



TEREZA PERTOT

Ricercatrice a tempo determinato – Università degli Studi di Trieste

PERSONAL DATA SUPPLYING: THE ISSUE OF BUNDLED CONSENT

SOMMARIO: 1. General introduction. – 2. Personal data as contractual (counter-)performance: still an open question? – 3. Personal data supplying and privacy consent: the relationship between (consumer) contract and data protection law. – 4. The meaning of Article 7(4) GDPR and the legitimacy of a bundled consent. – 4.1. A) The strict ban on tying. – 4.2. B) The possibility to bypass the bundling prohibition by use of legal basis for processing other than consent. – 4.3. C) Conditionality as one of several circumstances to be considered by assessing the freedom of consent. – 5. Adhesion to the opinion sub C). – 6. The (ongoing) evolution of CJEU case-law. – 7. Final remarks.

1. – New technologies enable enterprises to collect large amounts of data. Collected datasets may consist of personal or of non-personal data, depending on whether the information relates to an identified or identifiable natural person or not [cf. Article 4(1) of the GDPR and Article 3(1) of the Regulation (EU) 2018/1807].¹ Delineating the boundary between personal and non-personal data could be difficult in practice, as datasets are often mixed and as even data not related to an individual and/or which has been rendered anonymous may become personal by matching it with data from other sources.² Keeping this in mind, the paper will, however, only focus on the processing involving personal data.³ The latter, in fact, presents some specific problems, which arise where data is collected and used for commercial purposes, as increasingly happens nowadays.

There are many different ways in which personal data may be processed and monetized. For example, data concerning consumers' habits may be used to establish their preferences and, subsequently, for targeted

¹ According to Article 3(1) of the Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, (non-personal) data “means data other than personal data as defined in point (1) of Article 4 of 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 – GDPR*). For a general definition of “data”, see now Article 2(1) of the Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (*Data Governance Act – DGA*). Cf. Article 2(1) of the Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (*Data Act*), COM/2022/68 final.

² See C. IRTI, *Personal Data, Non-personal Data, Anonymised Data, Pseudonymised Data, De-identified Data*, in R. SENIGAGLIA-C. IRTI-A. BERNES (eds.), *Privacy and Data Protection in Software Service*, Springer, 2022, 49 ss. For restrictions concerning the “re-identification of data subjects from anonymised datasets”, see Recital no. 8 of the *Data Governance Act – DGA*.

³ As regards datasets composed of both personal and non-personal data, which could be “inextricably linked”, see Article 2(2) of the Regulation (EU) 2018/1807.



advertising.⁴ Moreover, (anonymized) personal data might be processed to train artificial intelligence systems as well as to verify their outcomes.⁵ It may also be “transferred” from individuals to (many) enterprises as well as from one enterprise to another, against payment.⁶

Building on the assumption that data are essential for innovation and economic growth, it is not surprising that the goal of the latest European strategy is to remove barriers for access to data in order to make it available to different players.⁷ This should be especially achieved by designing and putting in place fair and safe mechanisms of data sharing. Some of them are now provided, e.g., by the so-called Data Governance Act (hereinafter: DGA),⁸ which seeks *inter alia* to regulate trustworthy intermediaries, serving as neutral organizers of the exchange of data—personal and not—between data subjects and data holders, on the one side, and data users on the other [Articles 2(11) and 10 et seq.]. By providing for many safeguards in order to encourage voluntary data sharing (which may also occur for altruistic purposes: so-called data altruism, Articles 16 et seq.) as well as to promote the re-use of information held by the public sector (Articles 3 et seq.), the DGA clearly aims at developing both, the social and the economic potential of data, preventing its concentration and so avoiding lock-in effects (see Recital no. 2).⁹

Currently, large amounts of data, including personal data, are, in fact, still held and managed by a few market players, especially tech giants, which often obtain it directly from users’ online activity and interaction with different technological devices.¹⁰ In this regard, users’ willingness to disclose data also depends on what they receive in return. Therefore, aware of the economic value of data,¹¹ enterprises usually create oc-

⁴For some restrictions in this regard, see now, e.g., Articles 26(3) and 28(2) of the Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (*Digital Services Act – DSA*). On the DSA in general, see B. RAUE and H. HEESEN, *Der Digital Services Act*, in *NJW*, 2022, 3537 ss.

⁵On the AI, see the Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (*Artificial Intelligence Act*) and amending certain union legislative acts, COM/2021/206 final.

⁶Diversity in the structure and functioning of data markets is highlighted by V. ZENO-ZENCOVICH, *Do “Data Markets” Exist?*, in *MediaLaws*, 2/2019, 22 ss., available at <https://www.medialaws.eu/wp-content/uploads/2019/03/2-2019-Zeno-Zencovich.pdf> (accessed on March 28, 2023); cf. P. GALLO, *Il consenso al trattamento dei dati personali come prestazione*, in *Riv. dir. civ.*, 2022, 1054 ss.; F. BRAVO, *Il commercio elettronico dei dati personali*, in T. PASQUINO, A. RIZZO, M. TESCARO (eds.), *Questioni attuali in tema di commercio elettronico*, ESI, 2020, 83 ss.

⁷In particular, “the European data strategy aims to make the EU a leader in a data-driven society. Creating a single market for data will allow it to flow freely within the EU and across sectors for the benefit of businesses, researchers and public administrations”: see https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en (accessed on March 28, 2023). Cf. G. RESTA, *Pubblico, privato, collettivo nel sistema europeo di governo dei dati*, in ID.-V. ZENO-ZENCOVICH (eds.), *Governance of/through big data*, II, Roma TrE-Press, 2023, 605 ss.; P.G. PICT-H. RICHTER, *EU Digital Regulation 2022: Data Desiderata*, in *GRUR Int.*, 2022, 395 ss.; D. POLETTI, *Gli intermediari dei dati*, in *EJPLT*, 2022, 46 ss.

⁸See fn. 1. For additional schemes of data sharing, see also the Data Act Proposal (mentioned in fn. 1).

⁹On the DGA, cf. F. BRAVO, «Destinatario» dell’informazione e trattamento dei dati personali nell’evoluzione dell’ordinamento europeo, in V. D’AURIA (ed.), *I problemi dell’informazione nel diritto civile, oggi. Studi in onore di Vincenzo Cuffaro*, Roma TrE-Press, 2022, 431 ss.; ID., *Intermediazione di dati personali e servizi di data sharing dal GDPR al Data Governance Act*, in *Contr. impr.*, 2021, 199 ss.; D. POLETTI, *Gli intermediari dei dati*, cit., 46 ss.; M. HENNEMANN, L. v. DITFURTH, *Datenintermediäre und Data Governance Act*, in *NJW*, 2022, 1905 ss.; L. v. DITFURTH, G. LIENEMANN, *The Data Governance Act: – Promoting or Restricting Data Intermediaries?*, in *Competition and Regulation in Network Industries*, 2022, 270 ss.; G. RESTA, *Pubblico, privato, collettivo nel sistema europeo di governo dei dati*, cit., 605 ss., 612 ss.; H. RICHTER: *Looking at the Data Governance Act and Beyond: How to Better Integrate Data Intermediaries in the Market Order for Data Sharing*, in *GRUR Int.*, 2023, 458 ss. For an article-by-article commentary, see L. SPECHT, M-HENNEMANN (eds.), *Data Governance Act*, Hart, Beck, Nomos, 2023 (forthcoming).

¹⁰For gatekeepers’ practices of data collection, see Recital no. 36 of the Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (*Digital Markets Act – DMA*). As regards the gatekeepers’ obligations, see Article 5 of the DMA.

¹¹Cf. P. HACKER, *Regulating the Economic Impact of Data as Counter-Performance: From the Illegality Doctrine to the Unfair Contract Terms Directive*, in S. LOHSSE, R. SCHULZE, D. STAUDENMAYER (eds.), *Data as Counter-Performance – Contract Law 2.0?*,



casions for collection of information, e.g. by offering performances that users can only get (or can get for a cheaper price) if they allow their data to be processed by the supplier for specific, especially commercial purposes.

Such bundling practice, in which personal data is *de facto* somehow used as a counter-performance in exchange for services, contents and (other) goods (and from which intermediaries are now prevented according to the DGA),¹² is widespread in the field of supplying digital content and services:¹³ while access to such contents and services is generally advertised as being free of charge (according to one view misleadingly),¹⁴ consumers' personal data is often required to gain access to them. Data-based business models are used, for example, by social media platforms as well as by online newspapers and other internet websites, which increasingly demand users choose between reading their articles and contents while being tracked by (non-necessary) cookies and paying a certain fee to access them without being tracked.¹⁵ Similar business models are then also used in other fields, e.g. in that of telematics and so-called black box car insurance, where the insured may get a discounted premium, if he/she allows the insurer to collect data concerning his/her driving

Hart Publishing-Nomos, 2020, 48 ss.; G. RESTA, V. ZENO, ZENCOVICH, *Volontà e consenso nella fruizione dei servizi di rete*, in *Riv. trim. dir. proc. civ.*, 2018, 416 s.; G. MALGIERI, B. CUSTERS, *Pricing Privacy – The Right to Know the Value of Your Personal Data*, in *Computer Law & Sec. Rev.*, 2018, 289 ss.

¹² See Article 12(a) of the DGA: “the data intermediation services provider shall not use the data for which it provides data intermediation services for purposes other than to put them at the disposal of data users”.

