of services against personal data. For example, almost 30 % of antivirus, search software and cloud services, 77 % of download services (for example, *Spotify*) and 50 % of e-games, e-books and television is transmitted free of charge.[7] The supply of digital content or digital services free of charge may mean savings for the consumer (provision of personal data allows some services to be supplied free of charge, for example, in case of *Spotify*) or the raising of funds (for example, *Handshake*[8]). In freemium business models an initially free service or digital content may become chargeable after a certain period of use, after a certain level is reached (for example, *Dropbox*) or when

[4] Commission staff working document impact assessment accompanying the document Proposals for Directives of the European Parliament and of the Council (1) amending Council Directive 93/13/EEC, 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 and (2) on representative actions for the protection of the collective interests of consumers, and repealing Directive 2009/22/EC. SWD/2018/096 final – 2018/089 (COD).

[5] See more at *Staudenmayer, D*. Verträge über digitalen Inhalt. *New Juristische Wochenschrift*, No. 37, Vol. 69, 2016, p. 2722. See also Handbook on European Data Protection Law. 2018 edition. Luxembourg: Publications Office of the European Union, 2018, p. 143. Available: https://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf [last viewed 18.05.2020]. This does not mean, however, that consent can never be valid in circumstances where not consenting would have some negative consequences. For instance, if refusing a supermarket's customer card only results in not receiving a small reduction in the price of certain goods, consent could be a valid legal basis for processing the personal data of those customers who consented to having such a card. There is no subordination between company and customer and the consequences of not consenting are not serious enough to prevent the data subject's free choice (provided that the price reduction is small enough not to affect their free choice). However, where goods or services can only be obtained if certain personal data are disclosed to the controller or further on to third parties, the data subject's consent to disclose his or her data, which is not necessary for the contract, cannot be considered a free decision and is, therefore, not valid under data protection law. See GDPR, Art. 7(4).

[6] See more at *Lambrecht, A., Goldfarb, A., Bonatti, A., Ghose, A., Goldstein, D., Lewis, R. A., Rao, A., Sahni, N. S., Yao, S*. How Do Firms Make Money Selling Digital Goods Online? *Rotman School of Management Working Paper* No. 2363658, 2018. Available: https://ssrn.com/abstract=2363658 [last viewed 18.05.2020].

[7] Commission staff working document, Annex 11.

[8] *Handshake* is a platform created in 2011 that aims to disclose the monetary value of personal data, offering platform users the opportunity to actively transfer their data with their consent to process it, trade in price and decide to whom to sell the data. Homepage: https://www.joinhandshake.com [last viewed 18.05.2020]. See more about the platform at *Lambrecht, A., Goldfarb, A., Bonatti, A., Ghose, A., Goldstein, D., Lewis, R. A., Rao, A., Sahni, N. S., Yao, S*. How Do Firms Make Money Selling Digital Goods Online? *Rotman School of Management Working Paper*, No. 2363658, 2018.

a better service is desired (for example, *Amazon*, *Duolingo*, *Viber*). Differences in the level of consumer protection based on the nature of the consideration would discriminate between different business models, stimulate the supply of digital content for data and ultimately affect consumers' economic interests, as they would not be protected on an equal footing with consumers who pay a price for digital content or digital services.

1.2. Personal Data as a Commodity?

The extension of the scope of the DCDS Directive to contracts in which the consumer does not pay a price but provides his or her personal data has generally received a positive response.[9] However, the term 'consideration' used in the proposal for the directive was criticised and afterwards deleted from the text of the DCDS Directive. The most influential critic was the European Data Protection Supervisor (EDPS), whose opinion published in 2017 stated, *inter alia*, that "fundamental rights such as the right to the protection of personal data cannot be reduced to simple consumer interests, and personal data cannot be considered as a mere commodity".[10] In addition, the EDPS considered that that the term 'data as a counter-performance' should be avoided and the DCDS Directive shall be applied irrespective of whether a payment is required.[11] The treatment of personal data in return, i.e. the trade in personal data, has been seen as contrary to Article 8 of the Charter of Fundamental Rights of the European Union.[12] On the other hand the GDPR, which is adopted on the basis of Article 8 of the Charter of Fundamental Rights of the European Union and Article 16 of the Treaty on the Functioning of the European Union, is sufficiently appropriate to regulate the processing of personal data[13], and denial of the economic value of personal data is generally considered a disregard of common practice.[14] The legal literature also refers to the case law of the European Court of Justice on the protection of personal data and the protection of economic interests. The ECJ have considered it appropriate to draw an analogy with the author's personal

[9] Statement 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)634 (Digital Content Directive). Research Group 4 ("Data as a means of payment") at the Weizenbaum Institute for the Networked Society. The German Internet Institute, March 2018. Available: https://weizenbaum-institut.de/media/News/Statement/Statement_Weizenbaum-RG4-Statement-on-DCD-March2018.pdf [last viewed 18.05.2020].

[10] European Data Protection Supervisor (EDPS). Summary of the Opinion on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content. 2017/C 200/07. OJ EU C 200/10, p. 10.

[11] Ibid., p. 13.

[12] Charter of Fundamental Rights of the European Union. 2000/C 364/01. OJ EU C 326, 26.10.2012.

[13] In particular, the legal literature refers to Purtova's views. See more in *Purtova, N*. Property Rights in Personal Data: A European Perspective. The Hague: Kluwer Law International, 2011. See also study by Versaci, who analyses Purtova's point of view on the relationship between contract law and the protection of personal data. *Versaci, G.* Personal Data and Contract Law. *European Review of Contract Law*, Vol. 14, No. 4, 2018, pp. 382–383.

