

GRANULARITY AND SPECIFICITY OF CONSENT AND IMPLICATIONS THEREOF FOR THE DATA CONTROLLER IN THE LIGHT OF THE PRINCIPLE OF ‘PURPOSE LIMITATION’

Juanita Goicovici*

ABSTRACT

The study discusses the problematics of the granularity and specificity of the data subject’s consent, in the light of the principle of ‘purpose limitation’ when collecting and processing personal data while distinguishing between the imperatives deriving from the principle of purpose limitations (i) from those arising from the incidence of the principle of storage limitations (ii). These issues remain highly important in litigious hypotheses of processing personal data of customers collected and stored unlawfully, including in terms of post-verification of the processing purposes. Secondly, the study focuses on the limits of the purpose limitation principle, set out in Article 5 para. (1), (b) of the GDPR, including bifurcated components: personal data must, on the one hand, be collected for determined, explicit, and legitimate purposes, and, on the other hand, not to be further processed in a manner which becomes incompatible with the initial collecting purposes. We argue that the mentioned principle aims to delimit as clearly as possible the use of personal data by ensuring a balance between respect for the fundamental rights of data subjects in terms of privacy and data protection and the recognition of certain flexibility in favor of the operator in the management of such data, as imposed by digitalization and its inherent risks. In its second component, which is of particular interest to us in the present study, the purpose limitation principle seeks to define the extent to which personal data collected for a particular purpose may be reused by companies, since any processing after collection must be considered as ‘further processing’ and must therefore meet, with certain exceptions, the purpose-compatibility requirements.

KEYWORDS: *specificity of consent, the principle of accountability, granular consent, personal data, purpose limitation, GDPR.*

* Juanita Goicovici, Faculty of Law University Babes-Bolyai of Cluj-Napoca, Cluj-Napoca, Romania; juanita.goicovici@law.ubbcluj.ro.

1. INTRODUCTORY REMARKS

The problematics of the specificity of consent for the processing of consumers' personal data, especially in terms of complying with the granularity rules applicable to the collecting of consumers' consent, continue to generate provocative controversies, mainly from the perspective of detailing the data processing purposes and operations taxonomy for the personal data controller¹. Firstly, the study approaches the limitations related to the sequencing of processing purposes, in situations where the collecting and processing of personal data are based on the existence of consumer consent; the "stratification" of personal data processing purposes, as well as the "stratification" of consent for each type of processing operation represent special requirements arising from the condition of granular consent, implying that consumer's consent requested in general terms will not be valid, "for any personal data processing operation" or the so-called "purposes related to the execution of the contract", without an explicit statement and distinct from each of the data processing purposes (so-called "sequencing of the processing purposes"). Secondly, the granularity rule² is discussed about the exigencies of the principle of 'purpose limitation' when collecting and processing personal data, while distinguishing between the imperatives deriving from the principle of purpose limitations (i) from those arising from the incidence of the principle of storage limitations (ii), including in terms of post-verification of the processing purposes³.

¹ See, for further details, Brunessen, B.: *Protection des données personnelles et nouveaux modes de production du droit*, Bruylant, Bruxelles, 2022, pp. 84-96; Cellina, E.: *La commercialisation des données personnelles. Aspects de droit contractuel et de protection des données*, Schulthess, Geneva, 2020, pp. 37-41; Martial-Braz, N., Rochfeld, J.: *Droit des données personnelles. Les spécificités du droit français au regard du RGPD*, Dalloz, Paris, 2019, pp. 96-102; Mattatia, F.: *RGPD et droit des données personnelles*, 5e édition, Eyrolles, Paris, 2021, pp. 117-121; Maxim, M.: *Răspunderea civilă contractuală în domeniul protecției datelor cu caracter personal în contextul noului Regulament general (UE) privind protecția datelor 2016/679*, Universul Juridic, București, 2021, pp. 323-338.

² Claey's, I., Terryn, E.: *Digital Content and Distance Sales*, Intersentia, Bruxelles, 2017, pp. 92-104; Cremona, E., Laviola, F., Pagnanelli, V. (eds.): *Il valore economico dei dati personali tra diritto pubblico e diritto privato*, Giappichelli Editore, Torino, 2022, p. 117-123.

³ Custers, B., Vrabec, H., Friedewald, M.: *Assessing the Legal and Ethical Impact of Data Reuse*, European Data Protection Law Review 5 (3) 2019, pp. 317-337, DOI: <https://doi.org/10.21552/edpl/2019/3/7>.

Thirdly, the study focuses on the limits of the purpose limitation principle, set out in Article 5 para. (1), (b) of the GDPR, including bifurcated components: personal data must, on the one hand, be collected for determined, explicit, and legitimate purposes, and, on the other hand, not to be further processed in a manner which becomes incompatible with the initial collecting purposes. We argue that the mentioned principle aims to delimit as clearly as possible the use of personal data by ensuring a balance between respect for the fundamental rights of data subjects in terms of privacy and data protection and the recognition of certain flexibility in favor of the operator in the management of such data, as imposed by digitalization and its inherent risks⁴. In its second component, which is of particular interest to us in the present study, the purpose limitation principle seeks to define the extent to which personal data collected for a particular purpose may be reused by companies⁵, since any processing after collection must be considered as ‘further processing’ and must therefore meet, with certain exceptions, the compatibility requirement. The latter reflects the exigencies of a concrete, logical, and sufficiently close link between the purpose of data collection and further processing, requiring that this processing must not be disconnected from or contradict the original purpose of the data collection, and its content must be reconcilable with the rationale of the collection, regardless of any temporality issues. As it has been previously emphasized, the principle of purpose-related limitations is not a mere reflection or an expression of the principle of proportionality, unlike the principle of storage-related limitations set out in Article 5, para. (1), (e) of the GDPR. Particularly, the granularity of data processing agreements⁶

⁴ Haas, G.: *Guide juridique du RGPD. La réglementation sur la protection des données personnelles*, 3e édition, ENI éditions, 2022, pp. 94-102; Desgens-Pasanau, G.: *La protection des données personnelles. Les principales clés de décryptage du RGPD*, 5e édition, LexisNexis, Paris, 2022, pp. 71-83.

⁵ Rabagny-Lagoa, A.: *Fiches de droit du traitement et de la protection des données personnelles*, Ellipses, Paris, 2022, pp. 127-131; Raimondo, L.: *La protection des données personnelles. 100 questions-réponses pour comprendre et mieux se protéger*, Ellipses, Paris, 2021, pp. 67-83; Riccio, G. M., Scorza, G., Belisario, E. (eds.): *GDPR e normativa privacy. Commentato*, Editore IPSOA Gruppo di Wolters Kluwer Italia, 2018, pp. 112-117; Săvescu, A. (ed.): *RGPD – Regulamentul general privind protecția datelor cu caracter personal. Comentarii și explicații*, Hamangiu, Bucharest, 2018, pp. 134-147.

