PERSONAL DATA AS MEANS OF PAYMENT FOR DIGITAL CONTENT OR DIGITAL SERVICES IN THE SLOVENIAN IMPLEMENTATION OF THE DIGITAL CONTENT AND SERVICES DIRECTIVE

*Jernej Renko, LL. M.**

UDK: 342.738:366.5(497.4)
347.451.031:004.7(497.4)
366.5:004.7(497.4)
339.923:061.1(4)EU
DOI: 10.3935/zpfz.74.56.9
Pregledni znanstveni rad
Primljeno: veljača 2024.

One of the most significant features introduced by Directive (EU) 2019/770 (Digital Content and Services Directive, DCSD) is the regulation of contracts in which consumers provide their personal data to traders in exchange for digital content or digital services. The DCSD effectively places consumers who "pay" with their personal data on an equal footing with those who pay a monetary price for digital content or services. However, this results in the overlap of two entirely distinct legal fields: consumer law and data protection law. Should the provision of personal data be active? Should it include non-personal data as well? What happens when a consumer withdraws their consent for the processing of personal data? Since the DCSD leaves many such questions to the discretion of Member States, there is a considerable risk of diverging transpositions of the DCSD into national legal systems. Slovenia's implementation of the DCSD remains relatively conservative and closely follows the Directive's framework. Nevertheless, it addresses the trader's right to terminate the contract if the consumer withdraws consent for the processing of personal data.

Key words: digital content; digital services; personal data; non-personal data; data as counter-performance

* Jernej Renko, mag. iur., LL.M., Teaching and Research Assistant, University of Ljubljana, Faculty of Law, Poljanski nasip 2, 1000 Ljubljana, Slovenia; jernej.renko@pf.uni-lj.si;
ORCID ID: orcid.org/0009-0000-6145-8072

1. INTRODUCTION

Much has been written about the newly adopted 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 (DCSD).[1] One of the most significant features introduced by the DCSD is the regulation of contracts in which consumers provide their personal data to traders in exchange for digital content or digital services. Indeed, the classification of personal data as part of the consumer's contractual performance signals the end of the era of "free" services offered to consumers who provide consent for their personal data to be processed.

The previous paradigm treated consumer consent and the supply of digital content or services as two separate, independent transactions. Social media platforms, search engines, and many other digital content and service providers have not traditionally required monetary payment from consumers in exchange for their offerings. As a result, consumers have generally perceived such content and services as being free of charge. On the other side of the market, providers profit substantially by monetising consumer data, often using it, *inter alia*, for personalised advertising of third-party services.

The DCSD places consumers who "pay" with their personal data on an equal footing with those who pay a monetary price in exchange for digital content or services in terms of contractual rights. While this paradigm shift represents an innovative move towards greater legal predictability for consumers, it also creates an inevitable overlap between two entirely distinct legal areas: consumer law and data protection law. Several questions arise regarding the classification of personal data as a form of payment. Should the provision of personal data be active? Should it also encompass non-personal data? Where should the line between personal and non-personal data be drawn? When considering personal data as part of contractual performance, the relationship between providing personal data and the supply of digital content or services must be examined. Additionally, since consumers retain the right to withdraw consent for the processing of their personal data, the consequences of such withdrawal on the contract between the consumer and the trader must also be addressed.

As the DCSD leaves many of these questions to the discretion of Member States, there is a considerable risk of divergent transpositions of the DCSD into national legal systems. Slovenia's implementation of the DCSD, enacted through the Consumer Protection Act (ZVPot-1)[2], is relatively conservative – the ZVPot-1

[1] Official Journal, L 136, 22 May 2019.

[2] Zakon o varstvu potrošnikov, Uradni list RS, no. 130/2022.

practically copied the DCSD regime word-for-word. Nevertheless, it addresses the trader's right to terminate the contract if the consumer withdraws consent for the processing of personal data.

The primary objective of this paper is to critically assess the newly adopted regime regarding the provision of personal data as a form of payment under the DCSD and to explore the loopholes and risks that may arise from the friction between data protection law and consumer contract law. This is particularly important given that key aspects of DCSD's implementation are left to national legislators. Slovenia's implementation of the DCSD, found in Articles 103–127 ZVPot-1, largely replicates the directive and is included in Chapter III of the ZVPot-1, which governs contracts for the supply of digital content and services to consumers. Since Article 4 DCSD mandates full harmonisation, it is understandable that Slovenian legislators opted for a conservative approach, relying on creative solutions from other Member States, such as Germany. In doing so, Slovenia exercised the option provided in Article 3(10) DCSD, introducing, for instance, a special right for traders to terminate the contract if the consumer withdraws consent for the processing of personal data.

2. SUPREMACY OF GDPR REGARDING PERSONAL DATA IN THE DCSD REGIME

In 2015, the European Commission published the DCSD proposal[3], introducing a significant novelty: the recognition of personal data as a possible form of payment in contracts for the supply of digital content and services. This marked a fundamental shift, bringing consumer contract law into contact with data protection law. However, the unclear relationship between these two areas of law also posed challenges. While some provisions of the DCSD proposal reinforced the protection of consumers' personal data to the same extent as the General Data Protection Regulation (GDPR[4])[5], other controversial aspects, from a data protection perspective, were left unaddressed.[6]

[3] Proposal for a Directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content, COM(2015) 634 final, 9 December 2015.

[4] 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), Official Journal, L 119, 4 May 2016.

[5] See, for example, Article 13(2)(b) and (c) of the DCSD proposal.

[6] For example, the exclusion of the right to data portability as stipulated in Article 20 GDPR.