[14] *Staudenmayer, D*. Auf dem Weg zum digitalen Privatrecht – Verträge über digitale Inhalte. *Neue Juristische Wochenschrift*, No. 35, 2019, p. 2499; A. Metzger. Verträge über digitale Inhalte und digitale Dienstleistungen: Neuer BGB-Vertragstypus oder punktuelle Reform? *Juristenzeitung*, No. 12, 2019, pp. 577–586.

rights, as EU copyright law does not prohibit contractual agreements on the use of the author's personal rights for economic purposes.[15]

Would the use of personal data as contractual counter-performance be contrary to the basic principles of the GDPR? The answer to this question can be found in Article 13(2)(e) of the GDPR, which provides that the data subject has to be informed whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data. However, it must be borne in mind that the DCDS Directive does not limit or exclude the protection of personal data guaranteed by the GDPR, as the trader must comply with requirements, including processing of personal data and conditions for consent (Articles 5 and 7 GDPR).[16] The provisions of the GDPR must be complied with regardless of whether the provision of personal data has a contractual meaning or whether the supply of digital content or digital services is subject to the provisions of the DCDS Directive.[17]

In conclusion, it should be emphasised that personal data may have an economic value and that the supply of digital content and digital services provided for free as a business model should not affect the protection of consumer rights relating to personal data. According to recital 24 of the preamble to the DCDS Directive, the DCDS Directive should ensure that consumers are entitled to contractual remedies even if the consumer does not pay a price but provides personal data to the trader, recognising at the same time that the protection of personal data is a fundamental right and personal data cannot be considered a commodity. Finally, the DCDS Directive does not regulate the type of contract under which the digital content is supplied or the digital service is provided, i.e. the DCDS Directive should apply only to those parts of the contract that concern the supply of digital content or digital services; other elements of the contract are governed by the relevant rules of national law.[18] The question of whether such contracts constitute a contract of sale, a service, a lease or a *sui generis* contract should be left to the discretion of the Member State. Therefore, the rules of the type of contract governing payment of the price or the general rules if specific rules cannot be applied must apply to the provision or obligation to provide personal data. For example, in the case of a sales contract, the rules governing the payment of remuneration must apply to the provision or obligation to provide personal data.

1.3. The Scope of DCDS Directive

According to Article 2 (8) of the DCDS Directive, personal data means personal data as defined in Article 4(1) of the GDPR, i.e. any information relating to an identified or identifiable natural person (data subject). According to Article 4(1) of the GDPR an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to name, personal

[15] More on the use of the author's personal rights for economic purposes in *Versaci, G.* Personal Data and Contract Law. *European Review of Contract Law*, Vol. 14, No. 4, 2018, pp. 386–388.

[16] Ibid., p. 388.

[17] See also Manko's and Monteleone's comments on the proposal for the Directive in *Manko, R., Monteleone, S.* Briefing: Contracts for the supply of digital content and personal data protection. European Parliamentary Research Service, 2017, p. 6.

[18] See DCDS Directive, recital 33.

identification number, location information, network identifier or one or more physical, physiological, genetic, mental, economic, cultural or social characteristics of that natural person. The DCDS Directive should not apply to situations where personal data is exclusively processed by the trader to supply digital content or a digital service, or to allow 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.[19] Such situations can include, for instance, cases where the registration of the consumer is required by applicable laws for security and identification purposes, where the trader only collects metadata (except where this situation is considered to be a contract under national law) or 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.[20] Member States are free to extend the application of the DCDS Directive to all kinds of supply of digital content and services or provide their own special measures to protect the consumers.

Contracts offering software under a free and open-source licence are also excluded from the scope of the DCDS Directive, provided that the consumer does not pay a price and the trader processes personal data provided by the consumer only to improve the security, compatibility or interoperability of specific software (Art. 3(5)(f) DCDS Directive).

Member States are free to decide whether the requirements for the conclusion, existence and validity of a contract concluded under national law are met (Art. 3(10) DCDS Directive). It is left to the Member States to decide whether the consumer is comprehensively protected against the provision of personal data in the supply of digital content or digital services. As the DCDS Directive does not regulate the distribution of the burden of proof between the parties for the purposes of the processing of personal data[21], it must be shared in accordance with the GDPR. According to Article 5 (2) of the GDPR, the controller must prove the lawfulness of the processing of personal data, i.e. compliance with the requirements set out in Article 5 (1) of the GDPR. This means, *inter alia*, that the controller must demonstrate that personal data are collected for specified, explicit and legitimate purposes and processed in a way compatible with those purposes (Article 5 (1) (b) GDPR) and that there are no other purposes for processing the personal data.

[19] Art. 3(1) of the DCDS Directive.

[20] DCDS Directive, recital 24. See also comments in *Sein, K., Spindler, G.* The New Directive on Contracts for the Supply of Digital Content and Digital Services – Scope of Application and Trader's Obligation to Supply – Part 1. *European Review of Contract Law*, Vol. 15, No. 3, 2019, p. 264.

[21] For example, Spindler considers that although the burden of proof is not regulated in the proposed directive, it should not be imposed on the consumer, for whom it would be unreasonably burdensome. See *Spindler, G.* Contracts for the Supply of Digital Content – Scope of application and basic approach – Proposal of the Commission for a Directive on contracts for the supply of digital content. *European Review of Contract Law*, Vol. 12, No. 3, 2016, p. 193.

2. Supply of Personal Data in the Process of Formation of Contract

2.1. DCDS Directive

Article 3, para. 10 leaves to Member States the freedom to regulate aspects of general contract law, such as rules on the formation, validity and nullity.[22] According to the wording of Article 3(1) of the DCDS Directive, the supply of personal data may take place either at the time or after the conclusion of the contract if the consumer undertakes to provide personal data to the trader. The text of the DCDS Directive does not specify what is meant by the supply of personal data and what requirements must be met if the consumer undertakes only to supply personal data.[23]

The term "has provided" used in Article 3(1) of the DCDS Directive does not refer to the consumer's activity in submission of personal data,[24] unlike the wording used in the proposal for a DCDS Directive[25]. The solution is reasonable, because personal data is not collected only through active submission, but also indirectly, for example through social networks or cookies. Otherwise, widely used open access platforms, free software, etc., would be excluded from the scope of the DCDS Directive.[26] The waiver of the requirement for the consumer to actively communicate data has also been criticised, as in this case each website visit has to be treated as a contractual relationship,[27] ultimately leading to the regulation of the whole internet.[28] In particular, it is questionable

---

[22] For more on the relationship between consent to process personal data and the requirements for concluding a contract, see *Clifford, D., Graef, I., Valcke, P.* Pre-formulated Declarations of Data Subject Consent – Citizen-Consumer Empowerment and the Alignment of Data, Consumer and Competition Law Protections. *German Law Journal*, Vol. 20, No. 5, 2019, p. 707.