¹³ On data as counter-performance, see the proceedings collected in S. LOHSSE, R. SCHULZE, D. STAUDENMAYER (eds.), *Data as Counter-Performance – Contract Law 2.0?*, cit. See also, among others, V. RICCIUTO, *L'equivoco della privacy. Persona vs. dato personale*, ESI, 2022; T. BAUERMEISTER, *Die „Bezahlung“ mit personenbezogenen Daten bei Verträgen über digitale Produkte*, in *AcP*, 2022, 372 ss.; M. WALKER, *Die Kosten kostenloser Dienste*, Duncker Humboldt, 2021; A. LA SPINA, *La transmisión de los datos de carácter personal del consumidor para la adquisición de servicios y contenidos digitales*, in *Juscivile*, 2021, 1663 ss.; G. VERSACI, *La contrattualizzazione dei dati personali dei consumatori*, ESI, 2020; L. MISCHAU, *Daten als „Gegenleistung“ im neuen Verbrauchervertragsrecht*, in *ZEuP*, 2020, 335 ss.; F. BRAVO, *Lo “scambio di dati personali” nei contratti di fornitura di servizi digitali e il consenso dell'interessato tra autorizzazione e contratto*, in *Contr. impr.*, 2019, 34 ss.; P. HACKER, *Daten als Gegenleistung: Rechtsgeschäfte im Spannungsfeld von DS-GVO und allgemeinem Vertragsrecht*, in *ZfPW*, 2019, 148 ss.; G. RESTA, *I dati personali oggetto del contratto. Riflessioni sul coordinamento tra la Direttiva 2019/770 e il Regolamento 2016/679*, in *Annuario del contratto 2018*, Giappichelli, 2019, 125 ss.; B. ZÖCHLING-JUD, *Daten als Leistung*, in N. FORGÓ, B. ZÖCHLING-JUD (eds.), *Das Vertragsrecht des ABGB auf dem Prüfstand: Überlegungen im digitalen Zeitalter*, Manz, 2018, 241 ss.; S. THOBANI, *Diritti della personalità e contratto: dalle fattispecie più tradizionali al trattamento in massa dei dati personali*, Ledizioni, 2018, 158 ss.; C. LANGHANKE, *Daten als Leistung*. Mohr Siebeck, 2018; A. DE FRANCESCHI, *La circolazione dei dati personali tra privacy e contratto*, ESI, 2017; L. SPECHT, *Daten als Gegenleistung – Verlangt die Digitalisierung nach einem neuen Vertragstypus?*, in *JZ*, 2017, 763 ss.; A. METZGER, *Dienst gegen Daten: Ein synallagmatischer Vertrag*, in *AcP*, 2016, 817 ss.; C. PERLINGIERI, *Profili civilistici dei social network*, ESI, 2014; R. CATERINA, *Cyberspazio, social network e teoria generale del contratto*, in *AIDA*, 2011, 93 ss. For more publications, see A. METZGER, *A Market Model for Personal Data: State of Play under the New Directive on Digital Consent and Digital Services*, in S. LOHSSE, R. SCHULZE, D. STAUDENMAYER (eds.), *Data as Counter-Performance*, cit., 25 ss., fn. 1, 6 and 13 as well as S. PAGLIANTINI, *L'attuazione minimalista della Dir. 2019/770/UE: riflessioni sugli artt. 135-octies, 135-vicies ter c. cons. la nuova disciplina dei contratti b-to-c per la fornitura di contenuti e servizi digitali*, in *NLCC*, 2022, 1499 ss.

¹⁴ See, e.g., C. LANGHANKE-M. SCHMIDT-KESSEL, *Consumer Data as Consideration*, in *EuCML*, 2015, 218. See also the Italian Council of State – Consiglio di Stato 29 March 2021, no. 2631, in *Foro it.*, 2021, 6, 3, 325. On this point, see (also for further references) C. SOLINAS, *Circolazione dei dati personali, onerosità del contratto e pratiche commerciali scorrette*, in *Giur. it.*, 2021, 320 ss.; A. DE FRANCESCHI, *Digitale Inhalte gegen personenbezogene Daten: Unentgeltlichkeit oder Gegenleistung?*, in M. SCHMIDT-KESSEL-M. KRAMME (eds.), *Geschäftsmodelle in der digitalen Welt*, JWV, 2017, 115 and 131 s. As to the possibility to additionally apply contract and consumer law (remedies), V. RICCIUTO, *L'equivoco della privacy*, cit., 179 ss. In the sense that “the infringement of a rule relating to the protection of personal data may at the same time give rise to an infringement of rules on consumer protection or unfair commercial practices”, see CJEU 28 April 2022, C-319/20 – *Meta Platforms Ireland*, point 78.

¹⁵ As regards the so-called “cookie-walls”, see, also for references to French and Austrian Data Protection Authorities' statements, S. SCHULZ, *Artikel 7 GDPR*, in P. GOLA, D. HECKMANN (eds.), *Datenschutz-Grundverordnung – Bundesdatenschutzgesetz. Kommentar*, Beck, 2022, Rn. 31.



patterns. Such data is usually processed for risk assessment and fraud prevention; nevertheless, it may be also used for other (commercial) purposes, which allow the insurance company to profit from the information collected (and the insured to receive, potentially, an additional insurance premium reduction).

Even though exchange of personal data on the market is a widespread practice, researchers still disagree on how to deal with it from a legal point of view. On the one hand, data protection law (mainly laid down in the GDPR) primarily deals with personal data from a fundamental, personality rights perspective:¹⁶ hence, it does not present an exhaustive legal framework for managing the economic interests of subjects involved in transactions concerning their information. On the other hand, contract law seems to be the legal branch apt to govern the exchange of data for (digital) contents, services and (other) goods, ensuring a functioning and fair market, allowing users to exercise their autonomy consciously and even profit from monetary advantages deriving from the processing of their data.¹⁷

However, it is debated whether and how personal data can be legitimately used as a *contractual* (counter-)performance. One could also argue that data monetization and data trade are unethical and therefore undesirable. As such, they should not only be morally disapproved, but also legally banned.¹⁸ The latest legislative development at the European level would probably make such conclusion hard to accept. Nevertheless, the ambiguous character of some European provisions shows the existence of a tangible tension between different perspectives and instances, which clearly adds complexity to the issue of data contractualization.

2. – As a matter of fact, the question of whether personal data may be the object of contracts and contractual performances has been touched on by the European legislator. By adopting Directive no. 2019/770 on certain aspects concerning contracts for the supply of digital content and digital services (hereinafter: DCD), the application of contractual provisions and remedies was extended to cases in which “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” [Article 3(1) of the DCD].¹⁹ Cases in which the consumer does

¹⁶ However, the purpose of the GDPR is not only the protection of the data subject. It also aims at protecting the controller’s right to process personal data, providing for the latter’s free movement. The different “souls” of the GDPR are pointed out by N. ZORZI GALGANO, *Le due anime del GDPR e la tutela del diritto alla privacy*, in N. ZORZI GALGANO (ed.), *Persona e mercato dei dati. Riflessioni sul GDPR*, Wolters Kluwer-Cedam, 2019, 35 ss. With specific regard to the right to portability, which may be considered a tool to promote a data market, see S. TROIANO, *Il diritto alla portabilità dei dati personali*, in N. ZORZI GALGANO (ed.), *Persona e mercato dei dati*, cit., 195 ss.

¹⁷ Cf., for such consideration, D. STAUEMAYER, *Article 3*, in R. SCHULZE, D. STAUEMAYER (eds.), *EU Digital Law*, Hart, Beck, Nomos, 2020, 88 s., Rn. 141; V. MAK, *Contract and Consumer Law*, in V. MAK, E. TJONG TJIN TAI, A. BERLEE (eds.), *Research Handbook on Data Science and Law*, Edward Elgar Publishing, 2018, 17, 20, 32 and 35; N. HELBERGER, F. ZUIDERVEEN BORGESUIS, A. REYNA, *The Perfect Match? A Closer Look at the Relationship between EU Consumer Law and Data Protection Law*, in *CMLRev*, 2017, 1427; C. LANGHANKE, M. SCHMIDT-KESSEL, *Consumer Data*, cit., 219 s.

¹⁸ See, e.g., the 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, 7, point 17, note 27, available at https://edps.europa.eu/sites/edp/files/publication/17-03-14_opinion_digital_content_en.pdf (accessed on March 28, 2023).

¹⁹ On the DCD, see i.a. H. BEALE, *Digital Content Directive And Rules For Contracts On Continuous Supply*, in *JIPITEC*, 2021, 96 ss.; F. ROSENKRANZ, *Spezifische Vorschriften zu Verträgen über die Bereitstellung digitaler Produkte im BGB*, in *ZUM*, 2021, 195 ss.; A. CASSART-F. LORIAUX-A. CRUQUENAIRE, *La Directive 2019/770/UE du 20 mai 2019 relative à certains aspects concernant les contrats de la fourniture de contenus numériques et de services numériques*, in Y. NINANE (ed.), *Vers des relations entre entreprises plus équilibrées et une meilleure protection du consommateur dans la vente de biens et la fourniture de services numériques?*, Larcier, 2021, 209 ss.; I. FERNÁNDEZ CHACÓN, *Some Considerations on the Material Scope of the New Digital Content Directive: Too Much to Work Out for a Common European Framework*, in *ERPL*, 2021, 517 ss.; J. VANHERPE, *White Smoke, but Smoke Nonethe-*



not pay a price in money but provides personal data to the trader are also considered by Directive no. 2019/2161 (so-called *Omnibus Directive*),²⁰ which aims at extending the scope of application of Directive no. 2011/83 (hereinafter: CRD) to transactions in which “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” [see Article 4(2) and Recitals 31 et seq. of the *Omnibus Directive*; cf. the new Article 3(1a) of the CRD].²¹

However, such legislation does not further define the supply of digital contents and services in exchange for data in terms of contract,²² even going so far as to exclude that personal data may be considered a commodity (see Recital no. 24 of the DCD).²³ The application of the consumer (contract) law provisions to cases in which consumers receive contents and services against the disclosure of their data could be read as implicit assignment of contractual nature to such transactions: there will be a (synallagmatic) contract both when paying the price (in money) and when supplying personal data in exchange for digital content or a service [see § 327(3) of the German BGB;²⁴ cf. Preamble of the Spanish *Real Decreto-ley 7/2021, IX 20*].²⁵ Never-

less: *Some (Burning) Questions Regarding the Directives on Sale of Goods and Supply of Digital Content*, in *ERPL*, 2020, 251 ss.; R. SCHULZE, *Die Digitale-Inhalte-Richtlinie – Innovation und Kontinuität im europäischen Vertragsrecht*, in *ZEuP*, 2019, 695 ss.; C. CAMARDI, *Prime osservazioni sulla Direttiva (UE) 2019/770 sui contratti per la fornitura di contenuti e servizi digitali. Operazioni di consumo e circolazione dei dati personali*, in *Giust. civ.*, 2019, 499 ss.; G. SPINDLER, K. SEIN, *The new Directive on Contracts for the Supply of Digital Content and Digital Services – Parts 1 and 2*, in *ERCL*, 2019, 257 ss. and 365 ss.; C. ZOLINSKI, *Contrats de fourniture de contenus et de services numériques. À propos de la directive (UE) 2019/770 du 20 Mai 2019*, in *La Semaine Juridique*, 2019, 2062 ss.; I. BACH, *Neue Richtlinie zum Verbrauchergüterkauf und zu Verbraucherverträgen über digitale Inhalte*, in *NJW*, 2019, 1705 ss.; D. STAUDENMAYER, *Auf dem Weg zum digitalen Privatrecht – Verträge über digitale Inhalte*, in *NJW*, 2019, 2497 ss. See also the article-by-article commentary R. SCHULZE-D. STAUDENMAYER (eds.), *EU Digital Law*, cit. As regards the implementation of the Directive in selected Member States (France, Hungary, Portugal, Spain, Italy, Luxembourg, Belgium, Denmark), cf. the contributions (written by J. Senechal, F. Szilágyi, J. Morais Carvalho, E. Arroyo Amayuelas, A. De Franceschi, F. Pflücke, B. Keirsbilck, E. Terryn, M.J.Sørensen) published in *EuCML*, 2021-2022.