In the final text of the DCSD, the relationship between data protection law and consumer contract law was clarified through a provision stipulating that the DCSD regime must defer to the GDPR in any matter involving the processing of personal data (Article 3(8) DCSD). Where the DCSD and GDPR conflict, the GDPR prevails in matters of personal data protection. Furthermore, any separate regulation concerning contracts under the DCSD that might impact data protection law was removed from the final text. As a result, the GDPR governs the handling of personal data, while the DCSD applies to non-personal data.[7] Despite this clear delineation, points of tension between these two regimes still arise due to the conceptual differences between these distinct branches of law, as illustrated below.

3. CONTRACTS FOR THE SUPPLY OF DIGITAL CONTENT OR SERVICES WHERE THE CONSUMER PROVIDES PERSONAL DATA AS A MEANS OF PAYMENT

According to Article 3(10) DCSD, Member States retain the freedom to regulate aspects of general contract law, such as the rules on formation, validity, nullity, or effects of contracts, including the consequences of contract termination, insofar as these matters are not regulated by the DCSD. The same applies to the right to damages, which is excluded from the scope of the Directive. Recital 24 of the DCSD clarifies that this also applies in cases where personal data is provided. As a result, the demarcation between contractual and non-contractual relationships is determined by national law.

3.1. Scope of application of DCSD

3.1.1. Data as counter-performance?

The provision of personal data as part of a contract is not regulated by the DCSD as a type of contractual obligation of the consumer but is instead framed as part of the scope of the DCSD.[8] By doing so, the legislator avoided the controversial wording originally contained in the DCSD proposal. In Article 3(1) of the DCSD proposal, the consumer's active provision of a counter-performance, not in monetary form but in the form of personal or other data, was

[7] See, e.g., Articles 16(2) and 16(3) DCSD.

[8] Metzger, A., *Verträge über digitale Inhalte und digitale Dienstleistungen: Neuer BGB-Vertragstypus oder punktuelle Reform?*, JuristenZeitung, *vol.* 74, no. 12, 2019, p. 579.

referenced. This definition of data as counter-performance was criticised by the European Data Protection Supervisor (EDPS), who argued that it encouraged the monetisation of personal data, the protection of which is a fundamental right guaranteed by the Charter of Fundamental Rights of the European Union (EU Charter)[9] and the GDPR framework.[10]

Despite the somewhat exaggerated criticism from the EDPS – who compared the trade in personal data to the trade in human organs – the legislator followed this opinion and removed the term "counter-performance" from the final text of the DCSD.[11] Framing the provision of personal data in exchange for digital content or services as an extension of the scope of the DCSD, rather than as counter-performance, successfully addressed the EDPS's concerns, particularly through the clarification in Recital 24 DCSD that personal data should not be treated as a commodity. However, the deletion of the term "counter-performance" was mostly symbolic. Consumers who pay for digital content or services with money and those who provide their personal data are still granted the same contractual rights.[12]

The prevailing view, particularly among German scholars, is that the consumer's obligation to provide personal data and the trader's obligation to supply digital content or services are akin to a synallagmatic contract (*do ut des*).[13]

---

[9] Official Journal, C 326, 26 October 2012.

[10] European Data Protection Supervisor (EDPS), *Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content*, EDPS, 14 March 2017, pp. 7–8, https://www.edps.europa.eu/data-protection/our-work/publications/opinions/contracts-supply-digital-content_en (1 December 2022).

[11] For a discussion on the rationale behind deleting the term "counter-performance", see also: Metzger, A.; Efroni, Z.; Mischau, L.; Metzger, J., *Data-Related Aspects of the Digital Content Directive*, JIPITEC – Journal of Intellectual Property, Information Technology and E-Commerce Law, *vol.* 8, no. 1, 2017, pp. 93–94, paras. 19–20.

[12] See also Staudenmayer, D., *Auf dem Weg zum digitalen Privatrecht – Verträge über digitale Inhalte*, NJW – Neue Juristische Wochenschrift, *vol.* 72, no. 35, 2019, p. 2498, who argues that while the legislation avoids explicitly stating that personal data is provided as counter-performance, it allows this in practice and cannot prevent it.

[13] Bräutigam, P., *Das Nutzungsverhältnis bei sozialen Netzwerken – Zivilrechtlicher Austausch von IT-Leistung gegen personenbezogene Daten*, MMR – Zeitschrift für IT-Recht und Recht der Digitalisierung, *vol.* 15, no. 10, 2012, p. 640; Metzger, A., *Dienst gegen Daten: Ein synallagmatischer Vertrag*, Archiv für die civilistische Praxis, *vol.* 216, no. 6, 2016, p. 834; Specht, L., *Daten als Gegenleistung – Verlangt die Digitalisierung nach einem neuen Vertragstypus?*, JuristenZeitung, *vol.* 72, no. 15–16, 2017, p. 763; Zoll, F., *Personal Data as Remuneration in the Proposal for a Directive on Supply of Digital Content*, in: Lohsse, S.; Schulze, R.; Staudenmayer, D. (eds.), *Contracts for the Supply of Digital Content: Regulatory Challenges and Gaps – Münster Colloquia on EU Law and the Digital*

In this relationship, the trader supplies the digital content or services with the expectation that the consumer will consent to the processing of their personal data, which can be used by the trader, for example, to profile consumers for personalised advertising purposes.[14]

However, some argue against this view. Hacker, for example, suggests that a conditional (contingent) obligation is a more appropriate model for contracts involving the provision of personal data than a synallagmatic one. In his opinion, the synallagmatic construction is particularly unsuitable when the consumer's obligation to provide personal data is not explicitly agreed upon in the contract for the supply of digital content or services.[15]

According to the proposed conditional (contingent) model, the trader would only be obliged to supply digital content under the condition that the consumer provides personal data. This interpretation, in Hacker's view, would serve the consumer's interest by reinforcing the importance of informational self-determination as a fundamental right. It would also allow the trader to cease supplying digital content or services *ex nunc* if the consumer withdraws consent for data processing, without the need for legal action against the consumer. Major digital service providers, such as Facebook, already *de facto* treat their obligation to supply digital services as conditional on the consumer's provision of personal data, as evidenced by the "cookie wall" phenomenon, where user who refuse to consent to cookies on the provider's website are prevented from accessing the service.[16]