[23] *Clifford, D., Graef, I., Valcke, P.* Pre-formulated Declarations of Data Subject Consent – Citizen-Consumer Empowerment and the Alignment of Data, Consumer and Competition Law Protections. *German Law Journal*, Vol. 20, No. 5, 2019, p. 704.

[24] See Sein, K., Spindler, G. The New Directive on Contracts for the Supply of Digital Content and Digital Services – Scope of Application and Trader's Obligation to Supply – Part 1. *European Review of Contract Law*, Vol. 15, No. 3, 2019, p. 263.

[25] The proposal of the Directive, Art. 3 (1): "... and, in exchange, a price is to be paid or the consumer actively provides counter-performance other than money in the form of personal data or any other data." See Proposal for a Directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content. COM/2015/0634 final – 2015/0287 (COD). Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52015PC0634 [last viewed 18.05.2020]. The position published by the European Law Institute has found that the restriction in the proposed directive to apply the Directive only if the consumer provides personal data through an active activity leads to legal uncertainty. See Statement of the European Law Institute on the European Commission's proposed directive on the supply of digital content to consumers. COM (2015) 634 final. European Law Institute, 2016, p. 3. Available: https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Statement_on_DCD.pdf [last viewed 18.05.2020].

[26] See for example *Loos, M., Luzak, J. A.* Wanted: A Bigger Stick. On Unfair Terms in Consumer Contracts with Online Service Providers. *Journal of Consumer Policy*, No. 1, 2016, pp. 63–90; *Langhanke, C., Schmidt-Kessel, M.* Consumer Data as Consideration. *Journal of European Consumer and Market Law*, 2015, Vol. 4, No. 6, pp. 219–223.

[27] *Staudenmayer, D.* Verträge über digitalen Inhalt. *New Juristische Wochenschrift*, No. 37, Vol. 69, 2016, p. 2719.

[28] It would be unjustified to subject any use of the Internet related to data collection to contract law rules, as the protection of consumers' personal data should be sufficiently guaranteed by the GDPR. See *Sein, K., Spindler, G.* The New Directive on Contracts for the Supply of Digital Content and Digital Services – Scope of Application and Trader's Obligation to Supply – Part 1. *European Review of Contract Law*, Vol. 15, No. 3, 2019, pp. 263–264 and *Spindler, G.* Contracts for the Supply of Digital

whether the consumer would need protection guaranteed by the DCDS Directive in each such case, in addition to which submission of personal data by the consumer and the consent to their processing should not automatically constitute a contractual relationship.

2.2. Estonian Law

Under Estonian law, a contract is entered into by an offer being made and accepted or by the mutual exchange of declarations of intent in any other manner if it is sufficiently clear that the parties have reached an agreement (§ 9(1) LOA[29]). In typical contracts for the supply of digital content or services, it will be the service provider who makes an invitation to make offers if not otherwise indicated by the trader, and the offer is made by the consumer.[30] This conclusion is based on the § 16(3) of the LOA: "A proposal which is addressed to a previously unspecified set of persons and is made by sending advertisements, price lists, rates, samples, catalogues or the like or by displaying goods or by offering goods or services to a previously unspecified set of persons on a public computer network is deemed to be an invitation to make offers, unless the person making the proposal clearly indicates that it is an offer." Whether the invitation to make an offer or offers includes a proposal to enter into a contract with personal data as counter-performance has to be clarified by interpretation. Under Estonian law, the interpretation of unilateral declarations of intention is based on the objective standard, which means that a declaration of intention that is directed to the public shall be interpreted according to the understanding of a reasonable person (§ 75(2) GPCCA[31]).

While contracts concluded online are usually standard terms contracts, there might be a need to interpret standard terms as used by the trader. The question arises as to whether the average consumer understands, when concluding a contract, that the trader does not provide digital content or digital services free, but for personal data.[32] The processing of personal data requires the consent of the consumer (Art. 7(2) GDPR), in addition to which according to recital 42 of the GDPR, the data subject must be aware of at least who the controller is and for whom the processing is intended. If the condition that digital content or services will be supplied for personal data as counter-performance is a standard term (§ 35(1) LOA), the objective standard of interpretation applies, for example 'standard term' shall be interpreted according to the meaning that

Content – Scope of application and basic approach – Proposal of the Commission for a Directive on contracts for the supply of digital content. *European Review of Contract Law*, Vol. 12, No. 3, 2016, p. 194.

[29] Law of Obligations Act (LOA), in force from 1/07/2002. Available in English at https://www.riigiteataja.ee/en/eli/508082018001/consolide [last viewed 18/05/2020].

[30] There are no special rules concerning contracts providing digital content or services. See *Kull, I.* § 16. Võlaõigusseadus I. Üldosa (§ 1-207). Kommenteeritud väljaanne [Law of Obligations Act. Annotated edition]. *Varul, P., Kull, I., Kõve, V., Käerdi, M., Sein, K.* (eds.). Tallinn: Juura, 2016.

[31] General Part of the Civil Code Act (GPCCA), in force from 1/07/2002. Available in English: https://www.riigiteataja.ee/en/eli/509012018002/consolide [last viewed 18.05.2020].