⁶ Alboaic, L.: *Interpretarea principiilor privacy by design în era cloud computing*, Analele Științifice ale Universității „Alexandru Ioan Cuza” din Iași, Seria Științe Juridice, LXIII (2) 2017, pp. 21-32.

requires a separation of information on the data processing agreement for the rest of the information provided to consumers in the pre-contractual stage, as well as the implementation of the opting-in system for requesting consumer consent⁷, since General Regulation (EU) 2016/679 establishes the exigencies for an opting-in system, which excludes the validity of consent⁸ where passive behavior or lack of consumer reaction could be speculated by data controllers in the sense of assuming the consent of the data subject to the collecting and processing of personal data⁹. The absence of the consumer's reaction, as well as the failure to initiate an action on the data subject's part or the simple omission of selecting the options regarding the processing of personal data, do not represent legal grounds for the respective operations, and the consumer's consent, in this case, is practically inexistent. On the other hand, the valid consent expressed for the processing of personal data requires an unambiguous expression of will using an unequivocal statement or a clear affirmative action of the data subject, which implies that the data subject has taken a deliberate action to consent to each type of data processing (tacit or implicit consent based on consumer's silence or inaction of the data subject does not in itself constitute unequivocal consent to personal data collecting and processing). While analyzing the specific conditions for the validity of consent to the processing of personal data, the study aims at potentially answering questions such as: which elements are characteristic for collecting consumer's consent, based on which the free and untainted nature of the consumer's consent

⁷ Dalla Corte, L.: *On proportionality in the data protection jurisprudence of the CJEU*, International Data Privacy Law, 2022. [<https://academic.oup.com/idpl/advance-article-abstract/doi/10.1093/idpl/ipac014/6647961?redirectedFrom=fulltext>], accessed on 28/11/2022, DOI: <https://doi.org/10.1093/idpl/ipac014>; Davies, S.: *The Data Protection Regulation: A Triumph of Pragmatism over Principle?*, European Data Protection Law Review 2 (3) 2016, pp. 290-296, DOI: <https://doi.org/10.21552/EDPL/2016/3/5>; Davola, A.: *Fostering Consumer Protection in the Granular Market: The Role of Rules on Consent, Misrepresentation and Fraud in Regulating Personalized Practices*, Technology and Regulation, Special Issue: Should Data Drive Private Law, 2022, pp. 76-86, [<https://techreg.org/article/view/11177/12407>], accessed on 28/11/2022.

⁸ Kuner, Ch., Bygrave, L. A., Docksey, Ch., Drechsler, L., Tosoni, L. (eds.): *The EU General Data Protection Regulation: A Commentary/Update of Selected Articles*, Oxford University Press, 2021, pp. 45-48, available at SSRN: <https://ssrn.com/abstract=3839645> and <http://dx.doi.org/10.2139/ssrn.3839645>, accessed on 19/01/2023.

⁹ Böröcz, I.: *Risk to the Right to the Protection of Personal Data: An Analysis Through the Lenses of Hermagoras*, European Data Protection Law Review 2 (4) 2016, pp. 467-480, DOI: <https://doi.org/10.21552/EDPL/2016/4/6>.

to the processing of personal data by trade and service professionals in B2C contracts can be estimated? Are the provisions of Article 4, 11th par. of General Regulation (EU) 2016/679 sufficient for such elements to be deduced?

Particularly, it can be argued that: (a) consumer's freedom to opt for choosing or refusing¹⁰ the collecting and processing of personal data implies the controller's respecting of the real choice prerogatives¹¹ and the possibility of exercising real control by data subjects over the collected data (since the data subject's consent may be discretionarily withdrawn¹²; (b) in cases where the data subject does not benefit from a real choice or feels constrained to accept to the data processing by the controller or there is a fear that the data subject will suffer negative consequences should the latter refuse the data processing¹³, the consent will not be validly expressed; similarly, a 'blank' acceptance of the general terms and conditions cannot be seen as a clear affirmative action of consenting to the use of personal data¹⁴; (c) the provisions of General Regulation (EU) 2016/679 do not allow personal data controllers to provide pre-checked boxes or methods such as self-exclusion or 'voluntary exclusion' of consumers from the processing of personal data (opting-out consent), while prohibiting the means of presuming the existence of data subject's tacit consent, which require an intervention by the data subject to refuse the agreement (opt-out boxes) and

¹⁰ Dobrilă, M.-C.: *Aspecte teoretice și jurisprudențiale privind respectarea GDPR la încheierea și executarea unui contract*, Analele Științifice ale Universității „Alexandru Ioan Cuza” din Iași, Seria Științe Juridice, vol. LXVII, Supliment 2, 2021, pp. 93-106; Dobrilă, M.-C.: *Particularități privind noțiunea de date cu caracter personal necesare pentru încheierea sau executarea unui contract la care persoana vizată este parte*, Analele Științifice ale Universității „Alexandru Ioan Cuza” din Iași, Seria Științe Juridice, vol. LXVII, Supliment, 2021, pp. 211-225, DOI: <https://doi.org/10.47743/jss-2021-67-3-15>.

¹¹ Bercea, L.: *Standardul „consumatorului mediu” și consimțământul pentru prelucrarea datelor cu caracter personal*, Revista Română de Drept Privat (1) 2018, pp. 26-51.

¹² Netter, E.: *Regards sur le nouveau droit des données personnelles*, Éditions du Centre de droit privé et de sciences criminelles d'Amiens, Amiens, 2019, pp. 41-49; Ploeșteanu, N.-D., Lăcătușu, V., Farcaș, D.: *Protecția datelor cu caracter personal și viața privată – Jurisprudența CEDO și CJUE*, Universul Juridic, Bucharest, 2018, pp. 112-119.

¹³ Caravă, E.: *Personal Data Kept in Companies Registers: The Denial of the 'Right to be Forgotten'*, European Data Protection Law Review 3 (2) 2017, pp. 287-292, DOI: <https://doi.org/10.21552/edpl/2017/2/26>.

¹⁴ Van Alsenoy, B.: *Data Protection Law in the EU: Roles, Responsibilities and Liability*, Intersentia, Bruxelles, 2019, pp. 128-136.

which rely on the silence or data subject's passivity / non-assertively acceptance¹⁵.

Finally, the study emphasizes the fact that there is no perfect synonymy between the 'granularity' of the processing purposes rule and the principle of 'specificity' of consent to the processing of personal data. Certainly, the condition of the specificity of the data subject's consent¹⁶ cannot be understood in the absence of an analysis of the notion of 'granularity' of consent, which significantly enhances the significance of the first. Yet, are they synonymous, or do the two phrases cover distinct, autonomous, and conjugately applicable conditions in assessing the validity of the consumer's consent to the processing of personal data? We argue that the answer to the question in the final section can only be negative. Without being synonymous, the two expressions cover two distinct attributes that the consent required of the consumer to process personal data must meet. The specificity of consent¹⁷ is the opposite of generalizing or admitting as valid the consent to the processing of personal data for unspecified purposes (i), while the granularity of consent implies that data subjects have the freedom to choose the purpose they accept, without being forced to accept the 'full package' of purposes for the data processing and to be able to exclude some of these purposes (ii). Moreover, in hypotheses in which the procedure for obtaining

¹⁵ Drexler, J.: *Data Access and Control in the Era of Connected Devices. Study on Behalf of the European Consumer Organisation BEUC*, The European Consumer Organisation – Bureau Européen des Unions de Consommateurs (BEUC), Bruxelles, 2018, [https://www.beuc.eu/publications/beuc-x-2018-121_data_access_and_control_in_the_area_of_connected_devices.pdf], accessed on 28/11/2022; Duivenvoorde, B.: *The Liability of Online Marketplaces under the Unfair Commercial Practices Directive, the E-commerce Directive and the Digital Services Act*, Journal of European Consumer and Market Law 11 (2) 2022, pp. 43-52, [https://kluwerlawonline.com/journalarticle/Journal+of+European+Consumer+and+Market+Law/11.2/EuCML2022009], accessed on 28/11/2022.