Since the German legislator did not adopt the synallagmatic model, Bauermeister, who analysed the German implementation of the DCSD from the perspective of "payment with personal data", views the consumer's provision of personal data as an atypical condition precedent for the trader's supply of digital content or services. However, he stresses that this should not prevent consumers from asserting the contractual warranty claims provided by the DCSD.[17]

Economy II, Nomos, Baden-Baden, 2017, p. 180; Langhanke, C.; Schmidt-Kessel, M., *Consumer Data as Consideration*, EuCML – Journal of European Consumer and Market Law, *vol.* 4, no. 6, p. 221 *et seq.*

[14] Metzger, *op. cit.* (fn. 8), p. 579.

[15] The fact that traders process consumers' data is often mentioned only descriptively in privacy policies ("We collect your data"); see also Hacker, P., *Daten als Gegenleistung: Rechtsgeschäfte im Spannungsfeld von DS-GVO und allgemeinem Vertragsrecht*, ZfPW – Zeitschrift für die gesamte Privatrechtswissenschaft, *vol.* 5, no. 2, 2019, pp. 168–178.

[16] *Ibid.*, pp. 173–174.

[17] Bauermeister, T., *Die "Bezahlung" mit personenbezogenen Daten bei Verträgen über digitale Produkte*, Archiv für die civilistische Praxis, *vol.* 222, no. 3, 2022, pp. 395–396.

Similarly, the Slovenian legislator did not adopt the synallagmatic model. Article 104 ZVPot-1 states: "the provisions of this Chapter shall also apply to a contract by which a consumer undertakes to provide personal data to a company". As a result, there is nothing preventing the interpretation of the provision of personal data as a condition precedent for the trader's supply of digital content or services.

3.1.2. Provision of personal data

Under the DCSD, only the consumer's personal data can serve as a form of payment, as opposed to non-personal data or "any other data", which was mentioned in the wording of the Article 3(1) of the DCSD proposal but excluded from the final text of the DCSD. No clear explanation was provided for why non-personal data was excluded from the scope of the DCSD. In light of the broadly defined concept of personal data under the GDPR[18], it appears that non-personal data is comparatively negligible to personal data in value, which may suggest that the specific regulation of non-personal data as a means of payment is not as crucial.[19] However, the inclusion of non-personal data would still be desirable.[20]

In practice, distinguishing between personal and non-personal data can sometimes be very challenging. Moreover, with the introduction of new business models, it is possible that an increasing number of cases will involve non-personal data as part of a contract (e.g., a consumer obtains a voucher with credit from a trader in exchange for completing an anonymous survey, which can then be used to purchase a subscription to a music streaming service).[21] In such cases,

---

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

[19] Metzger *et al.*, *op. cit.* (fn. 11), p. 95, para. 21.

[20] This thesis is further supported by the fact that Article 16(3) and (4) DCSD grant certain rights in cases of withdrawal from a contract involving non-personal data ("content other than personal data").

[21] Mischau, L., *Daten als "Gegenleistung" im neuen Verbrauchervertragsrecht*, Zeitschrift für Europäisches Privatrecht, *vol.* 28, no. 2, 2020, p. 341. For a more detailed illustration of this hypothetical example of a contract where a consumer provides non-personal data to a trader in exchange for digital content or services, see: Efroni, Z.,

it would seem unfair to accept the traders' argument that they are not bound by the safeguards under the DCSD because non-personal data is involved.[22]

The Slovenian legislator has followed the approach taken by the DCSD and did not extend the application of the contract regime in the ZVPot-1 to cases where consumers provide non-personal data.

3.1.3. Active and passive provision of personal data

Given that the phrase "active counter-performance", which appeared in Article 3(1) of the DCSD proposal, was omitted in the final text of the DCSD, the question arises whether the scope of the DCSD covers only situations where the consumer actively provides personal data, or whether it also applies to cases where the consumer passively allows their personal data to be collected (e.g., their IP address or data collected through cookies) while using digital content or services.

The problematic nature of limiting the regime to purely active data provision was highlighted by the European Parliament in its report during the legislative process, which concluded that excluding personal data passively provided by the consumer could incentivise traders not to seek the consumer's consent for processing such data.[23] The European Law Institute also called for the removal of the term "actively" from the DCSD proposal, arguing that there is no reason why a consumer whose personal data is obtained, for example, through cookies, should receive less protection than one who actively provides their data.[24]

Despite the omission of the phrase "active counter-performance", it remains unclear whether the DCSD applies to cases where personal data is obtained

---

Gaps and Opportunities: The Rudimentary Protection for "Data-Paying Consumers" under New EU Consumer Protection Law, Common Market Law Review, *vol.* 57, no. 3, 2020, pp. 810–811.

[22] Efroni, *op. cit.* (fn. 21), p. 811.

[23] European Parliament legislative resolution of 26 March 2019 on the proposal for a directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content (COM(2015)0634 — C8-0394/2015 — 2015/0287(COD)), p. 87.

[24] European Law Institute, *Statement of the European Law Institute on the European Commission's Proposed Directive on the Supply of Digital Content to Consumers*, European Law Institute, Vienna, 2016, pp. 15–16 and 40, https://www.europeanlawinstitute.eu/projects-publications/publications/eli-statement-of-the-european-law-institute-on-the-european-commissions-proposed-directive-on-the-supply-of-digital-content-to-consumers/ (1 December 2022).

without the consumer actively providing it. While Recital 24 DCSD focuses on the active provision of data, it also refers to personal data that the "consumer might upload or create with the use of the digital content or digital service". In contrast, Recital 25 excludes from the scope of the DCSD the collection of "metadata, such as information concerning the consumer's device or browsing history", which could fall under the classification of passively collected personal data. Given this, there are indications that the DCSD may cover personal data provided passively by the consumer. However, the resolution of this issue largely depends on whether individual EU Member States extend the application of the DCSD to such situations and define passive provision of personal data as a form of contractual performance (Article 3(10) DCSD and the last sentence of Recital 25 DCSD).