[32] For example, a survey conducted in Germany in 2014 found that 67 % of internet users understood that providing personal data is a charge for services provided over the internet. See more in DIVSI Studie. Daten – Wahre und Währung. Hamburg, November 2014, p. 16. Available: https://www.divsi.de/wp-content/uploads/2014/11/DIVSI-Studie-Daten-Ware-Waehrung.pdf [last viewed 18.05.2020]. See also *Metzger, A*. Data as Counter-Performance: What Rights and Duties do Parties Have? *Journal of Intellectual Property, Information Technology and E-Commerce Law*, 8(1), 2017, p. 3.

reasonable persons of the same kind as the other party would give to them in the same circumstances. If there is doubt, standard terms shall be interpreted to the detriment of the party supplying the standard terms (§ 39(1) LOA).

The extension of the scope of the DCDS Directive to free contracts has been considered important precisely because of the possibility of fairness control of the rules for the use of digital content providers and other standard terms.[33] In particular, in the case of consent given for the processing of personal data, the question may arise as to whether the validity of the consent must be verified on the basis of Article 7(2) of the DGPR and § 37(3) of the LOA.[34] Although Article 3(8) of the DCDS Directive requires personal data to be subject to the GDPR, this does not pose any problems under contract law, as § 37(3) of the LOA is similar in substance to Article 7(2) of the GDPR.

Pursuant to § 68(1) of the GPCCA, a declaration of intent may be made in any manner, unless otherwise provided by law. Acceptance of such an offer may be declared explicitly by ticking boxes or implicitly by use of the service or by registering as a user of the platform. Pursuant to § 62^1(3) of the LOA, the trader must always confirm receipt of the order electronically[35] to provide the consumer with certainty that the order has been received. This confirmation may also have contractual meaning as an acceptance of the offer made by the consumer.[36] However, the contractual declaration of intent cannot be equated with consent to process personal data in all cases.[37]

The consent that was given in breach of requirements provided for in the GDPR, should be considered non-binding (Art. 7(2) GDPR). The validity of the contract on the other hand is not affected by the violation of the requirements for the processing of personal data (Art. 8(3) GDPR).

When concluding a contract via a computer network, the undertaking must ensure, in accordance with § 62^2(3) of the LOA, that the consumer clearly confirms by submitting the order that the order means an obligation to pay. If the trader does not comply with this requirement, the consumer is not bound by the contract or the order. If personal data is considered to be a consideration, then § 62^2(3) of the LOA should also extend to the submission or obligation to submit personal data.

---

[33] Although the DCDS Directive only applies to contracts where personal data are used for purposes other than the sole and narrow performance of the contract, this may not significantly affect the level of consumer protection, as the use of personal data for non-restricted purposes is likely to increase. See more in *Spindler, G., Sein, K.* Die endgültige Richtlinie über Verträge über digitale Inhalte und Dienstleistungen. Anwendungsbereich und grundsätzliche Ansätze. *Multimedia und Recht*, No. 7, 2019, p. 419.

[34] According to § 37(3) LOA, standard terms, the contents, wording or presentation of which are so uncommon or unintelligible that the other party cannot, based on the principle of reasonableness, have expected them to be included in the contract, or which the party cannot understand without considerable effort, are not deemed to be part of the contract.

[35] According to § 62^1(8) the provisions of this section do not preclude or restrict any obligations of a trader to provide the other contracting party with any other information prescribed by law.

[36] *Sein, K.* § 62^1. Võlaõigusseadus I. Kommenteeritud väljaanne. P. Varul jt (Law of Obligations Act I. Commented edition). Tallinn: Juura 2017, 4.3.

[37] Will it be an offer or an acceptance? See also *Langhanke, C., Schmidt-Kessel, M.* Consumer Data as Consideration. *Journal of European Consumer and Market Law*, Vol. 4, No. 6, 2015, p. 220.

2.3. Consumer Consent to Processing of Personal Data

According to the wording of Article 7(4) of the GDPR, the trader may refuse to conclude the contract if the consumer refuses to provide the personal data necessary for the performance of the contract. Under Article 3(1) of the DCDS Directive, the trader should have the same right if the consumer refuses to provide the trader with the personal data necessary to comply with legal requirements. When a trader offers digital content or a digital service against personal data, the processing of which brings benefits to the trader, these are inherently reciprocal obligations (*do, ut des*)[38] that should lead to corresponding legal consequences. This means that the trader should also have the right to refuse to enter into a contract if the consumer does not agree to provide the personal data that will be used for purposes other than those necessary to comply with the contract or the law.[39]

In order to process personal data that is not related to the performance of the contract, the consumer shall consent to process personal data. Consent to process consumer personal data must comply with the requirements of the GDPR, regardless of whether the personal data are submitted at the time of the conclusion of the contract, or later. For example, a consumer may provide personal information when registering on a web platform or uploading photos, videos or other material when using a digital service. According to Article 4 (1) of the GDPR, consent must be a voluntary, specific, informed and unambiguous declaration of intent by which the data subject consents to the processing of personal data concerning him or her, either in the form of a statement or by express consent.

Pursuant to Article 7(1) of the GDPR, the controller must be able to prove in the event of a dispute that the data subject has consented to the processing of his or her personal data. The GDPR does not exclude the possibility that consent to process personal data is given as a standard term with the order or order confirmation, but in such a case the consent must be clearly distinguishable, comprehensible and easily accessible in clear and simple language (Art. 7 (2) of the GDPR).[40] This could include ticking the appropriate box on the website, selecting technical equipment for information society services, or any other statement or behaviour that specifically indicates in this context the data subject's consent to the intended processing his or her personal data. Silence, pre-ticked boxes or omissions should therefore not be considered consent.