²⁰ An analysis may be found in G. VERSACI, *Le tutele a favore del consumatore digitale nella “Direttiva Omnibus”*, in *Pers. mercato*, 2021, 583 ss. and in M. ĐUROVIĆ, *Adaptation of Consumer Law to the Digital Age: EU Directive 2019/2161 on Modernisation and Better Enforcement of Consumer Law*, in *Anali Pravnog fakulteta u Beogradu*, godina, LXVIII, 2/2020, 62 ss. For the implementation of the Directive in Italy, see now the D.Lgs. no. 26/2023.

²¹ For a broad understanding of “remuneration” see recital no. 16 of the Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast). See also the interpretation of Article 2(4) by G. DE CRISTOFARO, *Legislazione italiana e contratti dei consumatori nel 2022: l’anno della svolta. Verso un diritto “pubblico” dei (contratti dei) consumatori?*, in *NLCC*, 2022, 10 s. A first reference to the business model of paying with data was made in recital no. 18 of the Proposal for a Regulation on a Common European Sales Law.

²² The DCD’s dispositions apply “where the trader supplies or undertakes to supply digital content or a digital service to the consumer, and the consumer provides or undertakes to provide personal data to the trader”: see Article 3(1) of the DCD and cf. Article 3(1a) of the CRD as amended by *Omnibus Directive*.

²³ By avoiding taking a stand on the controversial issue of data as contractual counter-performance, the European legislator probably tried to soothe the criticism already expressed regarding the Directive’s proposal COM(2015) 634: see EDPS Opinion 4/2017, 7, point 17, note 27. The main criticisms have been identified by J. MORAIS CARVALHO, *Sale of Goods and Supply of Digital Content and Digital Services – Overview of Directives 2019/770 and 2019/771*, in *EuCML*, 2019, 197. On the contrary, data may be considered as a tradable asset according to C. PERLINGIERI, *Data as the object of a contract and contract epistemology*, in T. PERTOT, M. SCHMIDT, KESSEL, F. PADOVINI (eds.), *Rechte an Daten*. Mohr Siebeck, 2020, 207 ss. and 210; A. METZGER, Z. EFRONI, L. MISCHAU, J. METZGER, *Data-Related Aspects of the Digital Content Directive*, in *JIPITEC*, 2018, 94; V. RICCIUTO, *L’equivoco della privacy*, cit., 153 ss., 166 ss.; A. DE FRANCESCHI-M. LEHMANN, *Data as Tradeable Commodity and the new Instruments for their Protection*, in *The Italian Law Journal*, 2015, 51 ss. For the controversial issue concerning the qualification and the legal treatment of data, see S. V. ERP, *Management as Ownership of Data*, in S. LOHSSE-R. SCHULZE, D. STAUDENMAYER (eds.), *Data as Counter-Performance*, cit., 77 ss.; D. HÜRLIMANN, H. ZECH, *Rechte an Daten*, in *sui-generis*, 2016, 89 ss. For a monographic study, see C. ANGIOLINI, *Lo statuto dei dati personali. Uno studio a partire dalla nozione di bene*, Giappichelli, 2020.

²⁴ Nevertheless, the German legislator avoided to use the term “Gegenleistung” (counter-performance): see A. METZGER, *Vorbermerkung (vor § 327 BGB)*, in *Münchener Kommentar zum BGB*, Beck, 2022, Rn. 15.



theless, the inclusion of those cases into the scope of application of the Directives' provisions could otherwise be considered merely the result of the European legislator's intention to better protect consumers providing their data in order to get a content or a service (advertised as being) free of charge.²⁶ A more agnostic approach was taken e.g. by the Italian legislator: when implementing the two Directives it replicated the formula(s) used by Article 3(1) of DCD and by Article 4(2) of the *Omnibus* Directive [see Articles 46(1-bis) and 135 *octies*(4) of the Italian *Codice del consumo*],²⁷ without taking a stance on the opportunity to qualify the case concerned in terms of a (synallagmatic) contract.

Actually, the contractualization of personal data seems to be implied also in the above-mentioned DGA and in the provided mechanisms of information sharing, which may involve data subjects and data holders (having the right to grant access to or to share certain data, including the personal data of others), on the one hand, and data users (that may process the accessed data for commercial purposes too) on the other [cf. Articles 2(7 et seq.) and 10]. The existence of contractual relationships between those who exchange data—directly or through an intermediary—could be gleaned, e.g., from Article 2(10) of the DGA, that defines 'data sharing' as the provision of data that may be "based on voluntary agreements". Also, the 'commercial relationships' that the 'data intermediation service' aims at establishing for the purpose of data sharing according to Article 2(11) of the DGA are unlikely to be carried out without passing through a contractual regulation. However, although the "agreements", "exchanges", and "commercial relationships" to which the DGA refers need (*inter alia*) contracts to be concluded between the involved parties,²⁸ the qualification, structure and content of the latter did—once again—not receive specific attention by the legislator.

In light of the divergent positions still existing at the national and European level, the question of whether and of how personal data may be legitimately considered the subject matter of contracts—specifically as a *contractual* (counter-)performance—is therefore still relevant, even more so considering that, by taking a position on new legislative developments in the field of data law, which clearly aims at making more data available for different, also commercial, uses, both—the European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS)—recently confirmed the criticism towards the phenomenon of personal data "commodification", already expressed regarding the Directive's proposal COM(2015) 634.²⁹ On the one hand, such "commodification" is somehow implied in many European provisions [see now also Article 12(h) of the DGA], while on the other, there is some hesitation when it comes to explicitly considering personal data as a commodity.³⁰

²⁵ See J. MORAIS CARVALHO, *Sale of Goods*, cit., 197, fn. 50. For the qualification issue, see then V. MAK, *Contract and Consumer Law*, cit., 17 and 33 and, from an Italian perspective, V. RICCIUTO, *L'equivoco della privacy*, cit., 152 s., 156 ss., 162 and 166; G. Buset, *Brevi note sull'attribuzione del godimento nel prisma della evoluzione tecnologica*, in *Juscivile*, 2022, 512, nt. 4; P. GALLO, *Il consenso al trattamento*, cit., 1064 s.; G.M. UBERTAZZI, *Models of Information Circulation and the Function of Privacy*, in *EuCML*, 2022, 210 s.

²⁶ Cf. C. CAMARDI, *Prime osservazioni*, cit., 508 s.

²⁷ See however V. RICCIUTO, *L'equivoco della privacy*, cit., 140 and 151 s.: in his opinion, there is a slight difference between the European and the Italian (implementing) provision (which replaces the verb "undertakes" with the verb "oblige"), showing that Article 135 *octies* (4) of the Italian *Codice del consumo* is less neutral than Article 3 of the DCD.

²⁸ According to Article 2(11) of the DGA data intermediation services may establish "commercial relationships" through many different, including legal, means.

²⁹ Cf. EDPS Opinion 4/2017, 7, point 17, note 27; EDPB Statement 05/2021 on the Data Governance Act in light of the legislative developments, 4, available at https://edpb.eu-ropa.eu/system/files/2021-05/edpb_statementondga_19052021_en_0.pdf (accessed on March 28, 2023) and EDPB-EDPS Joint Opinion 2/2022 on the Proposal of the European Parliament and of the Council on harmonised rules on fair access to and use of data (*Data Act*), 8, note 15 and 18, note 63, available at https://edpb.europa.eu/system/files/2022-05/edpb-edps_joint_opin-ion_22022_on_data_act_proposal_en.pdf (accessed on March 28, 2023).

³⁰ D. POLETTI, *Gli intermediari dei dati*, cit., 51, 54.



3. – By extending some contractual provisions to cases in which personal data are provided by consumers in order to obtain digital services and contents offered on the market and by defining set of rules to promote the sharing of data, including the personal data, the European legislator did not even clarify what personal data provision consists of in the considered cases.³¹

As a combined reading of the provisions laid down in the above-mentioned legislation shows, personal data may be actually provided by different actors (data subjects or data holders) and within various relationships (it may be shared with data users directly or through a provider of a data intermediation service). Without ignoring the different perspectives from which the problem concerning personal data provision may be investigated,³² in the following only the data subject's point of view will be analysed. More specifically, the attention will focus on the provision of personal data made by consumers, who disclose their data directly to the supplier of content and services in order to get the provided performance in return. The selected point of view should allow us to address and to deepen a specific question—that of the bundled data subject's consent—which is crucial and actually of preliminary nature when deciding on if and on how consumers' personal data may legitimately enter the market and become the object of economically valuable transactions.

Focusing the attention on the provision of personal data from the mentioned point of view, the first question that arises is whether such provision consists of the delivery of personal data as such or if something more than data supplying is required from the data subject acting as a consumer. In this regard, assuming the need for a specific GDPR legal basis for the processing of personal data, most scholars consider the European consumer law provisions laid down in the currently implemented DCD and *Omnibus* Directive to be based on the idea that consumers, by concluding the contract for the supply of digital content or service with the trader,³³ also agree to the processing of their data for accessory purposes, giving their consent under Article 6(1)(a) of the GDPR:³⁴ the latter is, in fact, essential to assign to the trader the right

³¹ On this point see C. LANGHANKE, M. SCHMIDT-KESSEL, *Consumer Data*, cit., 220; A. DE FRANCESCHI, *Italian consumer Law after the Transposition of Directives (EU) 2019/770 and 2019/771*, in *EuCML*, 2022, 73; C. IRTI, *Consenso “negoziato” e circolazione dei dati personali*, Giappichelli, 2021, 52; G. Buset, *Brevi note*, cit., 511 ss.; F. GRAF VON WESTPHALEN, C. WENDEHORST, *Hergabe personenbezogener Daten für digitale Inhalte – Gegenleistung, bereitzustellendes Material oder Zwangsbeitrag zum Datenbinnenmarkt?*, in *BB*, 2016, 2181; L. SPECHT, *Daten als Gegenleistung*, cit., 763 ss.; C. PERLINGIERI, *Data as the object of a contract*, cit., 207 ss.

³² See D. POLETTI, *Gli intermediari dei dati*, cit., 53 s.