Leaving the regulation of such a key aspect to the discretion of individual Member States introduces the risk of conflicting national regimes concerning contracts for the supply of digital content and services, especially given the cross-border nature of digital commerce. As a result, the European legislator's decision to leave this issue to Member States, while intending to promote full harmonisation of the contractual regime for the supply of digital content and services and consequently to avoid legal fragmentation (Recitals 6–9 DCSD), actually conflicts with the objective of achieving full harmonisation.

In its Explanatory Memorandum to the draft ZVPot-1, the Slovenian legislator explicitly defined both active and passive provision as possible forms of a consumer's provision of personal data to a trader for the purposes of concluding a contract for the supply of digital content or services.[25] This suggests that Slovenian law presumes the existence of a contract under the ZVPot-1 regime, even when the consumer passively allows the trader to collect personal data.[26]

---

[25] See also the Explanatory Memorandum to the draft ZVPot-1: Predlog Zakona o varstvu potrošnikov, EVA: 2015-2130-0005, 12 July 2022, p. 146.

[26] For a more detailed discussion on the effects of recognising the existence of a contract under the DCSD even when the consumer provides personal data passively (e.g., through acceptance of cookies), see Bauermeister, *op. cit.* (fn. 17), pp. 375–379. According to her thesis, consumers may not gain significantly from recognising the existence of a contract when cookies are used, but the threat of damages claims under national general contract law may deter traders from certain business models that rely on collecting personal data through cookies or other tracking technologies.

3.2. Consent to the processing of personal data as the core of the consumer's obligations

When a consumer provides personal data to a trader in exchange for digital content or services, their contractual obligation is not yet fully met. The consumer's personal data is of no value to the trader if the trader is unable to process it, which requires the consumer's consent under Article 6(1)(a) GDPR. Therefore, the consumer's obligation to provide personal data is secondary to the obligation to consent to its processing, especially since traders often obtain personal data during the pre-contractual stages but do not have authorisation to process it at that time.[27]

Regarding the consumer's consent to data processing as both an instrument of data protection law and a form of contractual performance under the DCSD, points of friction exist between the DCSD and GDPR regimes, despite the predominance of the GDPR in regulating contracts under the DCSD (Article 3(8)(2) DCSD). The DCSD does not require the consumer's consent (as data subject) to be valid for its application. If valid consent were required under the GDPR, a trader (as data controller) could benefit from non-compliance with GDPR requirements, potentially depriving the consumer of protections under the DCSD.[28] As a result, even invalid consent may suffice for the application of the DCSD, provided all other requirements are met.

A clear example of a friction between the two regimes is the relationship between the DCSD model of "payment" with personal data and Article 7(4) GDPR, which *inter alia* prohibits "bundling" consent with acceptance of terms or conditions, or "tying" the performance of a contract, including the provision of a service, to a request for consent to process personal data that is not necessary for the performance of that contract. If consent is obtained in such cases, it is presumed not to be freely given (Recital 43 GDPR).[29]

A strict interpretation of the necessity of consent for the performance of a contract would imply that, in all cases where consent to process personal data is not necessary for the supply of digital content or services but is required for, e.g., monetising the consumer's data in line with business models, this consent

---

27 Langhanke; Schmidt-Kessel, *op. cit.* (fn. 13), p. 220.

28 Mischau, *op. cit.* (fn. 21), p. 344; Hacker, *op. cit.* (fn. 15), p. 161.

29 See also European Data Protection Board (EDPB), *Guidelines 05/2020 on consent under Regulation 2016/679*, 4 May 2020, paras. 25–41, https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en (1 December 2022).

would be considered involuntary. However, this conclusion would *de facto* make the contractual arrangement of "payment with personal data", introduced by the DCSD, unworkable.[30] Such a strict interpretation would create an inconsistency between the DCSD and GDPR, effectively preventing contracts in which consumers provide personal data as payment. Therefore, a milder interpretation of Article 7(4) GDPR, one that places less emphasis on the GDPR's recitals, is more widely supported by scholars.[31] This interpretation allows for the mechanism of transferring consumer personal data in exchange for digital content or services to exist.

From a contract law perspective, the relationship between the DCSD and GDPR can be conceptually understood through the analogy of the relationship between a contractual transaction (*Verpflichtungsgeschäft*) and transaction of disposition (*Verfügungsgeschäft*).[32] Given the tensions between these two regimes, Metzger proposes a universal application of the abstraction principle from German civil law to resolve the potential conflicts.[33] The abstraction principle distinguishes between a contractual transaction (*Verpflichtungsgeschäft*) and a transaction of disposition (*Verfügungsgeschäft*) – the former can be valid while the latter may simultaneously be invalid. Following this logic, even if the consumer's consent were invalid due to Article 7(4) GDPR (transaction of disposition), the contract itself would not automatically be invalid under the DCSD (contractual transaction).

[30] Efroni, *op. cit.* (fn. 21), p. 806; Sattler, A., *Personenbezug als Hindernis des Datenhandels*, in: Pertot, T.; Schmidt-Kessel, M.; Padovini, F. (eds.), *Rechte an Daten*, Mohr Siebeck, Tübingen, 2020, p. 76; Riehm, T., *Freie Widerrufbarkeit der Einwilligung und Struktur der Obligation Daten als Gegenleistung?*, in: Pertot, T.; Schmidt-Kessel, M.; Padovini, F. (eds.), *Rechte an Daten*, Mohr Siebeck, Tübingen, 2020, p. 182.