2.4. Consent to Processing of Personal Data Conditional to Performance of the Contract

As mentioned, the conclusion of a contract does not depend on the submission of personal data or valid consent for processing. However, the question of voluntary consent to process personal data (Art. 7 (4) of the GDPR) could arise if the transfer of digital content or the provision of a digital service is also conditional on the provision of personal data that is not necessary to

[38] For more on this opinion see *Bach, I.* Neue Richtlinien zum Verbrauchsgüterkauf und zu Verbraucherverträgen über digitale Inhalte. *Neue Juristische Wochenschrift*, 72, 2019, 24, p. 1706.

[39] The text of the DCDS Directive refers to equating the provision of personal data with consideration, albeit only in limited functions. On the regulation of the provision of personal data in return for a DCDS Directive, see ibid., p. 1707.

[40] According to recital 32 of the GDPR, consent should be given in the form of a clear statement, such as written confirmation, including by electronic means, or an oral statement.

comply with the contract or law.[41] As explained in recital 43 of the GDPR, consent cannot be considered voluntary if the performance of the contract is conditional on such consent, even though it is not necessary for the performance of the contract. Linking the performance of the contract to consent does not preclude voluntary consent (Art. 7 (4) of the GDPR). The GDPR clarifies that the fact that the performance of a contract, including the provision of a service, is conditional, inter alia, on consent to the processing of non-contractual personal data must be taken into account as far as possible.[42] The burden of proving consent on a voluntary basis lies with the controller in accordance with Article 7 of the GDPR.[43] If the processing of personal data has taken place in breach of the provisions of the GDPR the consumer may use contractual remedies provided for in the DCDS Directive.[44]

In conclusion, it can be considered that consent to process personal data is not linked to the conclusion or validity of the contract, unless the parties themselves have given such meaning to the consent. However, consent to process personal data given in breach of the GDPR is not binding on the consumer. If consent to process personal data is given as a standard term, the regulation of standard terms applies.[45]

3. Contractual Consequences of the Right to Withdraw from Consent to Processing of Personal Data

3.1. Linking the Right to Withdrawal of the Consent to Processing of Data and Contractual Consequences

The processing of personal data for purposes other than ensuring the conformity of the performance of contractual obligations or the performance of requirements arising from law must be based on the consent of the data subject.[46] Since Article 3 (10) of the DCDS Directive requires all personal data to be subject to the provisions of the GDPR in addition to the requirements of the DCDS Directive, the consumer's right to withdraw consent to process

[41] *Malgieri, G., Janeček, V.* Data Extra Commercium. Data as Counter-Performance – Contract Law 2.0? In: *Lohsse, S., Schulze, R., Staudenmayer, D.* (eds.). Hart Publishing/Nomos, 2019.

[42] For more details on the links between personal data voluntariness and contract law, see *Clifford, D., Graef, I., Valcke, P.* Pre-formulated Declarations of Data Subject Consent – Citizen-Consumer Empowerment and the Alignment of Data, Consumer and Competition Law Protections. *German Law Journal*, Vol. 20, No. 5, 2019, pp. 713–717. See also *A. Metzger*. Data as Counter-Performance: What Rights and Duties do Parties Have? *Journal of Intellectual Property, Information Technology and E-Commerce Law*, 8(1), 2017, p. 5.

[43] Recitals 32, 42, 43 in the preamble to the GDPR; Summary of the EDPS Opinion (Ref. 22), p. 16. Consent that does not comply with the requirements of the GDPR is not binding on the consumer (Article 7(2) of DGPR).

[44] *Drechsler, L.* Data as Counter-Performance: A New Way Forward or a Step Back for the Fundamental Right of Data Protection? Datenschutz & LegalTech/Data Protection & LegalTech: Digitale Ausgabe zum Tagungsband des 21. Internationalen Rechtsinformatik Symposions IRIS 2018, pp. 35–43.

[45] About the application of the unfairness assessment of standard terms to the price of data as counter-performance see *Hacker, P.* Regulating the Economic Impact of Data as Counter-Performance: From the Illegality Doctrine to the Unfair Contract Terms Directive. In: *Lohsse, S., Schulze, R., Staudenmayer, D.* (eds.). Data as Counter-Performance – Contract Law 2.0? Hart Publishing/ Nomos, 2019.

[46] GDPR Art 6(1)(a) and (b).

personal data to the extent covered by the GDPR should be guaranteed.[47] However, the right to regulate the consequences of the withdrawal of consent is left to the Member States.[48]

The right of a Member State to regulate the consequences[49] of withdrawal does not answer the question of the relationship between the trader's obligation to supply digital content or digital services and the consumer's right to withdraw consent to process personal data. For example, if a consumer downloads a free mobile application and also consents to process personal data for purposes other than complying with the contract or legal requirements and withdraws consent during the performance of the contract, can the trader terminate the service or limit its scope?

Since the DCDS Directive requires traders to comply with the requirements of the GDPR when providing digital services, it is necessary to ask whether linking the right to withdraw consent to process personal data to the contractual consequences is compatible with the GDPR. To the extent that the consumer's right to withdraw consent has to be guaranteed, agreements which exclude or restrict the consumer's right of withdrawal do not apply and the consumer's exercise of the right of withdrawal cannot be considered non-performance. Pursuant to Article 7(4) of the GDPR, the assessment of the voluntary nature of consent must take into account to a large extent whether the performance of the contract, including the provision of a service, is conditional, *inter alia*, on consent to the processing of personal data. One possibility is to interpret the provisions of the GDPR and the DCDS Directive so that Article 7(4) of the GDPR only regulates voluntary consent and, although the GDPR takes precedence over the DCDS Directive (Art. 3(8)), it does not prohibit consent on supply of personal data as economic equivalent to monetary price.[50] Another possibility is to take the view that personal data is not a consideration that can be claimed and the refusal or withdrawal of consent given by the consumer to process personal data should not lead to the right to use remedies[51]. In this case withdrawal of consent should not lead to contractual consequences.[52]

---

[47] Recital 39 in the preamble to the Directive. Malgieri and Custers have argued, for example, that it would have been legally clearer not to link consent to the processing of personal data to a restriction on active submission, but rather to give consumers the right to know the economic value of their data. It would also have avoided ambiguity as to what the trader's rights would be in the event of withdrawal. For more details, see *Malgieri, G., Janeček, V.* Data Extra Commercium. Data as Counter-Performance – Contract Law 2.0? In: *Lohsse, S., Schulze, R., Staudenmayer, D.* (eds.). Hart Publishing/Nomos, 2019.