¹⁶ Chiara, P.: *The Balance Between Security, Privacy and Data Protection in IoT Data Sharing*, European Data Protection Law Review 7 (1) 2021, pp. 18-30, DOI: https://doi.org/10.21552/edpl/2021/1/6.

¹⁷ Goicovici, J.: *Consimțământul consumatorului la prelucrarea datelor personale în contractele business to consumer – condiția consimțământului granular*, Analele Universității de Vest din Timișoara, Seria Drept (2) 2019, pp. 7-24; Goicovici, J.: *Portabilitatea datelor cu caracter personal, prin prisma dispozițiilor RGDP și ale Directivei 2019/770: este gambitul reginei mutarea de deschidere adecvată?*, Analele Științifice ale Universității „Alexandru Ioan Cuza” din Iași, Seria Științe Juridice, Vol. LXVII, Supliment 2, 2021, pp. 57-80; Goicovici, J.: *Clauzele privind drepturile consumatorilor în contractele de servicii cloud computing*, Revista Română de Drept Privat (2) 2019, pp. 399-415.

consent does not allow the data subjects to give separate consent for the various personal data processing operations or different purposes of the processing, the very requirement of freely expressed consent would be seriously affected, due to the element of constraint which becomes present in such hypotheses¹⁸. As a corollary of the freedom of consent and the specificity of the data subject's consent¹⁹, the granular nature of consent is seen an important condition²⁰ when processing personal data for multiple purposes, requiring the solution to meet the conditions of validity of consent in terms of respecting the granularity of consumer's agreement and obtaining separate consent, for each of the processing purposes panoply mentioned by the data controller²¹.

2. DATA CONTROLLER'S INFORMATIVE TASKS TOWARD CONSUMERS

2.1. COLLECTING CONSENT FOR MULTIPLE PURPOSES OF PERSONAL DATA PROCESSING

In terms of establishing the consumer's capacity to adequately understand the multiple purposes of personal data processing²², it should be emphasized that, as resulting from the CJEU's decision from November 11, 2020, in case C-61/19²³, the data controller must demonstrate that

¹⁸ Enzmann, M., Selzer, A., Spychalski, D.: *Practitioner's Corner – Data Erasure under the GDPR – Steps towards Compliance*, European Data Protection Law Review 5 (3) 2019, pp. 416-420, DOI: <https://doi.org/10.21552/edpl/2019/3/17>.

¹⁹ *Ibidem*.

²⁰ *Idem*, p. 418.

²¹ van Eijk, N., Hoofnagle, J. C., Kanekens, E., *Unfair Commercial Practices: A Complementary Approach to Privacy Protection*, European Data Protection Law Review 3 (3) 2017, pp. 325-337, DOI: <https://doi.org/10.21552/edpl/2017/3/7>.

²² Dimitrova, D.: *The Right to Explanation under the Right of Access to Personal Data*, European Data Protection Law Review 6 (2) 2020, pp. 211-230, DOI: <https://doi.org/10.21552/edpl/2020/2/8>.

²³ In case C-61/19, it has been retained that “A contract for the provision of telecommunications services which contains a clause stating that the data subject has been informed of, and has consented to, the collection and storage of a copy of his or her identity document for identification purposes is not such as to demonstrate that that person has validly given his or her consent, as provided for in those provisions, to that collection and storage, where: – the box referring to that clause has been ticked by the data controller before the contract was signed, or where:

“the data subject has, by active behavior, given his or her consent to the processing of his or her personal data and that he or she has obtained, beforehand, information relating to all the circumstances surrounding that processing, in an intelligible and easily accessible form, using clear and plain language, allowing that person easily to understand the consequences of that consent, so that it is given with full knowledge of the facts.”

Nevertheless, it should be emphasized that, as regards, more specifically, the adequacy of the collecting of the data subject’s consent, especially in terms of avoiding (by design) any potential opacity when enunciating the purposes of data storage and processing, the data subject must have ‘unambiguously’ given his or her consent, which implies that the controller bears the burden of proof relating to the existence of valid consent, namely in hypotheses where personal data processing is based on consent, and that controller must be able to demonstrate that the data subject has consented to the processing of his or her data.

In the mentioned case, it resulted that during the procedure for concluding the contracts at issue in the main proceedings, the data controller’s sales agents did not inform the customers concerned, before concluding the contracts, on each of the purposes of collecting and storing copies of the identity documents and their choice as to that collection and storage, before obtaining their consent to that collection and storage operations. As a factual element, it has been retained that the box relating to the storage of copies of identity documents was pre-ticked by the company’s representatives solely based on a so-called ‘presumed consent’ of the individuals in terms of agreeing to the so-called ‘implied purposes’ of data storage, such as the storage of personal data to further enforce

– the terms of that contract can be misleading for the data subject as to the possibility of concluding the contract in question even if he or she refuses to consent to the processing of his or her data, or where:

– the freedom to choose to object to that collection and storage is unduly affected by that controller, in requiring that the data subject, in order to refuse consent, must complete an additional form setting out that refusal.”; the text of the CJEU’s decision in case 61/19 is available at <https://curia.europa.eu/juris/document/document.jsf?text=&docid=233544&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=23109>, accessed on 29/11/2022. The main problematics, in the mentioned case, were centered not on the ‘granularity of consent’ principle, but rather on the issue of the necessity of an assertive acceptance (through the mechanisms of an opting-in consent) from the data subject regarding the collecting and processing of specific personal data.

the creditor's rights against the debtor in the eventuality of payment unjustified delays²⁴.

On the other side of the discussion, in situations where the processing of the consumer's personal data is aimed at direct marketing, the data subject has the right to object at any time to the processing for this purpose of the personal data concerning the data subject, including the creation of profiles, insofar as it is related to direct marketing operations²⁵. We note that, if the consumer objects to the processing for the purpose of direct marketing, the personal data can no longer be processed for this purpose²⁶. As it has been accurately emphasized, in the cases where the processing of personal data for direct marketing purposes is mentioned in a standard clause, to the extent that this type of clause directly relates the conclusion of the contract on the expressing of consent to the future permission to use personal data to put in practice several marketing techniques directed at the targeted person, then such a clause must be considered invalid, which represents a solution justifiable through the probable lack of transparency²⁷ and the creation of an immediate imbalance between the rights and obligations of the parties, to the detriment of the consumer.

The adequacy of granular consent remains crucial for the validity of consumer consent, as the data operator / authorized representative of the data controller, the company's agents must ensure that they offer the data subjects, in the informative message presented at the time of col-

²⁴ For further analyses on the ethical reverberations, see Hijmans, H.: *How to Enforce the GDPR in a Strategic, Consistent and Ethical Manner?*, European Data Protection Law Review 4 (1) 2018, pp. 80-84, DOI: <https://doi.org/10.21552/edpl/2018/1/10>.