[31] Bauermeister, *op. cit.* (fn. 17), p. 387; Metzger, A., *Data as Counter-Performance: What Rights and Duties do Parties Have?*, JIPITEC – Journal of Intellectual Property, Information Technology and E-Commerce Law, *vol.* 8, no. 1, 2017, section 4.3; Spindler, G., *Verträge über digitale Inhalte – Anwendungsbereich und Ansätze – Vorschlag der EU-Kommission zu einer Richtlinie über Verträge zur Bereitstellung digitaler Inhalte*, MMR – Zeitschrift für IT-Recht und Recht der Digitalisierung, *vol.* 19, no. 3, 2016, p. 150.

[32] Bauermeister, *op. cit.* (fn. 17), p. 383; Metzger, *op. cit.* (fn. 13), p. 839.

[33] Metzger, A., *A Market Model for Personal Data: State of the Play under the New Directive on Digital Content and Digital Services*, in: Lohsee, S.; Schulze, R.; Staudenmayer, D. (eds.), *Data as Counter-Performance – Contract Law 2.0? Münster Colloquia on EU Law and the Digital Economy V*, Nomos, Baden-Baden, 2020, pp. 6–7.

3.2.1. Permissible exceptions to the requirement to obtain consent for a valid contract under DCSD

Article 3(1) DCSD excludes its application in cases where "the personal data provided by the consumer are exclusively processed by the trader for the purpose of supplying the digital content or digital service" or "for allowing the trader to comply with legal requirements to which the trader is subject, and the trader does not process those data for any other purpose". These limitations overlap with situations in which the personal data of an individual are processed under Article 6(1)(b)[34] and (c)[35] GDPR. In these cases, the consumer's personal data is not considered a form of payment or contractual performance under the DCSD.

Among the two exceptions to the scope of the DCSD, it is worth examining the exception for the processing of the personal data to supply digital content or a digital service. In this scenario, the consumer's personal data is processed not based on the consumer's consent under Article 6(1)(a) GDPR, but under Article 6(1)(b) GDPR, according to which the controller may have a legitimate basis for processing personal data even in cases where the processing is necessary for the performance of a contract.

At first glance, this provision seems to give the trader the right to process the consumer's personal data without needing their consent, as long as the processing is necessary for the performance of the contract. The question then arises: can contracts under Article 3(1) DCSD, where the consumer provides personal data as part of the contract, serve as the basis for processing under Article 6(1)(b) GDPR, thereby eliminating the need for consumer consent? The answer is no. The exception of necessity for the performance of the contract under Article 6(1)(b) GDPR is based on a more "technical" requirement for data processing, essential for the performance of the contract, and not on the legal relationship between the parties.[36]

For instance, processing the consumer's email address to deliver digital content or services is necessary for contract performance. However, if the essence of the contract revolves around the consumer providing personal data for the trader's commercial use, this is not a "technical" requirement (e.g., for delivery)

---

[34] "Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract."

[35] "Processing is necessary for compliance with a legal obligation to which the controller is subject."

[36] Zoll, *op. cit.* (fn. 13), p. 182.

but a legal one, requiring the trader to obtain the consumer's consent under Article 6(1)(a) GDPR. To prevent traders from misusing this exception, Graf von Westphalen and Wendehorst suggested introducing a legal presumption that consumer data is processed for commercial purposes if no consent has been obtained.[37] This would require the trader to obtain a second, new consent from the consumer for further processing of their personal data, especially if it is used for economic purposes (e.g., profiling for personalised advertising). Consent to data processing cannot be substituted by a declaration of intent (e.g., an offer or acceptance of an offer), which is required for concluding the contract; instead, it must be provided separately (Article 7(2) GDPR).[38]

Interestingly, the DCSD does not include among its exceptions the processing of personal data by the trader (as the controller) for the legitimate interests pursued by the trader or a third party, which is a legal basis for processing under Article 6(1)(f) GDPR.[39] This implies that a contract for the supply of digital content or services could still be considered valid under the DCSD, even if the trader processes consumer data to pursue legitimate interests, provided the trader balances their interests against those of the consumer. This conclusion is supported by the fact that if the European legislator had intended to limit the application of the DCSD regime solely to cases where the trader processes data based on consumer consent under Article 6(1)(a) GDPR, it would have explicitly stated so in the text of the DCSD.[40] Furthermore, Recital 38 DCSD suggests that processing consumer data provided as payment does not necessarily have to be based on consent for a contract to be valid under the DCSD regime.[41]

---

37 Graf von Westphalen, F.; Wendehorst, C., *Hergabe personenbezogener Daten für digitale Inhalte-Gegenleistung, bereitzustellendes Material oder Zwangsbeitrag zum Datenbinnenmarkt?*, BB – Betriebs Berater, no. 37, 2016, p. 2184.

38 *Ibid*., pp. 2182–2183.

39 Article 6(1)(f) GDPR: "processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child."

40 Mischau, *op. cit.* (fn. 21), p. 343.

41 *Ibid*., p. 343; see also Recital 38 DCSD, which *inter alia* states: "Where processing of personal data is based on consent, *in particular* pursuant to point (a) of Article 6(1) of Regulation (EU) 2016/679, the specific provisions of that Regulation including those concerning the conditions for assessing whether consent is freely given apply." (emphasis made by the author).

3.2.2. Consumer's right to withdraw consent to the processing of personal data – withdrawal from the contract?

Under Article 7(3) GDPR, the data subject has the right to withdraw consent at any time. This is a fundamental right of the individual (Article 8 of the EU Charter) that cannot be waived and is part of the common European *ordre public*.[42] Therefore, any contractual clause that requires the consumer to waive their right to withdraw consent to data processing would be contrary to the public policy of the European Union.[43]

This non-disposable right creates an interesting intersection between consumer contract law and data protection law due to the supremacy of the GDPR in matters of personal data protection. From a contract law perspective, it seems unusual to recognise a contract that, due to the consumer's ability to withdraw consent at any time, inherently includes the possibility of non-performance.