[48] GDPR, Art. 3(10).

[49] Ibid.

[50] For more details on the position, see *Metzger, A*. Data as Counter-Performance: What Rights and Duties do Parties Have? *Journal of Intellectual Property, Information Technology and E-Commerce Law*, 8(1), 2017, p. 5.

[51] *Sein, K., Spindler, G.* The New Directive on Contracts for the Supply of Digital Content and Digital Services – Scope of Application and Trader's Obligation to Supply – Part 1. European Review of Contract Law, Vol. 15, No. 3, 2019, p. 265.

[52] The legal literature also contains a proposal to give the trader the right to use legal remedies in case of withdrawal from the consent to the use of personal data, except for the claim for damages; for more details see *Metzger, A., Efroni, Z., Mischau, L., Metzger, J.* Data-Related Aspects of the Digital Content Directive. *Journal of Intellectual Property, Information Technology and E-Commerce Law*, Vol. 9, No. 1, 2018, p. 96. For the same view, see *Langhanke, C., Schmidt-Kessel, M.* Consumer Data as Consideration. *Journal of European Consumer and Market Law*, Vol. 4, No. 6, 2015, p. 222.

The provision or obligation to provide personal data allows the trader to process the submitted personal data for revenue. If the consumer withdraws consent to process personal data, the personal data provided will no longer have the economic value that the trader had taken into account when concluding the contract. Given the purpose of the DCDS Directive and the protection guaranteed by the GDPR, preference should be given to the interpretation that consumer redress in the event of withdrawal of consent to process personal data is not excluded. The trader may stipulate in the terms of the contract that the consumer will be able to use the services to a lesser extent upon receipt of the condition (in case of withdrawal of consent) or will lose the right to part of the originally authorised services.

As the consumer has the right to withdraw consent to process personal data at any time,[53] giving consent is not a counter-obligation that could be required from the consumer. However, the right to withdraw consent to process personal data does not mean that the contract is non-binding, i.e. the consumer has the right to demand that the trader fulfil his or her obligations at least until the withdrawal of consent[54] to process personal data.[55] Given the reciprocal nature of remunerated contracts, the trader's interests should be protected if the consumer uses his or her right to refuse to fulfil obligation with the right to terminate the contract.[56]

3.2. Contractual Consequences – the Trader's Right to Terminate the Contract and Claim Damages Under Estonian Law

Applying Estonian law to a situation in which the consumer withdraws consent to data processing could achieve the following results. Taking a sales contract as an example, the seller has an obligation to deliver the goods and transfer ownership, while the buyer has an obligation to pay the price and take delivery of the goods (§ 208 (1) LOA). If the buyer does not pay the agreed price, the seller (trader) may withdraw from the contract on the bases of § 116 of the LOA, which provides that withdrawal from the contract is permitted only if there is a fundamental non-performance (§ 116 (1) LOA). According to § 116 (2)(2) of the LOA[57], non-performance of such an obligation, the exact performance of which is a precondition for the other party's interest in the contract is fundamental non-performance. If the performance of the trader's obligations or the volume of performance is set dependent on the consent to process personal data, the predictability requirement provided for in § 116 (2)(2)

[53] GDPR, Art. 7(3).

[54] Directive, Art. 3(1).

[55] In principle, Estonian law also recognises binding obligations that can be withdrawn or cannot be demanded. For example, either party to a lease entered into for more than 30 years may cancel after 30 years, observing the term provided by law (§ 318 LOA), and the debtor may not be required to perform an incomplete obligation pursuant to § 4(1) of the LOA.

[56] For possible remedies under German law, see *Metzger, A*. Data as Counter-Performance: What Rights and Duties do Parties Have? *Journal of Intellectual Property, Information Technology and E-Commerce Law*, 8(1), 2017, p. 6. For more details on the two-step control model for the control of unjustified commercial use of personal data, see *Malgieri, G., Janeček, V*. Data Extra Commercium. Data as Counter-Performance – Contract Law 2.0? In: *Lohsse, S., Schulze, R., Staudenmayer, D.* (eds.). Hart Publishing/Nomos, 2019.

[57] Estonian LOA: "§ 116. Termination and cancellation as legal remedies (2) A breach of contract is fundamental if: 2) pursuant to the contract, strict compliance with the obligation which has not been performed is the precondition for the other party's continued interest in the performance of the contract...".

of the LOA is met and the trader has the right to terminate the contract without giving an additional term (§ 116(4) LOA). If it is considered that the consent given to process personal data is not an obligation, the strict observance of which is a prerequisite for maintaining the interest in performance of the contract, the trader must give the consumer an additional term (§ 114(1) LOA). If the consumer fails to use the additional term to cure the non-performance, the trader can terminate the contract. The termination can also be automatic (§ 116(5) LOA).

If the contract for the transfer of digital content or digital services corresponds to the features of a lease contract, the trader as a lessor could cancel the contract in the cases provided for in § 316 of the LOA. However, this provision is not directly applicable to personal data as counter-performance, therefore the cancellation of a contract on the basis of § 196(2) of the LOA, i.e. due to a fundamental non-performance, could be considered. Pursuant to § 196(2) of the LOA, the trader must in such a case give the consumer an additional term for performance, except in the cases provided for in § 116 (2)(2)-(4) of the LOA. The application of § 313 of the LOA could also be considered. Pursuant to § 313 of the LOA, the lessor has the right to cancel the lease contract if there is a good reason for doing so, in the event of which the party wishing to cancel cannot be expected to continue performing the contract. However, the application of this rule depends on how the mutual interests are weighed, i.e., the consumer's interest in the continuation of the contract and the trader's interest in obtaining an economic advantage from the processing of personal data. This is probably more of a legal policy issue that a Member State must address when transposing a DCDS Directive.