²⁵ de Hert, P., Lazcoz, G.: *When GDPR Principles Blind Each Other: Accountability, Not Transparency, at the Heart of Algorithmic Governance*, European Data Protection Law Review 8 (1) 2022, pp. 31-40, DOI: <https://doi.org/10.21552/edpl/2022/1/7>; de Hert, P., Papakonstantinou, V., Malgieri, G., Beslay, L., Sanchez, I.: *The Right to Data Portability in the GDPR: Towards User-Centric Interoperability of Digital Services*, Computer Law & Security Review, 2018, [<https://www.sciencedirect.com/science/article/pii/S0267364917303333>], accessed on 29/11/2022.

²⁶ Graef, I., Clifford, D., Valcke, P.: *Fairness and Enforcement: Bridging Competition, Data Protection and Consumer Law*, International Data Privacy Law 8 (3) 2018; Hahn, I.: *Purpose Limitation in the Time of Data Power: Is There a Way Forward?*, European Data Protection Law Review 7 (1) 2021, pp. 31-44, DOI: <https://doi.org/10.21552/edpl/2021/1/7>.

²⁷ Voigt, P., von dem Bussche, A.: *The EU General Data Protection Regulation (GDPR): A Practical Guide*, Springer International Publishing, 2017, pp. 56-59, DOI: <https://doi.org/10.1007/978-3-319-57959-7>.

lecting their personal data, a distinctive, punctual and sequential review of the purposes for which each category of personal data is collected (i) and that the purpose/purposes for which the data were initially collected will not be altered, nor expanded at a later moment, without the prior information of the concerned data subjects and without going through all the transitional steps necessary to obtain the consent of the consumer, when appropriate.

In terms of establishing the existence of company's liability, consumers' consent represents one of the six grounds of legality on which the processing of personal data can be based, as these grounds are listed in Article 6 of Regulation (EU) 2016/679 (the other five possible grounds referring to: (b) the processing necessary for the execution of a contract to which the data subject is a party or to take steps at the request of the data subject before concluding a contract; (c) the processing necessary to fulfill a legal obligation incumbent on the operator; (d) the processing necessary to protect the vital interests of the data subject or another natural person; (e) the processing necessary to fulfill a task that serves a public interest or that results from the exercise of the public authority with which the operator is vested; (f) the processing necessary for the purpose of the legitimate interests pursued by the operator or a third party, except in the case where the interests or fundamental rights and freedoms of the data subject prevail).

To the extent that they initiate activities or operations that involve the processing of personal data, the company, in its capacity of the data controller, must always evaluate to what extent the consent of the data subject (regardless of their consumer status) represents or not the appropriate legal basis for the processing of the collected personal data; otherwise, it is necessary to identify another legal basis. As pointed out, in business-to-consumer contracts, the consumer's consent can represent the appropriate legal basis only in situations where the data subject has been given control and the possibility of a real and effective choice between accepting or rejecting the terms conferred by the data operator²⁸.

²⁸ Kaiser E.: *The Concept of 'Freely Given, Specific and Informed' Consent under the Scrutiny of the European Court of Justice*, *European Data Protection Law Review*, Vol. 6, Issue 4 (2020), pp. 607-610, DOI: <https://doi.org/10.21552/edpl/2020/4/19>.

2.2. REVERBERATIONS OF THE 'PURPOSE-LIMITATION' PRINCIPLE

Defined in Article 5(1)(b) of the General Data Protection Regulation (GDPR), the 'purpose-limitation'²⁹ is notably seen as being the second principle related to the processing of personal data, which finds its normative expression³⁰ in the data subject's right to be properly and non-evasively informed on the multitude of purposes regarding the data collecting and processing. Moreover, the purpose-limitation meta-rule relates closely to the first principle of data protection, which relates to the lawfulness, fairness,³¹ and transparency³² of data collecting and processing and which requires that, fundamentally, a specific and legitimate reason is needed for any personal data that is collected based on the data subject's consent, since the personal data can only be used for the specified reasons³³ (obviously, exceptions could be made if further processing is meant for purposes such as archiving in the public interest, scientific or historical research, statistical reasons implying anonymized data, yet not implying pseudonymized data, which still permit individual traceability).

In the perimeter of establishing companies' liability for improper sequencing of personal data processing purposes, the concept of functional separation of processing purposes is likely to play a key role, and the extent to which this may be achieved could be an important

²⁹ Jasserand, C.: *Subsequent Use of GDPR Data for a Law Enforcement Purpose: The Forgotten Principle of Purpose Limitation?*, European Data Protection Law Review 4 (2) 2018, pp. 152-167, DOI: <https://doi.org/10.21552/edpl/2018/2/6>.

³⁰ *Ibidem*.

³¹ Jarovsky, L.: *Improving Consent in Information Privacy through Autonomy-Preserving Protective Measures (APPMs)*, European Data Protection Law Review 4 (4) 2018, pp. 447-458, DOI: <https://doi.org/10.21552/edpl/2018/4/7>; Jasmontaite, L., Kamara, I., Zanfir-Fortuna, G., Leucci, S.: *Data Protection by Design and by Default: Framing Guiding Principles into Legal Obligations in the GDPR*, European Data Protection Law Review 4 (2) 2018, pp. 168-189, DOI: <https://doi.org/10.21552/edpl/2018/2/7>.

³² Hinsch, W.: *Differences That Make a Difference: Computational Profiling and Fairness to Individuals*, in Voeneky, S., Kellmeyer, P., Mueller, O., Burgard, W. (Eds.): *The Cambridge Handbook of Responsible Artificial Intelligence: Interdisciplinary Perspectives*, Cambridge University Press, Cambridge, 2022, pp. 229-251, DOI:10.1017/9781009207898.019.

³³ Jabłonowska A.: *Consumer Protection in the Age of Data-Driven Behaviour Modification*, Journal of European Consumer and Market Law 11 (2) 2022, pp. 67-71, [<https://kluwer-lawonline.com/journalarticle/Journal+of+European+Consumer+and+Market+Law/11.2/EuC-ML2022012>], accessed on 29.11.2022.

factor in deciding whether further use of the data for (marketing or another purpose) research can be considered compatible. In these cases, data controllers need to guarantee the confidentiality and security of the data and take all necessary technical and organizational measures to ensure functional separation of processing purposes and to transparently inform the consumer of the existence of these purposes before the consenting.

The second potential set of reverberations arises from the data controller specifically wanting to extrapolate initial data processing purposes to further processing such as personalized marketing-oriented profiling techniques, which analyze or predict the personal preferences, behavior, and attitudes of individual customers, and which will subsequently motivate marketing strategies and personalized pricing³⁴ decisions that are taken concerning those consumers.

Especially, in these cases, namely in the hypotheses of intending to expand the initial purposes of data collecting as to comprise the profiling operations, there is a crucial need for respecting the free, specific, informed, and unambiguous opting-in consumer consent, which would almost always be required, otherwise further expanded use of personal data (initially collected for limited purposes) cannot be considered compatible with the ‘purpose-limitations’ principle. Importantly, such opting-in consent remains required for tracking and profiling for purposes of direct marketing, including the use of behavioral advertisement techniques, data-brokering, location-based advertising, or tracking-based digital market research, which all require explicit, granularly-given consent from the data subjects upon transparent informing on the existence of the multi-layered processing purposes³⁵. Avoidance of oversimplification and the adding of sufficient granularity will be needed³⁶ to ensure that all the different data-processing purposes are sufficiently

³⁴ Li, Z.: *Affinity-Based Algorithmic Pricing: A Dilemma for EU Data Protection Law*, Computer Law & Security Review, Vol. 46 (2022), [<https://ssrn.com/abstract=4144571>] and [<https://www.sciencedirect.com/science/article/pii/S0267364922000528>], accessed on 28.11.2022; Wachter, S., Mittelstadt, B.: *A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI*, Columbia Business Law Review (2) 2019, [<https://ssrn.com/abstract=3248829>], accessed on 28/11/2022.