If consumers are allowed to withdraw consent at any time, regardless of their obligation to provide personal data, the effect of withdrawing consent on the contract should be examined. The question arises whether such withdrawal constitutes a breach of contract and whether a national regime allowing traders to claim damages against consumers for non-performance in case of withdrawal is compatible with the DCSD. The regulation of this issue is ultimately a matter for national jurisdictions (see Recital 40 DCSD and Article 3(10) DCSD). Some authors suggest that the consumer's obligation in such contracts could be characterised as generally unenforceable, similar to a natural obligation.[44] Others, however, do not see a conflict between a trader's contractual claim to obtain personal data and the consumer's right to withdraw consent at any time.[45] They base their view on the concept of a gratuitous loan contract (loan for use) under national contract law[46], where the lender can demand the return of the borrowed item at any time.[47]

---

[42] Langhanke; Schmidt-Kessel, *op. cit.* (fn. 13), p. 220.

[43] *Ibid.*, p. 222.

[44] *Ibid.*, p. 221.

[45] Bauermeister, *op. cit.* (fn. 17), p. 384.

[46] See Article 583(3) of the Obligations Code (Obligacijski zakonik, Uradni list RS, no. 97/2007 – OZ-UPB1, with subsequent amendments), which states that the lender may demand the return of the borrowed item at any time if the duration and purpose of the loan are not specified.

[47] Bauermeister, *op. cit.* (fn. 17), p. 384.

The consumer's withdrawal of consent to data processing should not be considered a breach of contract, as it constitutes the exercise of a mandatory right, independent of contractual agreements. Consequently, any claim by the trader for damages resulting from the withdrawal of consent is, in principle, excluded.[48] Allowing a trader to claim damages in such a case could undermine the consumer's absolute right to withdraw consent.[49] The Slovenian legislator acknowledged this by explicitly excluding claims for damages in Article 121(2) ZVPot-1 for traders who experience a consumer's withdrawal of consent.[50]

The DCSD seems to recognise the absolute nature of the consumer's right to withdraw its consent to the processing of personal data. Notably, the DCSD does not permit consumers who pay a monetary price for digital content or services to withdraw from a contract due to minor non-conformities. *A contrario*, this restriction does not apply to contracts where the consumer provides personal data in lieu of payment.[51] Thus, merely withdrawing consent to data processing is sufficient to terminate such a contract, and the trader cannot claim that the withdrawal was based on minor non-conformity of the digital content or service. Recital 39 DCSD confirms that the consumer's right to withdraw under the DCSD is without prejudice to the right to withdraw consent under the GDPR.

By withdrawing consent to data processing, the consumer effectively requests the return of their performance, which could be viewed as exercising their right to withdraw under Article 15 DCSD.[52] To conceptualise the contractual effects of consent withdrawal, as well as of the invalid consent under the GDPR, we can again refer to the abstraction principle, which suggests that withdrawing consent would not affect the validity of the contract under the DCSD.[53] An alternative approach involves introducing a specific right for traders to withdraw from the contract if the consumer withdraws consent to data processing.[54] This solution was adopted by the German legislator in § 327q BGB, which allows traders to withdraw from the contract without notice period if the consumer withdraws

[48] Langhanke; Schmidt-Kessel, *op. cit.* (fn. 13), p. 222.

[49] *Ibid*., p. 221.

[50] See also § 327q(3) BGB.

[51] See Article 14 (6) DCSD and Recital 67 DCSD.

[52] Zoll, *op. cit.* (fn. 13), pp. 187–188.

[53] Metzger, *op. cit.* (fn. 33), pp. 6–7.

[54] *Cf.* Langhanke; Schmidt-Kessel, *op. cit.* (fn. 13), p. 223, who argue that the consumer's withdrawal of consent to data processing does not *ipso iure* constitute withdrawal from the contract but dilutes the contractual basis, which should allow the trader to withdraw from the contract.

consent or objects to further data processing, provided that, weighing the mutual interests, it would not be appropriate to require the trader to continue the contractual relationship until the agreed termination date or the expiry of the statutory or contractually agreed time limit. Fortunately, following the German example, the Slovenian legislator, in Article 121(1) ZVPot-1, allowed traders to withdraw from the contract if the consumer withdraws consent to personal data processing or objects to the continued use of personal data. Upon exercising the trader's right to withdraw from the contract pursuant to Article 121(1) ZVPot-1, the contract is terminated with immediate effect if adhering to a statutory or contractual notice period would impose a disproportionate burden on the trader. This solution is to be applauded as it provides legal certainty for traders and protects their business models, aligning with legal reality.

However, the withdrawal of consent does not prevent the trader from continuing to process personal data on other grounds listed in Article 6(1) GDPR.[55] For example, the trader could justify continued processing on the grounds of pursuing their legitimate interests (as long as the trader's interest outweighs the consumer's interest) under Article 6(1)(f) GDPR. This allows the trader to keep the contract valid to a certain extent under the DCSD.[56] The continued processing of personal data after consent withdrawal seems contrary to the DCSD regime, creating a point of friction between the DCSD and GDPR. Here, the GDPR is more permissive than the DCSD, contrary to the case of Article 7(4) GDPR[57] presented earlier.