³³ For the gratuitous structure of such contracts, see C. CAMARDI, *Prime osservazioni*, cit., 508 s. According to other Authors (cf. V. RICCIUTO, *Il contratto ed i nuovi fenomeni patrimoniali: il caso della circolazione dei dati personali*, in *Riv. dir. civ.*, 2020, 652 s.; G. Buset, *Brevi note*, cit., 512, fn. 4), there would be an “exchange” (“scambio”) between a performance and a counter-performance. Further, German authors qualify the contract entered into by the consumer as a “*schuldrechtlicher Vertrag*” (contract with obligatory effects): see A. METZGER, § 327 BGB, in *Münchener Kommentar zum BGB*, cit., Rn.18.

³⁴ A. METZGER, *A Market Model*, cit., 33; D. STAUDENMAYER, *Article 3*, cit., 73, Rn 60 s., 64; E. ARROYO AMAYUELAS, *The Implementation of the EU Directives 2019/770 and 2019/771 in Spain*, in *EuCML* 2022, 37; C. IRTI, *Consenso “negoziato”*, cit., 52; C. LANGHANKE, M. SCHMIDT-KESSEL, *Consumer Data*, cit., 220. As to the role of data subject's consent by “paying” with data, see G. DE CRISTOFARO, *Die datenschutzrechtliche Einwilligung als Gegenstand des Leistungsversprechens*, in T. PERTOT, M. SCHMIDT-KESSEL, F. PADOVINI (eds.), *Rechte an Daten*, cit., 151 ss.; M. SCHMIDT-KESSEL, *Consent for Processing of Personal Data and its Relationship to Contract*, in A. DE FRANCESCHI, R. SCHULZE (eds.), *Digital Revolution – New Challenges for Law*, Beck-Nomos, 2019, 75 ss.; V. RICCIUTO, *L'equivoco della privacy*, cit., 137 ss. and 160; G. Buset, *Brevi note*, cit., 511 ss. On the consent to data processing see also S. SCHULZ, *Artikel 6 DSGVO*, in P. GOLA, D. HECKMANN (eds.), *Datenschutz-Grundverordnung Datenschutz-Grundverordnung – Bundesdatenschutzgesetz*, Beck, 2022, Rn. 21 ss.; A. GENTILI, *La volontà nel contesto digitale: interessi del mercato e diritti delle persone*, in *Riv. trim. dir. proc. civ.*, 2022, 701 ss.; C. IRTI, *Consenso “negoziato”*, cit.; A. VIVARELLI, *Il consenso al trattamento dei dati personali nell'era digitale. Sfide tecnologiche e soluzioni giuridiche. Quaderni de «Il Foro napoletano»*, ESI, 2019; F. BRAVO, *Le condizioni di liceità del trattamento di dati personali*, in G. FINOCCHIARO (a cura di), *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Zanichelli, 2019, 110 ss.



to use the information gathered, unless another legal basis for processing is applicable in the specific case.³⁵

As a result, scholars further investigate the relationship between contractual consent and the one concerning data processing.³⁶ Many questions arise in this respect. There is discussion, e.g., of whether the privacy consent can be still regarded as freely given under the GDPR, when the data subject, by entering into the contract, commits to agreeing to the use of his/her information: the consent could in fact not be considered as freely given according to the GDPR, if the data subject took on an obligation to give it.³⁷ It is further debated, whether it makes sense to distinguish between the data subject's consent and the contractual one: while, according to some authors, they would necessarily be separate from each other and the validity of the privacy consent would be “no prerequisite of a valid contract to provide for (a right to use) personal data”,³⁸ in another view users would only give consent once, which would be subject to both contract and data protection law requirements.³⁹ Moreover, as the data subject may withdraw his/her consent at any time under Article 7(3) of the GDPR, one could also ask what the impact of such a withdrawal on the contract concluded with the supplier would be.⁴⁰

³⁵ See e.g. A. METZGER., § 327 BGB, cit., Rn. 20: legal basis other than consent – especially those in article 6(1)(d)(e) and (f) – could also be relevant in the given case. On the contrary, the DCD would not add an additional legal basis to those provided in the GDPR: D. STAUDENMAYER, *Article 3*, cit., 88, Rn. 140. The same goes, e.g., for the DGA, which “does not create a legal basis for the processing of personal data”: see Article 1(3) and cf. Recital no. 4. Cf. Article 5(2) and Recital no. 36 of the DMA, which restrict legal basis for data processing gatekeepers may rely on in some cases.

³⁶ R.M. GARCÍA PÉREZ, *Interacción entre protección del consumidor y protección de datos personales en la Directiva 770/2019: Licitud del tratamiento y conformidad de los contenidos y servicios digitales*, in E. ARROYO AMAYUELAS, S. CÁMARA LAPUENTE (directed by), *El Derecho privado en el nuevo paradigma digital*, Marcial Pons, 2020, 175 ss. For the coordination issue, see also M. SCHMIDT-KESSEL, *Consent for Processing*, cit., 75 ss.; C. IRTI, *Consenso “negoziato”*, cit., *passim*; G. VERSACI, *La contrattualizzazione dei dati personali*, cit., 113 ss., *passim*; J. SENECHAL, *The Implementation of the EU Directives 2019/770 and 2019/771 in France*, in *EuCML*, 2021, 266; A. DE FRANCESCHI, *Italian Consumer Law*, cit., 76.

³⁷ For the capability of the consent of being object of an obligation, see M. SCHMIDT-KESSEL, *Consent for the Processing*, cit., 78; ID., *Right to Withdraw Consent*, cit., 131: “the GDPR understands consent as being something ‘under’ the contract, which might even become the object of a promise so becoming the object of a contractual obligation”. Cf. A. METZGER, § 327 BGB, cit., Rn. 18. *Contra* C. IRTI, *Consenso “negoziato”*, cit., 103; G. MARINO, *Mercato digitale e sistema delle successioni mortis causa*, *ESI*, 2022, 129 s.

³⁸ M. SCHMIDT-KESSEL, *Consent for the Processing*, cit., 77 s.: in his opinion “the Regulation turns out to think of consent and contract as being different and at least somewhat separated institutions”. Cf. A. METZGER, *A Market Model*, cit., 33 s.; ID., § 327 BGB, cit., Rn; T. RIEHM, *Freie Widerrufbarkeit der Einwilligung und Struktur der Obligation. Daten als Gegenleistung?*, in *Rechte an Daten*, cit., 186 s. 18. For the existence of two different consents (and two different layers), see C. CAMARDI, *Prime osservazioni*, cit., 510; C. IRTI, *Consenso “negoziato”*, cit., 77. The idea that there are different validity requirements for the two consents could find a confirmation in Article 8 GDPR on child's consent: in fact, the provision “shall not affect the general contract law of Member States such as the rules on the validity, formation or effect of a contract in relation to a child”. A coordination between the general capacity requirements and the data protection law ones would be therefore necessary: see R. SENIGAGLIA, *Minore età e contratto. Contributo alla teoria della capacità*, Giappichelli, 2021, 75 ss. As specifically regards the consent given by a child, see, for the effects of considering the two consents as completely separate and independent from each other, V. RICCIUTO, *L'equivoco della privacy*, cit., 139; cf. S. THOBANI, *Diritti della personalità e contratto*, cit., 195 ss.

³⁹ V. RICCIUTO, *L'equivoco della privacy*, cit., 144 ss., spec. 149, 152 s. and 155: according to him specific rules (stemming from the GDPR) would (additionally) apply to contracts to the supply of goods, when data are used as counter-performance. Cf. P. GALLO, *Il consenso al trattamento*, cit., 1067 and 1070: in case of a conflict, data protection law requirements would however prevail over the contractual ones; thus, a consent would be valid, for example, even when given by a child (not yet 18 years old).

⁴⁰ See M. SCHMIDT-KESSEL, *Right to Withdraw Consent*, cit., 129 ss.; T. RIEHM, *Freie Widerrufbarkeit der Einwilligung*, cit., 175 ss.; A. METZGER, *A Market Model*, cit., 35; I. KULL, *Withdrawal from the Consent to Process Personal Data Provided as Counter-Performance: Contractual Consequences*, in *Juridiskā zinātne/Law*, No. 13, 2020, 33 ss.; G. VERSACI, *La contrattualizzazione dei dati personali*, cit., 182 ss.; C. IRTI, *Consenso “negoziato”*, cit., 112 ss.; S. THOBANI, *Diritti della personalità e contratto*, cit., 186 ss. Another question that arises as to the relationship between contract and data protection law is that concerning the possibility to con-



The European legislator did not give specific answers to all these questions. In fact, with a formula that is typical for European acts also involving personal data, it only stated that data protection law should prevail [over the contract law provisions: Article 3(8) and Recital no. 37 of the DCD; cf. also Recital no. 4 of the DGA]. However, by doing so, he failed to clarify any aspects regarding the interaction of the latter with (consumer) contract law.

Some national legislators have addressed certain issues regarding the interplay between different legal fields, such as that concerning the impact of exercising a data subject's right, by explicitly providing for the automatic termination of the contract [Article 7:50ab(5) of the Dutch WB] or at least for the possibility of such a termination after the withdrawal of consent [or after the consumer's objection: see e.g. § 327q(2) of the German BGB and Article 119 *ter*(7) of the Spanish *Texto Refundido de la Ley General de Defensa de los Consumidores y Usuarios* – TR-LGDCU].⁴¹ On the contrary, other legislators rather opted for a simple implementation of the European dispositions, merely confirming the priority of data protection law (see e.g. Article 135-*novies*(6) of the Italian *Codice del consumo*),⁴² hence leaving the relationship between the latter and contract (consumer) law to be ascertained by way of interpretation.⁴³

It is hardly necessary to mention that similar coordination issues also arise with regard to other legal frameworks now applying to personal data, which only can be legitimately processed when a legal basis according to the GDPR exists and the data user complies with other provisions laid down therein.⁴⁴

4. – When determining the interaction between data protection and (consumer) contract law, there is one provision in particular that should be preliminarily considered in order to establish if, when and how con-

sider the failure to comply with the GDPR as a lack of conformity according to the DCD: see G.M. UBERTAZZI, *Models of Information*, cit., 211 and, referring to the French implementation act, J. SENECHAL, *The Implementation of the EU Directives*, cit., 266.

⁴¹ Cf. A. METZGER, § 327q BGB, in *Münchener Kommentar zum BGB*, cit., Rn. 3 ss. and E. ARROYO AMAYUELAS, *The Implementation*, cit., 37: “the hypothesis on which this remedy granted to the trader is based has nothing to do with breach of contract and, consequently, it is questionable whether what is in fact only a right to withdraw from or to rescind the contract should be classified as a termination (“*resolución*”).”