³⁵ Veale, M., Nouwens, M., Santos, C.: *Impossible Asks: Can the Transparency and Consent Framework Ever Authorise Real-Time Bidding After the Belgian DPA Decision?*, Technology and Regulation, 2022, DOI: <https://doi.org/10.26116/techreg.2022.002>.

³⁶ *Ibidem*.

transparent³⁷ for the consumers, while renouncing the opaque and evasive enouncing of these purposes, which risk to be unintelligible to the data subjects, especially when the data controller intends to expand the initial substantial sphere of the data-collecting purposes³⁸.

2.3. CONSUMER'S OPTIONAL RIGHT OF WITHDRAWAL

The rules enounced in Regulation (EU) no. 679 of April 27, 2016, on the protection of natural persons concerning the processing of personal data, which regulates the civil liability of personal data operators and their representatives, do not remove the incidence of the provisions of national law on civil liability for the damage caused to data subjects, while not having an evasive effect on the rules of domestic law regarding civil liability³⁹, which represents an aspect that is also reiterated in the text of recital (146) of the GDPR. It is worth noticing, in this context, that the rules of Regulation (EU) 2016/679 generate a dual effect, both horizontally applicable since these rules can be invoked by the concerned data subjects directly against other natural/legal persons, as well as a vertical effect, arising from the prioritized application of the General Regulation on the processing of personal data.

The company's liability may also be retained for ignoring of the consumer's optional right to withdraw the consent to data processing. The consent issued by the consumer for processing his or her personal data can be withdrawn at any time, without the possibility of applying penalties, without further sanctions, in a non-onerous and discretionary manner, and without limits regarding the reasons for withdrawal. Generally, the exercise of the right to consent withdrawal must be engaged in a similarly facile manner as that in which its consent was requested by the data controller. Nonetheless, the withdrawal of consent regarding the processing of personal data can, in turn, be sequential, the consumer's withdrawal being able to target one or more of the processing purpos-

³⁷ *Ibidem.*

³⁸ Viterbo, F. G.: *The 'User-Centric' and 'Tailor-Made' Approach of the GDPR Through the Principles It Lays down*, *The Italian Law Journal* 5 (2) 2019, pp. 631-672.

³⁹ Karjalainen, T.: *All Talk, No Action? The Effect of the GDPR Accountability Principle on the EU Data Protection Paradigm*, *European Data Protection Law Review* 8 (1) 2022, pp. 19-30; Koch, B. A.: *Liability for Emerging Digital Technologies: An Overview*, *Journal of European Tort Law* 11 (2) 2020, pp. 115-136, DOI: <https://doi.org/10.1515/jetl-2020-0137>.

es stated initially, with the maintenance of consent for one or more of these purposes, depending on the consumer's decision.

3. FEATURES OF COLLECTING SEQUENTIAL CONSENT

3.1. CONSUMER'S CONSENT TO THE AUTOMATED PROCESSING OF PERSONAL DATA AND AUTOMATIC PROFILING

The right of the data subject to oppose the automated processing of personal data and automatic profiling⁴⁰ is stated in Article 22, 1st para. of Regulation (EU) 2016/679, as being a response of the European legislator to the dangers that may result for the person whose personal data have been collected, from the provoking aspects of traceability of automated decision-making (ADM) and of processing personal data in order to implement ADM techniques. Significantly relevant in this context remains the explanation provided in Recital (71) GDPR, which mentions the data subject's right to oppose an automated decision, when it produces legal effects that concern the data subject or similarly affects his or her legitimate expectations of a significant extent.

As highlighted in the specialized literature⁴¹, the need for specific consent for the processing of personal data, in conjunction with the notion of 'limitation of the purpose of processing' provided for in art. 5, 1st para. (b) of Regulation (EU) 2016/679 functions as a genuine guarantee against attempts to gradually increase the categories of operations involved in data processing or to significantly blur the clarity of the purposes for which the collected personal data are processed, after the moment when the data subject agreed with the initial collection of data and with their processing for certain previous purposes which were clearly mentioned by the data operator. Obviously, the phenomenon described, also known under the name of 'distortion of the processing function', presents significant risks for the persons concerned, as it can lead to the use of personal data by the operator that could not be anticipated by the consumer or to the use of

⁴⁰ Gräf, E.: *When Automated Profiling Threatens Our Freedom*, European Data Protection Law Review 3 (4) 2017, pp. 441-451, DOI: <https://doi.org/10.21552/edpl/2017/4/6>; Spiecker Genannt Döhmman, I., Tambou, O., Bernal, P., Hu, M., Molinaro, C. *et al.*: *Multi-Country – The Regulation of Commercial Profiling – A Comparative Analysis*, European Data Protection Law Review 2 (4) 2016, pp. 535-554, DOI: <https://doi.org/10.21552/EDPL/2016/4/12>.

⁴¹ Karjalainen, T., *op. cit.*, p. 29.

personal data by third parties for purposes that were not initially consented to and, therefore, to the loss or significant reduction of control of the data subjects over the processing of personal data.

Similarly, it is worth noticing, as already mentioned in the previous sections, that there is no perfect synonymy between the ‘granularity’ of processing purposes and the ‘specificity’ of consent to the processing of personal data. Notably, the condition of the specificity of the consent of the person concerned cannot be fully understood in the absence of the notion of ‘granularity’ of consent, which significantly enhances the meanings of the firstly mentioned meta-rule. Yet, the two expressions cover two distinct attributes that the consumer’s consent to the processing of personal data must cover; moreover, the specificity of consent is antonymic to the generalization of processing purposes or to the considering of the consumer’s acceptance as validated as consent regarding the processing of personal data for unspecified purposes. Nevertheless, while the granularity of consent implies that data subjects have the freedom to choose the purpose they accept, without being forced to accept non-stratified processing purposes or to consent to a package of processing purposes and to be able to exclude some or others of these purposes, the procedure for obtaining consumer’s consent at the pre-contractual stage must allow the data subjects to grant separate consent for the various personal data processing operations or the various purposes of the personal data processing.

Moreover, if a data operator seeks to initiate personal data processing operations that are necessary for the execution of the contract itself, it is most likely that the legal basis for this processing is represented by the provisions of art. 6, 1st para. (b) of Regulation (EU) 2016/679 (execution of the contract as the basis of personal data processing, and not the consumer’s consent). In this case, it is obvious that, for the data operator⁴², it is not necessary (nor possible) to use another legal basis, such as the consent of the person concerned⁴³, since there is already a legal basis for the processing of personal data⁴⁴, namely the contract whose execution requires the processing of the respective personal data⁴⁵.

⁴² Viterbo, F. G., *op. cit.*, p. 632.