In principle, it could also be considered that the trader requires the consumer to compensate damage on the basis of § 115(1) of the LOA instead of performance.[58] This could be done by the trader without setting an additional term, if the withdrawal of consent to the processing of personal data is considered a case provided for in § 116(2) of the LOA and § 115(3) of the LOA. The precondition for a claim for compensation for damage is the liability of the consumer for the breach of the obligation, i.e. the consumer is released from liability if the breach was caused by force majeure (§ 103 LOA). It is difficult to imagine circumstances that could excuse the withdrawal of the consumer's consent. However, there are opinions that withdrawal of consent should not give rise to remedies or should be significantly restricted in the light of the objectives of the GDPR.[59] The legal consequences for the trader of the consumer's withdrawal from content are governed by Article 16 of the DCDS Directive. The consumer shall have the right to request the deletion of his or her personal data and the termination of their further processing upon termination of the contract or withdrawal of consent.[60] If the consumer does not withdraw from the contract, he or she may only request the deletion and termination of personal data that are not necessary for the further performance of the contract, or request the transfer

[58] However, in the case of a claim for damages, the question arises as to the determination of the economic value of personal data; for more details see *Malgieri, G., Custers, B.* Pricing Privacy – The Right to Know the Value of Your Personal Data. *Computer Law & Security Review*, Vol. 34, No. 2, 2018, pp. 289–303.

[59] *Langhanke, C., Schmidt-Kessel, M.* Consumer Data as Consideration. *Journal of European Consumer and Market Law*, Vol. 4, No. 6, 2015, p. 222.

[60] See GDPR, Art. 17.

of personal data to another controller, if technically possible.[61] Granting the trader the right of withdrawal would ensure the balance of the rights and obligations of the contracting parties and would not be in conflict with the basic principles of Estonian private law. When transposing the DCDS Directive, it must therefore be decided whether, in the event of withdrawal of consent to process personal data, it is intended to draft specific rules based on the type of contract concerned or to lay down general rules that will apply to all contracts.[62] General rules would be the most certain way to guarantee the right to consent to process personal data and traders' interest to use the processing of personal data in their business models.

Summary

The purpose of the article was to examine the contractual consequences of withdrawing consent to the processing of personal data in Estonian law taking into account the contractual significance of personal data. Extending the scope of the DCDS Directive to contracts for the supply of digital content or digital services against personal data or the obligation to provide personal data is a pragmatic solution in line with the business models used. There is no doubt that the right to process personal data has an economic value as counter-performance and this has been taken into account in both the GDPR and the DCDS Directive. The choice given to Member States to extend the scope of the contracts covered by the DCDS Directive and to ensure consumer protection provides the necessary flexibility to transpose the DCDS Directive and find appropriate solutions. Given the reciprocal nature of remunerated contracts, the trader's interests should be protected if the consumer uses his or her right to refuse to consent to process personal data and this can be done with the right to terminate the contract. If transposing the DCDS Directive into Estonian law, general rules concerning the contractual consequences of the withdrawal from the consent would be the most certain way to guarantee the interests of consumers and of traders who are interested in using right to process personal data in their business.

Bibliography

1. *Bach, I.* Neue Richtlinien zum Verbrauchsgüterkauf und zu Verbraucherverträgen über digitale Inhalte [New guidelines on consumer goods sales and consumer contracts for digital content]. *Neue Juristische Wochenschrift*, 72, 2019, 24, pp. 1705–1711.
2. *Clifford, D., Graef, I., Valcke, P.* Pre-formulated Declarations of Data Subject Consent – Citizen-Consumer Empowerment and the Alignment of Data, Consumer and Competition Law Protections. *German Law Journal*, Vol. 20, No. 5, 2019, pp. 670–721.
3. *Drechsler, L.* Data as Counter-Performance: A New Way Forward or a Step Back for the Fundamental Right of Data Protection? Datenschutz & LegalTech/Data Protection & LegalTech: Digitale Ausgabe zum Tagungsband des 21. Internationalen Rechtsinformatik Symposions IRIS 2018, pp. 35-43.
4. *Hacker, P.* Regulating the Economic Impact of Data as Counter-Performance: From the Illegality Doctrine to the Unfair Contract Terms Directive. In: Data as Counter-Performance – Contract Law 2.0? *Lohsse, S., Schulze, R., Staudenmayer, D.* (eds.). Hart Publishing/Nomos, 2019.
5. *Lambrecht, A., Goldfarb, A., Bonatti, A., Ghose, A., Goldstein, D., Lewis, R. A., Rao, A., Sahni N. S, Yao, S.* How Do Firms Make Money Selling Digital Goods Online? Rotman School of Management

[61] Directive, recital 68.

[62] *Metzger, A.* Data as Counter-Performance: What Rights and Duties do Parties Have? *Journal of Intellectual Property, Information Technology and E-Commerce Law*, 8(1), 2017, p. 7.