⁴² As regards the effects of the consent's withdrawal, from an Italian perspective, P. GALLO, *Il consenso al trattamento*, cit., 1088 ss.; S. THOBANI, *Diritti della personalità e contratto*, cit., 186 ss.; C. IRTI, *Consenso “negoziato”*, cit., 113 s.; S. PAGLIANTINI, *L'attuazione minimalista della Dir. 2019/770/UE*, cit., 1522 ss.

Further, the specific issue of the contractual consequences of the consent withdrawal was not explicitly addressed by the French legislator: cf. J. SENECHAL, *The Implementation*, cit., 266, in whose opinion “when the consumer's consent is the legitimate basis for the processing of his personal data, the withdrawal of consent cannot affect the survival of the contract concluded between the consumer, the holder of the data, and the trader, even if the contract does not provide for a price to be paid by the consumer”.

Provisions concerning the consequences of the consent's withdrawal are also missing in Austria, where some Authors argue for the survival of the obligation (after the consent's withdrawal) as a natural obligation (*Naturalobligation*): for the implementation of the DCD in Austria, cf. J. FLUME, C. KRONTHALER, S. LEIMER (hrsg.), *VGG – Verbrauchergewährleistungsgesetz*, Verlag Österreich, 2022, *passim*.

⁴³ The different approaches taken in some selected legal orders are pointed out by G. VERSACI, *Il valore negoziale dei dati personali del consumatore: spigolature sul recepimento della direttiva 2019/770/UE in una prospettiva comparata*, in E. CREMONA-F. LAVIOLA, V. PAGNANELLI (eds.), *Il valore economico dei dati personali tra diritto pubblico e diritto privato*, Giappichelli, 2022, 163 ss.

⁴⁴ Cf. G. RESTA, *Pubblico, privato, collettivo nel sistema europeo di governo dei dati*, cit., 623 s.; F. BRAVO, *Intermediazione di dati personali e servizi di data sharing dal GDPR al Data Governance Act*, cit., 199 ss.; M. HENNEMANN, L. V. DITFURTH, *Datenintermediäre und Data Governance Act*, cit., 1910; D. GERADIN, K. BANIA, T. KARANIKIOTI, *The Interplay Between the Digital Markets Act and the General Data Protection Regulation*, 2022, available at <https://ssrn.com/abstract=4203907> (accessed on June 04, 2023); B. STEINRÖTTER, *Verhältnis von Data Act und DS-GVO. Zugleich ein Beitrag zur Konkurrenzlehre im Rahmen der EU-Digitalgesetzgebung*, in *GRUR*, 2023, 216 ss.; L. SPECHT-RIEMENSCHNEIDER, *Der Entwurf des Data Act*, in *MMR*, 2022, 810 s.



sumers may lawfully give consent to the processing of their personal data by concluding a contract for the supply of (digital) contents or services. The reference here is to Article 7(4) of the GDPR, according to which “when assessing whether consent is freely given, utmost account shall be taken of whether, *inter alia*, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract”.

In following the attention will be focused on this disposition, which apparently covers instances that fall within the scope of European consumer law and especially of the DCD. The latter, in fact, does not apply when data is exclusively processed for the purpose of supplying the content or the service [i.e. for the contractual performance, or for allowing the trader to comply with legal requirements: Article 3(1) subpara 2 of the DCD]. Moreover, traders generally accept data instead of money only if they have the possibility of monetizing it, by using information for secondary purposes which are extraneous to the performance of the contract concluded with the data subject. Such use of personal data typically requires consent according to Article 6(1)(a) of the GDPR, on which the performance of the contract is therefore conditional.

Indeed, the extracontractual use of data could be also based on a legitimate interest according to Article 6(1)(f) of the GDPR,⁴⁵ which, however, does not allow the processing of all categories of personal data: for example, it is not a suitable basis for processing data according to Article 9 of the GDPR or by automated individual decision-making *ex* Article 22 of the GDPR. Additionally, the existence of a legitimate interest requires an assessment on a case-by-case basis in order to establish if it is overridden by other interests and fundamental rights and freedoms of the data subject. Moreover, relying on Article 6(1)(f) of the GDPR is not permitted, e.g., in case of some gatekeepers’ data processing activities [cf. Article 5(2) and Recital no. 36 of the DMA]. Following, Article 6(1)(f) of the GDPR would in many cases not constitute an appropriate legal basis for the secondary use of data, which is usually pursued by traders supplying digital contents and services (free of charge). On the contrary, consent according to Article 6(1)(a) of the GDPR would often be essential for this purpose.⁴⁶

Regardless of whether such consent may be considered separate from the contractual one or not, it would in any case be subject (also) to the GDPR provisions, including Article 7(4) of the GDPR. However, it is unclear if the latter disposition, on the one side, and the contract law provisions (contained in the DCD as well as in the national implementing laws), on the other side, may be reconciled. One could argue, for example, that consent bundling is highly undesirable or even prohibited according to Article 7(4) of the GDPR. This would lead to a coordination issue or rather to a conflict between data protection law and the DCD, which applies *inter alia* where the consent is tied to the performance of the contract for the supply of digital content or a service, i.e. where the consumer allows the supplier to use his/her data for purposes not necessary for the contractual performance and where the consumer’s consent to such a use of data is often essential if he/she wants to obtain the content or the service offered by the trader (or, at least, to get it without paying a monetary price).

Considering the bundled consent, on which the phenomenon of “paying” with personal data is typically based, as prohibited according to Article 7(4) of the GDPR, could even lead to a deprivation of consumer rights when contents and services are supplied against the data subject’s information. According to the priority given by the European legislator to data protection law [see Article 3(8) and cf. Recital no. 37 of the

⁴⁵ Legal basis *ex* Article 6(1)(d) and (e) could be relevant as well: see A. METZGER., § 327 *BGB*, cit., Rn. 20.

⁴⁶ The role of data subject’s consent seems to be even reinforced according to the latest European legislation (see especially the provisions laid down in the DGA and in the DMA).



DCD] and therefore also to Article 7(4) of the GDPR, contracts the performance of which is made dependent upon the consent to personal data processing that is not needed for the performance itself would be in infringement of the GDPR and could be regarded as illegal and eventually as void.⁴⁷ Consequently, the contract law provisions and remedies of the DCD, which imply the existence of a (valid) contract, would not apply.⁴⁸ This conclusion would also follow from an understanding of consent and contract as separate but (functionally) related acts which, as a rule (and unless adhering to the German principle of abstraction), exist and fall together (*simul stabunt, simul cadent*).⁴⁹

Nevertheless, such conclusion could render Article 3(1) of the DCD meaningless or, at least, of little relevance, as consumer (protection) law would only apply when personal data processing would (and could) be exceptionally based on legal basis other than consent. Hence, an interpretation such as that mentioned above can only be shared if Article 7(4) of the GDPR cannot be understood otherwise. As will be shown, however, coordination between different legal frameworks (i.e. between data protection and consumer contract law) is certainly possible.

4.1. – Supposing that the European (consumer) contract law provisions are, in principle, based on the assumption that consumers give their consent to data processing, the possibility to reconcile them with Article 7(4) of the GDPR depends eventually on whether the latter really provides for a bundling prohibition and, if so, on how such a prohibition shall be understood.⁵⁰

This has already been discussed before the GDPR entered into force. Although Directive no. 95/46/EC did not contain any provision that was analogous to Article 7(4) of the GDPR, some national legislators provided for a specific rule concerning the ban on tying within their national laws [see e.g. the former § 28(3b) of the German BDSG]. Furthermore, in some Member States which did not implement specific rules on the ban on tying, data protection authorities derived the existence of such a ban from the principle of freedom to consent [cf. Articles 2(h) and 7 of Directive no. 95/46/EC].⁵¹

However, even providing that a prohibition of coupling privacy consent and contract exists, there are different ways of how to interpret it. For example, some scholars, courts and authorities reckon that the bundling prohibition (does not only exist, but) should also be interpreted strictly. In this view, consent cannot be considered as freely given if the contractual performance (or the conclusion of the contract) is conditional on the data subject's consent to process his/her data for purposes extraneous to it.⁵²

⁴⁷ D. STAUDENMAYER, *Article 3*, cit., 89, Rn. 142; A. METZGER, *A Market Model*, cit., 33; ID., § 327 BGB, cit., Rn. 18 and 20; cf. § 327q BGB, cit., Rn. 3 s.; P. HACKER, *Regulating the Economic Impact*, cit., 48 ss.

⁴⁸ For some criticism, see Authors in fn. 47.

⁴⁹ Cf. (also for some solution proposals) G. VERSACI, *La contrattualizzazione dei dati personali*, cit., 177 ss.; S. PAGLIANTINI, *L'attuazione minimalista della Dir. 2019/770/UE*, cit., 1528 ss. See however (from a German perspective) A. METZGER, § 327q BGB, cit., Rn. 3; ID., *A Market Model*, cit., 33; B. LAHUSEN, *Verdinglichung durch Datenschutz*, in *AcP*, 2021, 14 s.; L. SPECHT, *Daten als Gegenleistung*, cit., 768.

⁵⁰ See, for the different interpretations, G. RESTA, *I dati personali oggetto del contratto*, cit., 137 ss.; ID.-V. ZENO-ZENCOVICH, *Volontà e consenso nella fruizione dei servizi di rete*, cit., 426 ss. and 430 ss.; G. VERSACI, *La contrattualizzazione dei dati personali*, cit., 98 ss.; S. PAGLIANTINI, *L'attuazione minimalista della Dir. 2019/770/UE*, cit., 1515 s., nt. 74; A. GENTILI, *La volontà nel contesto digitale: interessi del mercato e diritti delle persone*, cit., 711.

⁵¹ It. Garante della Privacy 28 May 1997, in *Corr. giur.*, 1997, 915 ss. (with the case note by V. ZENO-ZENCOVICH, *Il "consenso informato" e la "autodeterminazione informativa" nella prima decisione del Garante*).

⁵² Cf. P. VOIGT, A. VD BUSSCHE, *EU-Datenschutz-Grundverordnung (DSGVO)*, Springer, 2018, 123; S. GIERSCHMANN, *Was „bringt“ deutschen Unternehmen die DS-GVO? – Mehr Pflichten, aber die Rechtsunsicherheit bleibt*, in *ZD*, 2016, 54; U. DAMMAN,



A similar approach was taken by the Austrian Supreme Court in 2018:⁵³ there would be a strong presumption of invalidity of the consent bundled with the acceptance of contractual terms and conditions that cannot be renounced (without renouncing the contract, too) and such presumption could not be overcome by simply demonstrating the lack of the controller's monopoly position in the market.