⁴³ See, for further details, Goicovici, J.: *Consimțământul consumatorului la prelucrarea datelor personale (...)*, *cit. supra*, pp. 21-22.

⁴⁴ *Idem*, p. 19.

⁴⁵ *Idem*, p. 23.

3.2. CONSUMER'S FREELY EXPRESSED CONSENT AND ASSUMPTIONS OF COERCION

In cases in which the consumer feels compelled to accept several purposes selected by the data controller for justifying the personal data collecting and further processing, the very requirement of freely expressed consent is seriously affected, due to the element of coercion present in such assumptions. As a corollary of the freedom of consent and the specificity of the consent of the data subject, the granular nature of the consent remains a necessary condition when the processing of personal data aims at multiple purposes since the solution to fulfill the conditions of the validity of the consent consists in the granularity of the consent of the consumer, namely in the separation of these purposes from those which remain unselected by the data operator when obtaining separate consent, for each of the data processing purposes. As follows from Recital (47) of Regulation (EU) 2016/679, the legitimate interests of a personal data operator, including those of a data controller to whom the personal data may be disclosed or of a third party, may constitute a basis legal for the processing of this data (yet not in the absence of a clear action by the consumer in the sense of consent to the processing), provided that it selects the situations where the interests or the fundamental rights and freedoms of the person concerned do not prevail over the interest of the operator; the latter aspect will be evaluated, as follows from Recital 47, the second thesis, of the General Regulation on the protection of personal data, taking into account the reasonable expectations of the data subjects based on their relationship with the data controller. This legitimate interest could exist, for example, as the European legislator specifies in the text of the cited recital when there is a relevant and appropriate relationship between the data subject and the data controller, such as in the case where the data subject is a customer of the data operator (a consumer of services or products marketed by the data controller in a B2C contractual context). However, the existence of a legitimate interest of the data operator that makes the request for the consumer's consent dispensable would require a careful assessment, which also establishes whether a data subject can reasonably expect, at the time and in the context of the collection of personal data, that the collected personal data will be processed for that respective purpose (personalized marketing strategies, for example) by the data operator.

Is it possible for the data controller to rely on distinct and multiple legal grounds to justify the processing of personal data collected from consumers of services and/or products if the processing of the data in question takes place for multiple purposes? In our opinion, the answer to this question is affirmative, given that each purpose of the processing must be supported by a legal basis. However, as pointed out in the previous section, the data operator must identify these purposes and related legal bases before starting the processing of personal data, and not afterward. Moreover, it is worth mentioning that the legal basis for processing personal data cannot be changed during these later-on strategized processing operations. Consequently, after data collection and processing has been initiated, the operator cannot ‘switch’ from one legal basis of processing to another. For example, the retroactive use of the legitimate interest by a personal data operator to justify the processing of these data is not allowed, in cases where problems have been encountered regarding the validity of the data subject’s consent. Therefore, under the rules set out by the provisions of art. 5, 1st para. and of art. 6, 1st para. of Regulation (EU) 2016/679, generally data controllers who request the consent of the persons concerned for the processing of personal data, should not be able to rely on another legal basis for processing from those mentioned in art. 6 of the General Regulation, as a back-up plan when they cannot demonstrate the validity of the consent of the concerned person or if his/her valid consent was subsequently withdrawn. Given the obligation to disclose the legal grounds on which the operator acts at the time when personal data is collected, the company must decide before the initiation of data collection⁴⁶, which are the legal grounds applicable to each of the purposes of personal data processing⁴⁷ and, should the data controller intend a later-on envisaged expansion of the initially-selected categories of processing purposes, based on consumer’s consent⁴⁸, the further requesting of consumer’s specific (granular) consent remains essential⁴⁹.

Especially relevant in contracts from the business-to-consumer category remains the fact that the personal data operator can base its processing operations on the provisions of art. 6 1st para. (b) GDPR to process

⁴⁶ *Idem*, p. 18.

⁴⁷ *Ibidem*.

⁴⁸ *Ibidem*.

⁴⁹ *Idem*, p. 20.

personal data when, according to the obligations of responsibility under art. 5 2nd para., the company may establish that the processing takes place in the context of a valid contract concluded with the data subject (i) and that the processing is necessary to execute that contract with the data subject (ii). If the data operators cannot demonstrate: (a) the existence of the contract, (b) the fact that the said contract is valid and concluded according to the applicable national law in the field of contracts and (c) the fact that the processing of the contractual partner's personal data is objectively necessary for the execution of the contract, the data operator will have to consider another legal basis for data processing. It is also highlighted that the simple reference or mention regarding data processing inserted by trade/service professionals in a B2C adhesion contract is not *per se* sufficient to consider the said data processing as falling within the scope of the provisions of art. 6, 1st (b) of the GDPR. It should also be emphasized that the processing of personal data may be objectively necessary even if it is not specifically mentioned in the respective contract, yet the data operator must fulfill its obligations arising from the principle of transparency of personal data processing. From this point of view, in situations where a personal data operator aims to invoke the fact that the processing of this data is based on the execution of a B2C contract concluded with the data subject, it is important to evaluate the various nuances of what represents, in that respective context, the so-called 'necessary objective for the execution of the contract'. The phrase 'processing necessary for the execution of the contract', from the perspective of the substantial applicability of the provisions of art. 7, 4th para. Of the GDPR, which concerns the validity of the data subject's consent, it is necessary to make an explicit distinction between the processing activities necessary for the execution of a contract (i) and the clauses that address the provisions on the contractual performance and to the consumer's consent to the entering into the paradigm of certain data-processing activities which are not actually necessary for the performing of the business-to-consumer contract (ii).

Guided by the premise of an asymmetric distribution of control over the information necessary to issue a free and unadulterated consent, the mechanism provided for in the General Regulation on the protection of personal data for the granular collection of the data subject's consent is based on the need for transparency felt by the data subjects at the time of the collecting of these data. The specific requirements arising for personal data operators from the perspective of detailing the

collection purposes and the stratification of the operations involved in the processing of consumers' personal data continue to raise questions for legal practitioners, especially if the processing of personal data is based on the consent of the consumer since the data operator must be able to demonstrate that the data subject has given specific consent for the multifaceted processing of personal data. The granular consent requirement implies, among other aspects, that, if the consumer's consent to the processing of his/her personal data is given in the context of a statement that also refers to other contractual aspects, the consent request must be presented in a form that differentiates it clearly from the other legal aspects, in a form intelligible to the consumer, while using clear language, and avoiding excessively technical terms which would be considered opaque by the uninstructed consumer.

4. CONCLUDING REMARKS

To conclude, it must be emphasized that, certainly, when establishing the existence of a company's liability for the opaque selecting of personal data processing purposes, the condition of the specificity of the data subject's consent cannot be understood in the absence of an analysis on the notion of 'granularity' of consent, which significantly enhances the meanings of the first. Yet, are they synonymous or do the two phrases cover distinct, autonomous, and conjugately applicable conditions in assessing the validity of the consumer's consent to the processing of personal data? We argue that the answer to the question in the final section can only be negative. Without being synonymous, the two expressions cover two distinct attributes that the consent required of the consumer to process personal data must meet.

The specificity of consent is the opposite of generalizing or admitting as valid the consent to the processing of personal data for unspecified purposes (i), while the granularity of consent implies that data subjects have the freedom to choose the purpose they accept, without being forced to accept the 'full package' of purposes for the data processing and to be able to exclude some of these purposes (ii).