Working Paper No. 2363658, 2018. Available: https://ssrn.com/abstract=2363658 [last viewed 18.05.2020].
6. *Loos, M., Luzak, J. A*. Wanted: A Bigger Stick. On Unfair Terms in Consumer Contracts with Online Service Providers. *Journal of Consumer Policy*, No. 1, 2016, pp. 63–90.
7. *Langhanke, C., Schmidt-Kessel, M.* Consumer Data as Consideration. *Journal of European Consumer and Market Law*, Vol. 4, No. 6, 2015, pp. 219–223.
8. DIVSI Studie. Daten – Wahre und Währung. Hamburg, November 2014, p. 16. Available: https://www.divsi.de/wp-content/uploads/2014/11/DIVSI-Studie-Daten-Ware-Waehrung.pdf [last viewed 18.05.2020].
9. *Kull, I.* § 16. Võlaõigusseadus I. Üldosa (§ 1-207). Kommenteeritud väljaanne [Law of Obligations Act. Commented edition]. *Varul, P., Kull, I., Kõve, V., Käerdi, M., Sein, K.* (eds.). Tallinn: Juura, 2016.
10. *Metzger, A*. Data as Counter-Performance: What Rights and Duties do Parties Have? *Journal of Intellectual Property, Information Technology and E-Commerce Law*, 8(1), 2017, pp. 2–8.
11. *Metzger, A*. Verträge über digitale Inhalte und digitale Dienstleistungen: Neuer BGB-Vertragstypus oder punktuelle Reform? *Juristenzeitung*, No. 12, 2019, pp. 577–586.
12. *Manko, R., Monteleone, S*. Briefing: Contracts for the supply of digital content and personal data protection. European Parliamentary Research Service, 2017.
13. *Sein, K., Spindler, G.* The New Directive on Contracts for the Supply of Digital Content and Digital Services – Scope of Application and Trader's Obligation to Supply – Part 1. European Review of Contract Law, Vol. 15, No. 3, 2019, pp. 257–279.
14. *Spindler, G.* Contracts for the Supply of Digital Content – Scope of application and basic approach – Proposal of the Commission for a Directive on contracts for the supply of digital content. *European Review of Contract Law*, Vol. 12, No. 3, 2016, pp. 183–217.
15. *Staudenmayer, D.* Auf dem Weg zum digitalen Privatrecht – Verträge über digitale Inhalte. Neue Juristische Wochenschrift, 72, 2019, 35, pp. 2497–2501.
16. *Metzger, A., Efroni, Z., Mischau, L., Metzger J.* Data-Related Aspects of the Digital Content Directive. *Journal of Intellectual Property, Information Technology and E-Commerce Law*, 9(1), 2018, pp. 90–109.
17. *Malgieri, G., Janeček, V. Data Extra Commercium*. Data as Counter-Performance – Contract Law 2.0? In: *Lohsse, S., Schulze, R., Staudenmayer, D.* (eds.). Hart Publishing/Nomos, 2019. Available: https://ssrn.com/abstract=3400620 [last viewed 07.10.2019].
18. *Malgieri, G., Custers. B.* Pricing Privacy – The Right to Know the Value of Your Personal Data. *Computer Law & Security Review*, Vol. 34, No. 2, 2018, pp. 289–303.
19. *Purtova, N.* Property Rights in Personal Data: A European Perspective. The Hague: Kluwer Law International, 2011.
20. *Spindler, G., Sein, K.* Die endgültige Richtlinie über Verträge über digitale Inhalte und Dienstleistungen. Anwendungsbereich und grundsätzliche Ansätze. *Multimedia und Recht*, No. 7, 2019, pp. 415–420.
21. *Sein, K.* § 62[1]. Võlaõigusseadus I. Kommenteeritud väljaanne. P. Varul jt [Law of Obligations Act I. Commented edition]. 4.3, Tallinn: Juura, 2017.
22. *Staudenmayer, D*. Verträge über digitalen Inhalt [Digital content contracts]. *New Juristische Wochenschrift*, No. 37, Vol. 69, 2016, pp. 2719–2725.
23. *Versaci, G.* Personal Data and Contract Law. *European Review of Contract Law*, No. 14/4, 2018, pp. 374–392.

Other Sources

1. Charter of Fundamental Rights of the European Union. 2000/C 364/01. OJ EU C 326, 26/10/2012.
2. Commission staff working document impact assessment accompanying the document Proposals for directives of the European Parliament and of the Council (1) amending Council Directive 93/13/EEC, 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 and (2) on representative actions for the protection of the collective interests of consumers, and repealing Directive 2009/22/EC. SWD/2018/096 final – 2018/089 (COD).
3. 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 (Text with EEA relevance). 22/05/2019, OJ L 136, 22/05/2019, pp. 1–27.

4. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). OJ L 201, 31/07/2002, pp. 37–47.
5. Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance). OJ L 119, 4/5/2016, pp. 1–88.
6. European Data Protection Supervisor (EDPS). Summary of the Opinion on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content. 2017/C 200/07. OJ EU C 200/10.
7. Handbook on European data protection law. 2018 edition. Luxembourg: Publications Office of the European Union, 2018, p. 143. Available: https://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf [last viewed 18.05.2020].
8. General Part of the Civil Code Act (GPCCA), in force from 01/07/2002. Available in English at https://www.riigiteataja.ee/en/eli/509012018002/consolide.
9. Law of Obligations Act (LOA), in force from 01/07/2002. Available in English: https://www.riigiteataja.ee/en/eli/508082018001/consolide [last viewed 18.05.2020].
10. 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 final – 2015/0287 (COD).
11. 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.
12. Statement 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)634 (Digital Content Directive). Research Group 4 ("Data as a means of payment") at the Weizenbaum Institute for the Networked Society. The German Internet Institute, March 2018. Available: https://weizenbaum-institut.de/media/News/Statement/Statement_Weizenbaum-RG4-Statement-on-DCD-March2018.pdf [last viewed 18.05.2020].
13. Statement of the European Law Institute on the European Commission's proposed directive on the supply of digital content to consumers. COM (2015) 634 final. European Law Institute 2016, p. 3. Available: https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Statement_on_DCD.pdf [last viewed 18.05.2020].

Abbreviations

Art.	Article
DGDS Directive	Directive (EU) 2019/770
GDPR	General Data Protection Regulation
GPCCA	General Part of Civil Code Act (Estonia)
EDPS	European Data Protection Supervisor
EU	European Union
LOA	Law of Obligations Act (Estonia)
No.	Number
Para.	Paragraph
Vol.	Volume