Also, according to Guidelines no. 05/2020 of the EDPB, consent bundled to the contractual performance should be presumed not to be freely given⁵⁴ (for such presumption see then Recital no. 43 of the GDPR). In fact, the data subject—not wishing to make his/her information available for uses not strictly necessary for the contractual performance—would be unable to refuse the consent without renouncing the service or the content to the supplying of which the consent is tied. In other words, if interested in the contract, he/she would be “forced” to agree with the extracontractual use of data. As the compulsion would hinder the free exercise of the data subject's will, and would therefore render his/her consent invalid, the possibility of coupling consent and contract (and, eventually, of “paying” with personal data) would be excluded.

Indeed, cases in which the consent would be free and valid, despite conditionality, could exist from both the Austrian Supreme Court's and the EDPB's point of view. Nevertheless, such cases would be highly exceptional. To overcome the (strong) presumption of the consent's invalidity, the controller would need to prove that the data subject was effectively able to choose between paying with data (allowing its use for purposes not strictly necessary for contractual performance) and getting an equivalent performance (from the same controller) without consenting to data processing.⁵⁵ By lack of such evidence, the data subject's consent would be invalid and the question concerning the validity of the contract, which is conditional on it, would also arise. In order not to deprive consumers of the protection given by the DCD when the contract is based on an invalid consent and is therefore in infringement of the data protection law, one could only argue that the occurrence of a data breach does not automatically result in the Directive's non-application, regardless of the validity of the contract entered into by the data subject to which the (invalid) consent is tied.

4.2. – In another opinion, the ban on tying, whether existing or not, would, on the contrary, not hinder the possibility to (legitimately) use personal data in order to “pay” for the service or the content supplied. A consent according to Article 6(1)(a) of the GDPR would in fact not be necessary for the purpose. As data monetization is closely linked with the performance of the contract concluded with the trader supplying contents, services or (other) goods,⁵⁶ in the discussed cases data processing would rather find its legal basis in Article 6(1)(b) of the GDPR [cf. Article 7(b) Directive no. 95/46/EC], which provides for the lawfulness of data

Erfolge und Defizite der EU-Datenschutzgrundverordnung – Erwarteter Fortschritt, Schwächen und überraschende Innovationen, in ZD, 2016, 311. According to N. HÄRTING, *Internetrecht*. Otto Schmidt, 2017, A. II Rz. 56, the bundling prohibition could even be regarded as reinforced by the GDPR. For the unlawfulness of the tying operations “in principle”, A. GENTILI, *La volontà nel contesto digitale: interessi del mercato e diritti delle persone*, cit., 711.

⁵³ OGH 31 August 2018 – 6 OB 140/18 H. For a case note, see S. SCHWAMBERGER, *Reichweite des Koppelungsverbots nach alter und neuer Rechtslage*, in GPR, 2019, 57 ss.

⁵⁴ EDPB Guidelines 05/2020, cit., 10 ss., 12, point 35.

⁵⁵ EDPB Guidelines 05/2020, cit., 10 ss., 12, points 35, 37 s.; OGH 31 August 2018 – 6 OB 140/18 H; cf. A. GOLLAND, *Das Kopplungsverbot in der Datenschutz-Grundverordnung. Anwendungsbereich, ökonomische Auswirkungen auf Web 2.0-Dienste und Lösungsvorschlag*, in MMR, 2018, 134 s.

⁵⁶ Although the DCD only applies to the supply of digital contents and services, personal data may be potentially used also in order to “pay” non-digital content and services as well as other goods.



processing “necessary for the performance of a contract to which the data subject is party”.⁵⁷ Accordingly, the collection and use of a consumer’s data would be possible and lawful regardless of his/her consent, and Article 7(4) GDPR (which only applies “where processing is based on consent”) would play no role by determining whether the practice of “paying” with data is legitimate or not.

Such interpretation is not convincing, as Article 6(1)(b) of the GDPR only considers cases in which data processing is necessary for the contractual performance and data is not used for any other purpose. However, this is not the case when a service or a content is supplied against data. As stated above, the trader is only willing to waive payment (in money), if he has the possibility to monetize data, which typically requires the possibility to process it for purposes not necessary to the performance of the contract. Consequently, Article 6(1)(b) of the GDPR does not constitute an appropriate legal basis for the processing of data provided to get content or a service.⁵⁸

The idea that consumers “paying” with personal data need to accept the use of the latter for extracontractual purposes seems also to be confirmed by the wording of Article 3(1) subpara 2 of the DCD [cf. Article 4(2) of the *Omnibus* Directive and the new Article 3(1a) of the CRD]. According to this provision, which clearly wants to address cases where consumers “pay” with their own data, European contract–or, rather, consumer–law does not apply where personal data are exclusively processed by the trader for the purpose of supplying the digital content or digital service in accordance with the Directive (or for allowing the trader to comply with legal requirements to which the trader is subject) and the trader does not process data for any other purpose.⁵⁹

Considering the similarities between the exceptions to the DCD’s scope of application and the legal basis laid down in Article 6(1)(b) and (c) of the GDPR [as well as the limited relevance of those mentioned in Article 6(1)(d) and (e) of the GDPR in the cases under discussion],⁶⁰ providing data in order to get a digital content or service under the European consumer law could be essentially based whether on a trader’s legitimate interest [Article 6(1)(f) of the GDPR] or on the data subjects’ consent [Article 6(1)(a) of the GDPR].

⁵⁷ See (before the GDPR entered into force) P. BRÄUTIGAM, *Das Nutzungsverhältnis bei sozialen Netzwerken – Zivilrechtlicher Austausch von IT-Leistung gegen personenbezogene Daten*, in *MMR*, 2012, 640; T. WEICHERT, *Die Ökonomisierung des Rechts auf informationelle Selbstbestimmung*, in *NJW*, 2001, 1467. Cf. also C. WENDEHORST, *Die Digitalisierung und das BGB*, in *NJW*, 2016, 2612; ID.-F. GRAF VON WESTPHALEN, *Das Verhältnis zwischen Datenschutz-Grundverordnung und das AGB-Recht*, in *NJW*, 2016, 3747.

⁵⁸ Cf. B. SCHMITZ, E. BUSCHUEW, *(Be-)Zahlen mit Daten. Im Spannungsverhältnis zwischen Verbot mit Erlaubnisvorbehalt und Privatautonomie*, in *MMR*, 2022, 172 s.; A. SATTLER, *Autonomy or Heteronomy – Proposal for a Two-Tier Interpretation of Art. 6 GDPR*, in S. LOHSSE, R. SCHULZE, D. STAUDENMAYER (eds.), *Data as Counter-Performance*, cit., 241 s.; E.M. FRENZEL, *Artikel 7*, in B. PAAL-D. PAULY (eds.), *Datenschutz-Grundverordnung*, Beck, 2021, Rz. 20. Additionally, relying on Article 6(1)(b) of the GDPR is not permitted, e.g., in case of some gatekeepers’ data processing activities: see Article 5(2) and Recital no. 36 of the DMA. As regards the legal basis of Article 6(1)(b) of the GDPR, see now CJEU 4 July 2023, C-252/21 – *Meta Platforms and Others*, points 97 ss., 125.

⁵⁹ This is basically what data intermediation service providers only can do according to the DGA: in fact, as stated by Article 12(1)(a) of the DGA, an intermediary “shall not use the data for which it provides data intermediation services for purposes other than to put them at the disposal of data users”.

⁶⁰ A. METZGER, *A Market Model*, cit., 2020, 33; cf. D. STAUDENMAYER, *Article 3*, cit., 73, Rn 60 s. and 64: according to the latter, similarities of the exception in Article 3(1) subpara 2 of the DCD and Article 6(1)(b) and (c) of the GDPR, “are not to be interpreted as references to the legal grounds for processing personal data”. For the possibility of a synchronization between Directive no. 2019/770 and the GDPR based on Article 6(1)(b) of the GDPR, see A. SATTLER, *Autonomy or Heteronomy*, cit., 241 s.: even if “the relationship between Art. 3(1) sentence 2 DSCD and Art. 6(1)(b) is less clear than the respective wording suggests”, “it is unlikely that Art. 6(1)(b) provides an option to synchronize the DSCD and the GDPR”. For a synchronization based on Article 6(1)(f) GDPR, see then pages 242 ss.



However, as there are many cases in which Article 6(1)(f) of the GDPR can also not be considered a suitable basis for data processing,⁶¹ the data subject's consent would often likely be essential for the extracontractual use and, therefore, for the monetization of data, the possibility of which is the requirement that the trader does not want to do without when supplying a content or a service "for free".⁶²

4.3. – From a different point of view, "paying" with one's own data would also be admitted by identifying the basis of processing in the data subject's consent. This would be possible, even though the latter is bundled up as a condition of the contractual performance. To consider the bundled consent freely given in a specific case, it would be only necessary to interpret Article 7(4) of the GDPR differently, trying a relaxation of the ban on tying.⁶³ One could argue, e.g., that the GDPR provision, when interpreted literally, only addresses cases in which the contractual performance and not the conclusion of the contract is conditional on the data subject's consent, which is not necessary for the performance itself. As in many cases in which consumers "pay" with their data, the consent according to Article 6(1)(a) GDPR is essential in order to enter into the contract with the trader (rather than to perform it), Article 7(4) GDPR would therefore not apply to them.⁶⁴

However, also extending the scope of application of Article 7(4) GDPR, affirming its applicability to cases in which the conclusion of the contract is conditional on the data subject's consent, would not prevent the consideration of such contracts in accordance with the GDPR. Whether the connection between contractual conclusion and/or performance and the data subject's consent should be allowed or not would depend, in fact, not only on the link existing between consent and contract, but also on other circumstances:⁶⁵ among others on the data subject's relationship to the other party (see Recital no. 43, sentence 1, of the GDPR)⁶⁶ and on the specific performance to be carried out,⁶⁷ as well as on the possibility of further access to it (see Recital no. 42, sentence 5, of the GDPR).⁶⁸

⁶¹ See above, para 4. See now also C-252/21 – *Meta Platforms and Others*, points 105 ss., 126.

⁶² As highlighted by D. STAUDENMAYER, *Article 3*, cit., 73, Rn. 64; A. METZGER, *A Market Model*, cit., 33.

⁶³ See M. BECKER, *Eine Materialisierung des datenschutzrechtlichen Koppelungsverbots. Zur Regulierung des vertragslosen Tauschs von Daten gegen Leistungen*, in *CR*, 2021, 230 ss.; A. BIJOK, *Kommerzialisierungsfester Datenschutz. Rechtliche Problemlagen der Datennutzung in der Informationswirtschaft*, *Nomos*, 2020, 129 s., 212 ss., 234, 260, 317, 388, 412, 419; A. SATTLER, *Neues EU-Vertragsrecht für digitale Güter – Die Richtlinie (EU) 2019/770 als Herausforderung für das Schuld-, Urheber-, und Datenschutzrecht*, in *CR*, 2020, 152; G. VERSACI, *La contrattualizzazione dei dati personali*, cit., 98 ss. In the sense that Article 7(4) GDPR would even not provide for a prohibition, *i.a.*, F. FAUST, *Ausschließlichkeitsrecht an Daten? In Stiftung Datenschutzrecht, Dateneigentum und Datenhandel*, Erich Schmidt, 2019, 90. Also, according to C. WENDEHORST, *Die Digitalisierung*, cit., 2612, the significance of the ban on tying should be reconsidered.