The granularity of data processing agreements and the separation of information regarding the data processing agreement from the rest of the information provided remain crucial in B2C relations; especially, the necessity for an opting-in system when requesting consumer's consent

to each of the data-collecting purposes, which excludes the validity of the data subject's consent in cases in which the passive behavior or lack of reaction of the consumer could be speculated by data operators in the sense of presuming the existence of the consent of the data subject to the collection and processing of data with personal character. The absence of the consumer's assertive response, as well as the non-initiation of an action or the simple omission of demarcation of the options regarding the processing of personal data, do not represent legal grounds for the respective operations, and the consumer's consent in these hypotheses is practically non-valid or inexistent, as a legal ground for data processing. On the contrary, the valid consent expressed for processing personal data requires an unambiguous manifestation of will by means of an unequivocal statement or through a clear affirmative action of the data subject, which implies that the data subject has taken a deliberate action to consent to that data processing. Therefore, in the context of the provisions of Regulation (EU) 2016/679, of consent-based data processing, companies may be held liable for deducing the consumer's consent from the silence or inaction of the data subject, or from conduct which does not constitute *per se* unequivocal consent.

Specific conditions for the validity of consent to the processing of personal data include the prerequisites of granular consent and those of stratified consent to multiple-purposed processing. What are the elements based on which the free and untainted nature of the consumer's consent to the processing of his personal data by trade and service professionals can be assessed, in business-to-consumer contracts? From the text of art. 4 para. (11) of Regulation (EU) 2016/679, a set of five salient elements can be deduced from Regulation (EU) 2016/679:

(a) the collecting of the data subject's freely-expressed consent to the processing of personal data implies a real choice and the possibility of exercising real control on the part of the data subjects over the collected data; on the other hand, in the cases where the data subject does not benefit from a real choice or he feels obliged to accept the processing of personal data by the data controller or there is a fear that the consumer will suffer negative consequences, should the data subject refuse to express the agreement regarding data processing, the consumer's consent will not be validly expressed; likewise, if the processing agreement personal data is requested based on a non-negotiable clause within B2C general business terms and conditions unilaterally drawn up by the pro-

fessional, it is presumed that the consumer's consent is not expressed freely, especially when the data subject is placed in the impossibility of refusing or withdrawing it without suffering material damage;

(b) in the hypotheses in which the consumer has given consent specifically for the data collection/processing operations for the purpose/purposes initially selected and declared by the data controller, it remains crucial that the companies respect the 'granularity of consent' prerequisites since the consumer cannot be forced to accept a package of data processing operations for which consent has not been requested individually, i.e. for each type of operation separately; the same rule applies to the plurality of purposes of personal data processing;

(c) when the data subject's consent has been given with knowledge of the existence of multi-stratified processing purposes, which imply the complete, correct, and transparent information of the data subject by the data operator concerning the type of processing operations, with each of the purposes of the processing and with regard to the right discretion to withdraw this consent at a later moment, violations of consumer's right of withdrawal may constitute a legal ground for engaging company's liability for the prejudicial conduct causing the consumers' damage;

(d) the unambiguous expression of the data subject's consent by which he/she accepts (through an opting-in statement or an unequivocal action), that the personal data concerning him/her will be processed, represents a salient prerequisite for sequestering multiple-purposes-based data processing; it is worth mentioning, in the perimeter of the analyzing of the 'granularity of consent' rule, that from the text of art. 7, para. (4) of Regulation (EU) 2016/679, it results that, when the personal data operators are tempted to 'associate' the consent to the processing of personal data with the consumer's consent to the acceptance of the general terms and contractual conditions, without the latter being necessary for the execution of that contract or the provision of the respective B2C relations, the mentioned type of commercial practices are considered to be undesirable, as representing a violation of the principle of freedom of consent to the processing of personal data; there is an absolute, irrefutable presumption that for the processing of the consumer's personal data, the consent was not freely expressed (by the requirements resulting from Recital 43 of Regulation 2016/679). Simultaneously, data operators must ensure that the purpose of processing consumers' personal data is not disguised or requested in an indissociable manner with the

services owed based on a business-to-consumer contract for the execution of which the personal data were initially collected.

(e) Similarly, the provisions of art. 7, para. (4), and of art. 4, para. (11) of Regulation (EU) 2016/679 are insisting on the idea that the processing of personal data for which the data subject's consent is requested should nevertheless, directly or indirectly, become a consideration for the execution of the contract, and the request for consent to data processing personal data should not be lacking in clarity; requesting consent to take place through opting-in mechanisms, and not through the means of an opting-out system of collecting consumers' consent to multiple-purposed data processing (through a statement or through an unequivocal action, excluding options for pre-checking the options by the operator), as it has been highlighted in the previous sections, remains essential for the consumer's consent to be considered valid, should the data subject exercise a real choice and to the extent that there is no risk of malicious or willfully non-transparent behavior on the part of the data operator, a risk of coercion of the consumer or the risk of bearing some significant negative consequences (for example, substantial additional costs) associated with the refusal of consent to the processing of personal data. Special attention should be devoted, in these cases, to the fact that the consumer's consent will not be freely given unless there is no room left for any element of coercion, pressure, or inability to freely exercise the will of the person concerned. From the provisions of art. 4 par. (11) from Regulation (EU) 2016/679 the need for an opting-in option can be deduced, which excludes the opting-out options for requesting the consumer's consent for the collecting and processing of personal data by the companies in B2C contractual relations.

LITERATURE

1. Alboaie, L.: *Interpretarea principiilor privacy by design în era cloud computing*, Analele Științifice ale Universității „Alexandru Ioan Cuza” din Iași, Seria Științe Juridice, LXIII (2) 2017, pp. 21-32.
2. Bercea, L.: *Standardul „consumatorului mediu” și consimțământul pentru prelucrarea datelor cu caracter personal*, Revista Română de Drept Privat (1) 2018, pp. 26-51.
3. Böröcz, I.: *Risk to the Right to the Protection of Personal Data: An Analysis Through the Lenses of Hermagoras*, European Data Protection Law Review 2 (4) 2016, pp. 467-480.
– DOI: <https://doi.org/10.21552/EDPL/2016/4/6>