This raises the question of whether a Member State's implementation that prohibits a trader from further processing data after consent withdrawal (and possibly requires the trader to return all personal data to the consumer) would violate Article 3(8) DCSD, which establishes the supremacy of the GDPR over the DCSD regarding data protection. Such a regime might be inconsistent with the non-prejudice rule of the DCSD, especially if analysed through a systematic interpretation of the DCSD and a consistent application of Recital 4 DCSD. This suggests that legal certainty and predictability brought by uniform application of the law (here, the GDPR) is not only in the interest of the consumer (as data subject), but also in the interest of traders (as data controllers).[58]

---

[55] Ernst, S., *Die Widerruflichkeit der datenschutzrechtlichen Einwilligung*, ZD – Zeitschrift für Datenschutz, *vol.* 10, no. 8, 2020, p. 384.

[56] For a practical example of a trader continuing to process personal data, based on Article 6(1)(f) GDPR, after the consumer's withdrawal of consent, see Efroni, *op. cit.* (fn. 21), pp. 807–808.

[57] *Ibid.*, p. 807.

[58] *Ibid.*, p. 808.

Nonetheless, scholars advocate for a very restrictive application of Article 6(1)(f) GDPR, particularly for profiling for the purposes of personalised advertising on various networks like Facebook or Google.[59] It is argued that this legal basis is too weak for commercial processing of personal data, since under Article 21 GDPR, consumers can *inter alia* object at any time to processing of personal data based on Article 6(1)(f) GDPR, and traders will rarely be able to demonstrate compelling legitimate grounds for continued processing.[60]

4. CONCLUSION

The DCSD marks the first concrete step towards recognising that the provision of consumers' personal data can constitute a contractual performance. At the level of harmonised European law, this step was indispensable, as it has long been avoided by legislators at both European and national levels. In addition to breaking new ground, the DCSD takes a pragmatic approach by not creating a market for personal data but acknowledging the pre-existing practice of consumers "paying" with their personal data, placing them on an equal footing with consumers who pay in cash in terms of contractual rights.

Although the main purpose of the DCSD is to strengthen the position of the consumer, the European legislator's decision not to regulate in more detail the contractual rights of traders (with the exception of Article 17 DCSD, which governs consumer obligations in the event of withdrawal) raises concerns about legal certainty. It is foreseeable that several challenges will arise in defining the conditions under which traders can require consumers to fulfil their obligations by providing data, all while remaining within the framework of the GDPR. The Slovenian legislator, in its implementation of the DCSD, has not clearly classified the relationship between the consumer's provision of personal data and the trader's obligation to supply the digital content or services.

As previously mentioned, the DCSD allows national legislators the freedom to regulate the formation, validity, nullity, or effects of contracts, including the consequences of the termination or the right to damages. While this approach is understandable given the absence of harmonised and uniform contract law at the EU level, it also opens up a significant number of gaps and the associated risks of divergent legal regimes in the area of the supply of digital content and services. More comprehensive harmonisation in these areas would be necessary to achieve a single European digital market – one of the key objectives of the

[59] Sattler, *op. cit.* (fn. 30), p. 83.

[60] *Ibid.*, p. 71.

DCSD – especially when introducing a completely new mechanism such as "payment with personal data".

The Slovenian legislator has not been particularly innovative in implementing the DCSD, as the text of the Directive has been almost verbatim transposed into the new ZVPot-1. However, the clarification (albeit only in an explanatory memorandum) that a contract exists under Slovenian law even when the consumer passively provides personal data, along with the regulation of the trader's right to withdraw from the contract without a notice period if the consumer withdraws consent to data processing, should be commended.

BIBLIOGRAPHY

Bauermeister, T., *Die "Bezahlung" mit personenbezogenen Daten bei Verträgen über digitale Produkte*, Archiv für die civilistische Praxis, *vol.* 222, no. 3, 2022, pp. 372–400, DOI: 10.1628/acp-2022-0015

Bräutigam, P., *Das Nutzungsverhältnis bei sozialen Netzwerken – Zivilrechtlicher Austausch von IT-Leistung gegen personenbezogene Daten*, MMR – Zeitschrift für IT-Recht und Recht der Digitalisierung, *vol.* 15, no. 10, 2012, pp. 635–641

Efroni, Z., *Gaps and Opportunities: The Rudimentary Protection for "Data-Paying Consumers" under New EU Consumer Protection Law*, Common Market Law Review, *vol.* 57, no. 3, 2020, pp. 799–830, DOI: 10.54648/cola2020693

Ernst, S., *Die Widerruflichkeit der datenschutzrechtlichen Einwilligung*, ZD – Zeitschrift für Datenschutz, *vol.* 10, no. 8, 2020, pp. 383–385

European Data Protection Board (EDPB), *Guidelines 05/2020 on consent under Regulation 2016/679*, 4 May 2020, https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en (1 December 2022)

European Data Protection Supervisor (EDPS), *Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content*, EDPS, 14 March 2017, https://www.edps.europa.eu/data-protection/our-work/publications/opinions/contracts-supply-digital-content_en (1 December 2022)

European Law Institute, *Statement of the European Law Institute on the European Commission's Proposed Directive on the Supply of Digital Content to Consumers*, European Law Institute, Vienna, 2016, https://www.europeanlawinstitute.eu/projects-publications/publications/eli-statement-of-the-european-law-institute-on-the-european-commissions-proposed-directive-on-the-supply-of-digital-content-to-consumers/ (1 December 2022)

Graf von Westphalen, F.; Wendehorst, C., *Hergabe personenbezogener Daten für digitale Inhalte-Gegenleistung, bereitzustellendes Material oder Zwangsbeitrag zum Datenbinnenmarkt?*, BB – Betriebs Berater, no. 37, 2016, pp. 2179–2187

Hacker, P., *Daten als Gegenleistung: Rechtsgeschäfte im Spannungsfeld von DS-GVO und allgemeinem Vertragsrecht*, ZfPW – Zeitschrift für die gesamte Privatrechtswissenschaft, *vol.* 5, no. 2, 2019, pp. 148–197