⁶⁴ Cf. G. RESTA, *I dati personali oggetto del contratto*, cit., 140.

⁶⁵ See e.g. E.M. FRENZEL, *Artikel 7*, cit., Rn. 18.

⁶⁶ The above-mentioned recital contains a reference to an imbalance that would exist, e.g., "in the employment context [...] between the employer and the employee" and "whenever the controller is a public authority": so EDPB Guidelines 05/2020, cit., 7 ss. Cf. E.M. FRENZEL, *Artikel 7*, cit., Rn. 18. An imbalance is also typical for the relationship between a customer and a bank: see, e.g., Cass. 21 October 2019, no. 26778, in *Dir. inf.*, 499 ss. (with the case note by S. THOBANI, *Richieste preventive di consenso al trattamento dei dati: quando la tutela rischia di essere eccessiva*).

⁶⁷ S. THOBANI, *I requisiti del consenso al trattamento dei dati personali*, Maggioli, 2016, 56.

⁶⁸ A. METZGER, *327q BGB*, cit., Rn. 5; K.-U. PLATH, *Artikel 7*, in K.-U. PLATH (ed.), *BDSG/DSGVO*, Otto Schmidt, 2018, Rz. 14; B. STEMME, *Artikel 7 DS-GVO*, cit., Rz. 49.1. See also the Austrian Data Protection Authority 30 November 2018, no. DSB-D122.931/0003-DSB/2018, available at https://www-ris-bka-gv-at.translate.google.com/JudikaturEntscheidung.wxe?Abfrage=Dsk&Dokumentnummer=DSBT_20181130_DSB_D122_931_0003_DSB_2018_00&x_tr_sl=de&x_tr_tl=it&x_tr_hl=it&x_tr_pto=nui



Additionally, in some scholars' opinion, the consent would be freely given and consequently valid— independent of the trader's monopoly position⁶⁹—if the latter makes clear that a contract is going to be concluded between the parties (including the use of data as counter-performance within the purposes for which the data subject's permission is given);⁷⁰ additionally, if the data subject is made aware of the possibility to withdraw the consent already given: the right of withdrawal according to Article 7(3) of the GDPR would, in fact, present the real safeguard of the data subject's freedom of choice in the case of a bundled consent.⁷¹ According to this view, the (weak) ban on tying—if it actually exists—would therefore primarily fulfil a transparency function (*Transparenzfunktion*).⁷²

The idea that the existence of a conditionality does not prevent from affirming the freedom of consent and from considering paying with personal data as legal is also shared by some national courts. For example, in a decision from 2018 the Italian Supreme Court stated that the link established between the contractual performance and the consumer's consent to the processing of his/her data does not hinder the voluntary nature (*i.e.* the freedom) of the latter⁷³. In the case decided by the Italian judges, the access to a newsletter service was conditional on the consent to the use of the consumer's data. Unlike the *Garante della Privacy*⁷⁴, the Court did not consider the circumstance of bundling as an impediment to the validity of the operation, rather focusing on the attributes of the data subject's consent as the prerequisite of a legitimate personal data disclosure. According to the judges, “paying” with (or giving access to) personal data would be allowed, provided that free, informed and specific consent was given by the data subject when concluding the contract. With special regard to the freedom of consent, the latter would not be excluded just because of the tying if the counterparty's performance were fungible (*i.e.* replaceable with an analogous one) and deniable by the data subject (without detriment). In case of a newsletter service, *e.g.*, the user would have the possibility to get the same information through *other* (chargeable) internet sites or newspapers and could therefore deny his/her consent to data processing without suffering any negative effect: hence, the link between such a performance (delivery of news through a newsletter service) and the consent would not automatically lead to an exclusion of the freedom requirement.

The question concerning the interpretation of the so-called *Koppelungsverbot* (*i.e.* the German expression for the ban on tying) was further addressed by the Court of Appeal of Frankfurt am Main,⁷⁵ which eventually shared the view of the Italian judges. However, while the latter decided on a case still covered by the “old” law, the German case fell *ratione temporis* under the GDPR. Nonetheless, the judges did not focus on the interpretation of Article 7(4) of the GDPR, but rather assessed the effects of the conditionality only in the light of the principle of freedom of consent *ex* Article 4(11) of the GDPR [also referring to the rules of Directive

op.elem.sc. (accessed on March 28, 2023): in order to consider the consent as freely given, the data subject should have the possibility to choose between payment of a price in money and “payment” by consenting to data access (*e.g.* for tracking purposes).

⁶⁹ See however A. DE FRANCESCHI, *Digitale Inhalte gegen personenbezogene Daten*, cit., 119. For the question as to whether the application of Article 7(4) of the GDPR also depends on a monopoly position of the data controller or not, B. STEMMER, *Artikel 7*, in H.A. WOLFF-S. BRINK (eds.), *BeckOK Datenschutzrecht*, Beck, 2022, Rn. 46 s.

⁷⁰ C. LANGHANKE, *Daten als Leistung*, cit., 136 s.; M. SCHMIDT-KESSEL, *Consent for the Processing*, cit., 77; ID.-A. GRIMM, *Unentgeltlich oder Entgeltlich?*, in *ZfPW*, 2017, 91.

⁷¹ G. VERSACI, *Consenso al trattamento dei dati personali e dark patterns tra opzionalità e condizionalità*, in *NLCC*, 2022, 1144.

⁷² See Authors in fn. 70 s.

⁷³ Cass. 2 July 2018, no. 17278, in *Giur it*, 2019, 530 ss., with the case note by S. THOBANI, *Operazioni di tying e libertà del consenso*.

⁷⁴ It. Garante della Privacy 25 September 2014, n. 427, available at <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3457687> (accessed on March 28, 2023).

⁷⁵ OLG Frankfurt a.M. 27 June 2019 – Az.: 6 U 6/19, in *BeckRS*, 2019, 17820.



no. 95/46/EC: see Article 2(h)]. They stated in particular that the consent to processing of personal data for advertising purposes may be considered freely given, even if the participation in a lottery is conditional on it. For this purpose, it would be only necessary to ensure that the data subject's consent to the use of data is expressed without pressure (*ohne Zwang*), giving him/her the possibility to refuse or to withdraw the consent, without any prejudice (see Recital no. 42 of the GDPR).

Although the German Court's decision can be understood as a confirmation of the weak character of the bundling prohibition, it does, however, deserve some criticism, as the judges did not explicitly consider Article 7(4) of the GDPR, avoiding taking a position on its role by assessing the freedom of consent, as well as by determining the legality of the widespread practice of "paying" with personal data. A statement on this point would have been desirable, as other authorities still prefer a different, stricter interpretation of the bundling prohibition, which clearly increases the uncertainty on the manner in which the Regulation's disposition should be interpreted.

5. – The opinion on the existence of a weak ban on tying is surely preferable as it does allow better coordination with the existing consumer law provisions and with the needs rising from today's digital and data economy. Moreover, it seems to be in line with the European data protection law and specifically with the *ratio* of the European Regulation, that "adheres to the freedom of contract", considering its "illegality and voidness as the exception" (and not *vice versa*).⁷⁶

Also, the wording of Article 7(4) of the GDPR (cf. Recitals no. 42 and 43) does not allow an argument against the freedom and therefore the validity of the consent just because the access to information and its use is required for (the conclusion of the contract and/or for) the contractual performance. On the contrary, according to the GDPR, there is simply the need to take "utmost account" of the conditioning by determining, whether consent has been freely given or not. As the situation of tying has only to be considered "*inter alia*", the link between consent and contractual performance is therefore only one of the factors that shall be taken into account when deciding about the freedom of the data subject's consent.⁷⁷ Thus, it is not enough to conclude on its invalidity and for the illegitimacy and/or the illegality of contractual operations involving personal data. This is also what those preferring a strict interpretation of Article 7(4) of the GDPR basically admit: by confirming the existence of a strong presumption of the invalidity of the consent tied to the performance of the contract, they cannot deny that there is still a "limited space for cases where [...] conditionality would not render the consent invalid".⁷⁸

One can only ask whether the proof of the possibility for the data subject to get the identical (or at least an equivalent) content or service from the same (or from another) supplier without consenting to data use for additional purposes really represents the only exonerating circumstance for the controller [as regards gate-

⁷⁶M. SCHMIDT-KESSEL, *Right to Withdraw Consent*, cit., 134 ss. See, also for the history of Article 7(4) of the GDPR, G. VERSACI, *La contrattualizzazione dei dati personali*, cit., 98 ss. Further, arguments against the above-mentioned opinion cannot be drawn from the EDPB's statements. In fact, by arguing that "the controller to whom consent has been provided by the data subject to the processing of her or his personal data is not entitled to 'exchange' or 'trade' personal data (as a so-called 'commodity') in a way that would result as not being in accordance with all applicable data protection principles and rules" (EDPB Statement 05/2021, cit., 4), the EDPB left open the possibility that personal data may be exchanged and traded by the controller to whom the data subject gave his/her consent *in a manner that is compliant* with the data protection law.

⁷⁷See also A. METZGER, *A Market Model*, cit., 34.

⁷⁸EDPB Guidelines 05/2020, cit., 11, point 35.



keepers, see, e.g., Recital no. 36 of the DMA];⁷⁹ or whether disclosure of appropriate information about the use of consumers' data [and the possibility of a withdrawal according to Article 7(3) of the GDPR] is enough, including by lack of alternatives, in order to ensure the data subject a genuine and free choice (see Recital no. 42, sentence 5, of the GDPR) and to conclude for the validity of the consent given. Only by opting for the latter interpretation would traders offering services or contents not available otherwise (exclusively) against personal data actually have a possibility to have their business model recognized as GDPR compliant and therefore as legally acceptable, provided they are not subject to stricter provisions⁸⁰ and their users were appropriately informed as to the use and the significance of their data within the specific transaction [also receiving the pre-contractual information according to the CRD as amended by the *Omnibus Directive*].⁸¹

In this regard, it may be incidentally noted that the need to ensure the data subject's capacity for self-determination is crucial whenever personal data enter the market. Such need now additionally receives attention within the latest legislation at European level.⁸² For example, the already mentioned DGA provides for a specific category of neutral data intermediation services, the purpose of which is to grant assistance to data subjects "in exercising their rights under Regulation (EU) 2016/679, in particular giving and withdrawing their consent to data processing". The providers of such services should ensure "that there are no misaligned incentives that encourage individuals to use such services to make more data relating to them available for processing than would be in their interest". They should also advise "individuals on the possible uses of their data (...) making due diligence checks on data users before allowing them to contact data subjects, in order to avoid fraudulent practices" (Recital no. 30; cf. also Recital no. 31). However, as specific provisions concerning personal data should be without prejudice to data protection law, the assistance provided would hardly be considered sufficient to avoid a data breach where the entity actually processing personal data would not be GDPR compliant.