Langhanke, C.; Schmidt-Kessel, M., *Consumer Data as Consideration*, EuCML – Journal of European Consumer and Market Law, *vol.* 4, no. 6, pp. 218–223

Metzger, A., *Dienst gegen Daten: Ein synallagmatischer Vertrag*, Archiv für die civilistische Praxis, *vol.* 216, no. 6, 2016, pp. 817–865

Metzger, A., *Data as Counter-Performance: What Rights and Duties do Parties Have?*, JIPITEC – Journal of Intellectual Property, Information Technology and E-Commerce Law, *vol.* 8, no. 1, 2017, pp. 2–8

Metzger, A., *Verträge über digitale Inhalte und digitale Dienstleistungen: Neuer BGB-Vertragstypus oder punktuelle Reform?*, JuristenZeitung, *vol.* 74, no. 12, 2019, pp. 577–586, DOI: 10.1628/jz-2019-0178

Metzger, A., *A Market Model for Personal Data: State of the Play under the New Directive on Digital Content and Digital Services*, in: Lohsse, S.; Schulze, R.; Staudenmayer, D. (eds.), *Data as Counter-Performance – Contract Law 2.0? Münster Colloquia on EU Law and the Digital Economy V*, Nomos, Baden-Baden, 2020, pp. 23–46, DOI: 10.5771/9783748908531-23

Metzger, A.; Efroni, Z.; Mischau, L.; Metzger, J., *Data-Related Aspects of the Digital Content Directive*, JIPITEC – Journal of Intellectual Property, Information Technology and E-Commerce Law, *vol.* 8, no. 1, 2017, pp. 90–109

Mischau, L., *Daten als "Gegenleistung" im neuen Verbrauchervertragsrecht*, Zeitschrift für Europäisches Privatrecht, *vol.* 28, no. 2, 2020, pp. 335–365

Riehm, T., *Freie Widerrufbarkeit der Einwilligung und Struktur der Obligation Daten als Gegenleistung?*, in: Pertot, T.; Schmidt-Kessel, M.; Padovini, F. (eds.), *Rechte an Daten*, Mohr Siebeck, Tübingen, 2020, pp. 175–206, DOI: 10.1628/978-3-16-159147-1

Sattler, A., *Personenbezug als Hindernis des Datenhandels*, in: Pertot, T.; Schmidt-Kessel, M.; Padovini, F. (eds.), *Rechte an Daten*, Mohr Siebeck, Tübingen, 2020, pp. 49–86, DOI: 10.1628/978-3-16-159147-1

Specht, L., *Daten als Gegenleistung – Verlangt die Digitalisierung nach einem neuen Vertragstypus?*, JuristenZeitung, *vol.* 72, no. 15–16, 2017, pp. 763–770, DOI: 10.1628/002268817X14998705990087

Spindler, G., *Verträge über digitale Inhalte – Anwendungsbereich und Ansätze – Vorschlag der EU-Kommission zu einer Richtlinie über Verträge zur Bereitstellung digitaler*

Inhalte, MMR – Zeitschrift für IT-Recht und Recht der Digitalisierung, *vol*. 19, no. 3, 2016, pp. 147–153

Staudenmayer, D., *Auf dem Weg zum digitalen Privatrecht – Verträge über digitale Inhalte*, NJW – Neue Juristische Wochenschrift, *vol*. 72, no. 35, 2019, pp. 2497–2501

Zoll, F., *Personal Data as Remuneration in the Proposal for a Directive on Supply of Digital Content*, in: Schulze, R.; Staudenmayer, D.; Lohsse, S. (eds.), *Contracts for the Supply of Digital Content: Regulatory Challenges and Gaps – Münster Colloquia on EU Law and the Digital Economy II*, Nomos, Baden-Baden, 2017, pp. 179–188, DOI: 10.5771/9783845281391-179

Sažetak

Jernej Renko*

OSOBNI PODATCI KAO SREDSTVO PLAĆANJA ZA DIGITALNI SADRŽAJ ILI DIGITALNE USLUGE U SLOVENSKOJ IMPLEMENTACIJI DIREKTIVE O DIGITALNOM SADRŽAJU I USLUGAMA

Jedna od najznačajnijih novina koju donosi Direktiva (EU) 2019/770 (Direktiva o digitalnom sadržaju i uslugama, DCSD) jest uređenje ugovora u kojima potrošači pružaju svoje osobne podatke trgovcima u zamjenu za digitalni sadržaj ili digitalne usluge. DCSD učinkovito stavlja potrošače koji "plaćaju" svojim osobnim podatcima u ravnopravan položaj s onima koji plaćaju novčanu cijenu za digitalni sadržaj ili usluge. Međutim, to dovodi do preklapanja dvaju potpuno različitih pravnih područja: potrošačkog prava i prava zaštite podataka. Treba li pružanje osobnih podataka biti aktivno? Treba li obuhvatiti i neosobne podatke? Što se događa kada potrošač povuče svoj pristanak za obradbu osobnih podataka? Budući da DCSD mnoge takve aspekte prepušta diskreciji država članica, postoji znatan rizik različitog transponiranja DCSD-a u nacionalne pravne poretke. Slovenska implementacija DCSD-a relativno je konzervativna i usko slijedi okvir Direktive. Ipak, predvidjela je pravo trgovca raskinuti ugovor ako potrošač povuče pristanak za obradbu osobnih podataka.

Ključne riječi: digitalni sadržaj, digitalne usluge, osobni podatci, neosobni podatci, podatci kao protučinidba

* Jernej Renko, mag. iur., LL.M., asistent Pravnog fakulteta Sveučilišta u Ljubljani, Poljanski nasip 2, 1000 Ljubljana, Slovenija; jernej.renko@pf.uni-lj.si; ORCID ID: orcid.org/0009-0000-6145-8072