6. – The view which considers conditionality as (only) one of the several circumstances to be considered by assessing the freedom of consent deserves approval. However, the uncertainty that still exists due to the

⁷⁹ It is debated, however, if the consent can be considered as freely given also when a "choice exists between" the controller's "service that includes consenting to the use of personal data for additional purposes on the one hand, and an equivalent service offered by a different controller on the other hand": see (against such possibility) EDPB Guidelines 05/2020, cit., 11, point 38; on the contrary, according to A. METZGER, *327q BGB*, cit., Rn. 5, consent would be free if there were the possibility for the consumer to switch to a paid offer from the same provider or if there were (only) the possibility to gain a comparable services from other providers.

⁸⁰ For gatekeepers and intermediaries, cf. Recital no. 36 of the DMA ("to ensure that gatekeepers do not unfairly undermine the contestability of core platform services, gatekeepers should enable end users to freely choose to opt-in to" certain "data processing and sign-in practices by offering a less personalised but equivalent alternative, and without making the use of the core platform service or certain functionalities thereof conditional upon the end user's consent") and Article 12(a) of the DGA ("the data intermediation services provider shall not use the data for which it provides data intermediation services for purposes other than to put them at the disposal of data users").

⁸¹ See especially Article 6(1)(e) of the CRD. For personal data as counter-performance and to the coordination with the CRD (no. 2011/83), see M. ĐUROVIĆ, *Adaptation of Consumer Law to the Digital Age*, cit., 68; A. DE FRANCESCHI, *Personal Data as Counter-Performance*, in R. SENIGAGLIA, C. IRTI, A. BERNES (eds.), *Privacy and Data Protection in Software Services*, cit., 65; A. ADDANTE, *La circolazione negoziale dei dati personali nei contratti di fornitura di contenuti e servizi digitali*, in *Giust. civ.*, 2020, 912 ss.; G.M. UBERTAZZI, *Models of Information Circulation*, cit., 211 s. Additional information duties are now provided by the *Digital Services Act – DSA* (see in particular Articles 15 and 24 ss.).

⁸² Cf. G. RESTA, *Pubblico, privato, collettivo nel sistema europeo di governo dei dati*, cit., 617 s.



ambiguous formulation of Article 7(4) of the GDPR, the non-binding character of the Regulation's recitals and (consequently) due to the different opinions concerning the facts to be taken into account by assessing the freedom of the (bundled) consent would make a clarifying statement by the European Court of Justice desirable.⁸³

Indeed, the European judges have already taken a stand on some questions concerning the validity requirements of the data subject's consent given in connection with the conclusion and/or the performance of a contract (especially, with a controller using so-called dark patterns).⁸⁴ For example, in *Orange România*, they confirmed the link between transparency and freedom of consent, stating that the latter "cannot be regarded as freely given or, moreover, as having been given in an informed manner" if the contractual terms are misleading as to the possibility of concluding the contract without giving it.⁸⁵ Nevertheless, in the case referred to the Court, the contract was not properly conditional on the consent to the processing of one's personal data, as *Orange România* did not refuse to conclude contracts with those who did not allow the storage of their data.⁸⁶

On the contrary, this appeared to be the case in *Planet49*, where the user's consent to the processing of his/her data for advertising purposes (given by a pre-selected checkbox) was a prerequisite to participate in a promotional lottery.⁸⁷ However, the question of whether a data subject's consent can be tied or not has been left open by the Court, as it was not explicitly referred to.⁸⁸

Finally, the opportunity to address the issue of the validity of a bundled consent has come with the *Meta Platforms* case.⁸⁹ In fact, one of the questions referred for a preliminary ruling also concerns the validity of the consent to the processing of personal data. In particular, the national court is asking whether such consent may be given effectively and freely to an undertaking having a dominant position in the market. As consent to process data (from different sources) appears to be an essential requirement for using the social network operated by the undertaking involved in the specific case, the CJEU will not be exempt from assessing the validity of consent conditional to the conclusion and performance of the contract.⁹⁰ In his (nonbinding) opinion the Advocate General has already suggested an answer to the question referred to the Court, stating that the circumstance of enjoying a dominant position by the recipient cannot, on its own, render the user's consent invalid.⁹¹ The market power of the controller may certainly play a role by assessing the consent's free-

⁸³ This is pointed out also by F. FAUST, *Ausschließlichkeitsrecht an Daten?*, cit., 90.

⁸⁴ For an analysis, see G. VERSACI, *Consenso al trattamento dei dati personali*, cit., 1134 and S. PAGLIANTINI, *L'attuazione minimalista della Dir. 2019/770/UE*, cit., 1501, 1516, 1518 s., 1534. As regards so-called dark patterns, see now Articles 25 and 31 of the *Digital Services Act-DSA*. For a definition, cf. Recital no. 67.

⁸⁵ CJEU 11 November 2020, C-61/19 – *Orange România*, point 41. See the case notes written by C. ANGIOLINI, *A proposito del Caso Orange Romania deciso dalla Corte di Giustizia dell'UE: il rapporto fra contratto e consenso al trattamento dei dati personali*, in *NLCC*, 2021, 247 ss.; T.W. DORNIS, *Sammlung und Aufbewahrung von Ausweiskopien durch TK-Anbieter*, in *GRUR-Prax*, 2020, 625 ss.

⁸⁶ C-61/19 – *Orange România*, point 25.

⁸⁷ CJEU 1 October 2019, C-673/17, *Planet49*. For a case note, see M. OGOREK, *Zustimmung zur Speicherung von Cookies*, in *JA*, 2020, 478 ss. See also the opinion delivered by the Advocate General on 21 March 2019 (point 99).

⁸⁸ See point 64 of the judgment. Instead, the issue was addressed by the Advocate General, who explicitly excluded that the prohibition on bundling has an absolute character (point 98 s. of his opinion).

⁸⁹ C-252/21 – *Meta Platforms and Others*. At the time of writing the case (decided on 4 July 2023) was still pending before the CJEU.

For an analysis of the (German) Facebook case and the interplay between competition law and data protection law, see e.g. W. HERBER, K.K. ZOLNA, *The German Facebook case: the law and economics of the relationship between competition and data protection law*, in *European Journal of Law and Economics*, 2022, 217 ss.

⁹⁰ As highlighted by G. VERSACI, *Consenso al trattamento dei dati personali*, cit., 1148.

⁹¹ See the opinion delivered on 20 September 2022, points 71-77.



dom (which is for the controller to demonstrate). Nevertheless, other factors should be considered as well.⁹² As far as it matters, according to the Advocate General, the ban on tying seems therefore not to be absolute in its nature. Hence, the fact that a consent is the condition to the conclusion of a contract does not prevent it from being regarded as freely given, if other circumstances (examined on a case-by-case basis) allow it. As regards big market players, the question should be now evaluated also considering the latest development in the EU legislation, which provides for stricter requirements for large digital companies, especially for online platforms qualified as “gatekeepers”.

7. – Despite the increasing attention given to the flow of personal data and especially to the phenomenon of supplying personal data in order to obtain content or a service, there are still many questions arising from the use of data instead of money and its exchange on the market that need to be answered. In particular, it is still debated whether personal data can be legitimately considered a tradeable asset or not. In this regard, the relationship between contract and data protection law is to be more precisely defined.

The wording, as well as the *ratio*, of Article 7(4) of the GDPR does not seem to prevent a data subject’s consent from being bundled to the conclusion of a contract and/or to the contractual performance, as is usually the case when (digital) contents, services and (other) goods are supplied against data. Bundling should be taken into account by determining whether the consent can be regarded as freely given or not. However, by evaluating the freedom and therefore the validity of consent other circumstances may and should be considered as well.

As scholars, courts, and national and European authorities still have different opinions not only with regard to the question of whether Article 7(4) of the GDPR provides for a (strict or weak) ban on tying, but also regarding the question of which specific facts must be considered when determining the consent’s freedom and validity (despite the link existing with the contract and the contractual performance), a clarifying statement by the European Court of Justice would be certainly desirable.⁹³

Additionally, as there would still be cases in which conditionality could render the data subject’s consent invalid, there would eventually be a need to confirm the application of the DCD regardless of a GDPR infringement: otherwise, consumers could be deprived from the protection provided therein and traders infringing data protection law could be put in a better position than the ones respecting it.⁹⁴

⁹² Point 77 of the opinion delivered by the Advocate General. In its decision from 4 July 2023, the CJEU answered the question referred to it by ruling “that point (a) of the first subparagraph of Article 6(1) and Article 9(2)(a) of the GDPR must be interpreted as meaning that the fact that the operator of an online social network holds a dominant position on the market for online social networks does not, as such, preclude the users of such a network from being able validly to consent, within the meaning of Article 4(11) of that regulation, to the processing of their personal data by that operator. This is nevertheless an important factor in determining whether the consent was in fact validly and, in particular, freely given, which it is for that operator to prove”.

⁹³ For the role dominance plays by assessing the consent’s validity, see now C-252/21 – *Meta Platforms and Others*, points 140 ss.

⁹⁴ As stated by D. STAUDENMAYER, *Article 3*, cit., 89, Rn. 143 (“the trader who did not respect the GDPR would be in a better position than the trader that respect it”); A. METZGER, *A Market Model*, cit., 33 [“the application of the DCD does not require the consent of the consumer (or data-subject) to be valid under Article 6(1) GDPR” as, “otherwise, the controller would profit from its non-compliance with the conditions of the GDPR”]; ID., § 327 *BGB*, cit., Rn. 18 and 20; cf. § 327q *BGB*, cit., Rn. 3 s.; P. HACKER, *Regulating the Economic Impact*, cit., 48 ss. For the effects of an invalid *privacy* consent, see, from an Italian perspective, S. THOBANI, *Diritti della personalità e contratto*, cit., 198 ss. For some solution proposals, see then G. VERSACI, *La contrattualizzazione dei dati personali*, cit., 177 ss.