4. Brunessen, B.: *Protection des données personnelles et nouveaux modes de production du droit*, Bruylant, Bruxelles, 2022.
5. Caravà, E.: *Personal Data Kept in Companies Registers: The Denial of the 'Right to be Forgotten'*, *European Data Protection Law Review* 3 (2) 2017, pp. 287-292. – DOI: <https://doi.org/10.21552/edpl/2017/2/26>.
6. Cellina, E.: *La commercialisation des données personnelles. Aspects de droit contractuel et de protection des données*, Schulthess, Geneva, 2020.
7. Chiara, P.: *The Balance Between Security, Privacy and Data Protection in IoT Data Sharing*, *European Data Protection Law Review* 7 (1) 2021, pp. 18-30. – DOI: <https://doi.org/10.21552/edpl/2021/1/6>.
8. Claeys, I., Terryn, E.: *Digital Content and Distance Sales*, Intersentia, Bruxelles, 2017. – DOI: <https://doi.org/10.1017/9781780686035>
9. Cremona, E., Laviola, F., Pagnanelli, V. (eds.): *Il valore economico dei dati personali tra diritto pubblico e diritto privato*, Giappichelli Editore, Torino, 2022.
10. Custers, B., Vrabec, H., Friedewald, M.: *Assessing the Legal and Ethical Impact of Data Reuse*, *European Data Protection Law Review* 5 (3) 2019, pp. 317-337. – DOI: <https://doi.org/10.21552/edpl/2019/3/7>.
11. Dalla Corte, L.: *On proportionality in the data protection jurisprudence of the CJEU*, *International Data Privacy Law*, 2022. [<https://academic.oup.com/idpl/advance-article-abstract/doi/10.1093/idpl/ipac014/6647961?redirectedFrom=full-text>], accessed on 28/11/2022. – DOI: <https://doi.org/10.1093/idpl/ipac014>.
12. Davies, S.: *The Data Protection Regulation: A Triumph of Pragmatism over Principle?*, *European Data Protection Law Review* 2 (3) 2016, pp. 290-296. – DOI: <https://doi.org/10.21552/EDPL/2016/3/5>.
13. Davola, A.: *Fostering Consumer Protection in the Granular Market: The Role of Rules on Consent, Misrepresentation and Fraud in Regulating Personalized Practices*, *Technology and Regulation, Special Issue: Should Data Drive Private Law*, 2022, pp. 76-86. [<https://techreg.org/article/view/11177/12407>], accessed on 28/11/2022.
14. Desgens-Pasanau, G.: *La protection des données personnelles. Les principales clés de décryptage du RGPD*, 5e édition, LexisNexis, Paris, 2022.
15. Dimitrova, D.: *The Right to Explanation under the Right of Access to Personal Data*, *European Data Protection Law Review* 6 (2) 2020, pp. 211-230. – DOI: <https://doi.org/10.21552/edpl/2020/2/8>.
16. Dobriță, M.-C.: *Aspecte teoretice și jurisprudențiale privind respectarea GDPR la încheierea și executarea unui contract*, *Analele Științifice ale Universității „Alexandru Ioan Cuza” din Iași, Seria Științe Juridice*, vol. LXVII, Supliment 2, 2021, pp. 93-106. – DOI: <https://doi.org/10.47743/jss-2021-67-4-6>

17. Dobrilă, M.-C.: *Particularități privind noțiunea de date cu caracter personal necesare pentru încheierea sau executarea unui contract la care persoana vizată este parte*, Analele Științifice ale Universității „Alexandru Ioan Cuza” din Iași, Seria Științe Juridice, vol. LXVII, Supliment, 2021, pp. 211-225.
– DOI: <https://doi.org/10.47743/jss-2021-67-3-15>.
18. Drexler, J.: *Data Access and Control in the Era of Connected Devices. Study on Behalf of the European Consumer Organisation BEUC*, The European Consumer Organisation – Bureau Européen des Unions de Consommateurs (BEUC), Bruxelles, 2018. [https://www.beuc.eu/publications/beuc-x-2018-121_data_access_and_control_in_the_area_of_connected_devices.pdf], accessed on 28/11/2022.
19. Duivenvoorde, B.: *The Liability of Online Marketplaces under the Unfair Commercial Practices Directive, the E-commerce Directive and the Digital Services Act*, Journal of European Consumer and Market Law 11 (2) 2022, pp. 43-52. [<https://kluwerlawonline.com/journalarticle/Journal+of+European+Consumer+and+Market+Law/11.2/EuCML2022009>], accessed on 28/11/2022.
20. Enzmann, M., Selzer, A., Szychalski, D.: *Practitioner’s Corner – Data Erasure under the GDPR – Steps towards Compliance*, European Data Protection Law Review 5 (3) 2019, pp. 416-420.
– DOI: <https://doi.org/10.21552/edpl/2019/3/17>.
21. Goicovici, J.: *Consimțământul consumatorului la prelucrarea datelor personale în contractele business to consumer – condiția consimțământului granular*, Analele Universității de Vest din Timișoara, Seria Drept (2) 2019, pp. 7-24.
22. Goicovici, J.: *Portabilitatea datelor cu caracter personal, prin prisma dispozițiilor RGPD și ale Directivei 2019/770: este gambitul reginei mutarea de deschidere adecvată?*, Analele Științifice ale Universității „Alexandru Ioan Cuza” din Iași, Seria Științe Juridice, Vol. LXVII, Supliment 2, 2021, pp. 57-80.
– DOI: <https://doi.org/10.47743/jss-2021-67-4-4>
23. Goicovici, J.: *Clauzele privind drepturile consumatorilor în contractele de servicii cloud computing*, Revista Română de Drept Privat (2) 2019, pp. 399-415.
24. Gräf, E.: *When Automated Profiling Threatens Our Freedom*, European Data Protection Law Review 3 (4) 2017, pp. 441-451.
– DOI: <https://doi.org/10.21552/edpl/2017/4/6>.
25. Graef, I., Clifford, D., Valeke, P.: *Fairness and Enforcement: Bridging Competition, Data Protection and Consumer Law*, International Data Privacy Law 8 (3) 2018.
– DOI: <https://doi.org/10.1093/idpl/ipy013>
26. Haas, G.: *Guide juridique du RGPD. La réglementation sur la protection des données personnelles*, 3e édition, ENI éditions, 2022.
27. Hahn, I.: *Purpose Limitation in the Time of Data Power: Is There a Way Forward?*, European Data Protection Law Review 7 (1) 2021, pp. 31-44.
– DOI: <https://doi.org/10.21552/edpl/2021/1/7>.

28. de Hert, P., Lazcoz, G.: *When GDPR Principles Blind Each Other: Accountability, Not Transparency, at the Heart of Algorithmic Governance*, European Data Protection Law Review 8 (1) 2022, pp. 31-40.
– DOI: <https://doi.org/10.21552/edpl/2022/1/7>.
29. de Hert, P., Papakonstantinou, V., Malgieri, G., Beslay, L., Sanchez, I.: *The Right to Data Portability in the GDPR: Towards User-Centric Interoperability of Digital Services*, Computer Law & Security Review, 2018.
– DOI: <https://doi.org/10.1016/j.clsr.2017.10.003>
30. Hijmans, H.: *How to Enforce the GDPR in a Strategic, Consistent and Ethical Manner?*, European Data Protection Law Review 4 (1) 2018, pp. 80-84.
– DOI: <https://doi.org/10.21552/edpl/2018/1/10>.
31. Hinsch, W.: *Differences That Make a Difference: Computational Profiling and Fairness to Individuals*, in Voeneky, S., Kellmeyer, P., Mueller, O., Burgard, W. (Eds.): *The Cambridge Handbook of Responsible Artificial Intelligence: Interdisciplinary Perspectives*, Cambridge University Press, Cambridge, 2022, pp. 229-251.
– DOI: <https://doi.org/10.1017/9781009207898.019>.
32. Jabłonowska A., *Consumer Protection in the Age of Data-Driven Behaviour Modification*, Journal of European Consumer and Market Law 11 (2) 2022, pp. 67-71, [<https://kluwerlawonline.com/journalarticle/Journal+of+European+Consumer+and+Market+Law/11.2/EuCML2022012>], accessed on 29.11.2022.
33. Jarovsky, L.: *Improving Consent in Information Privacy through Autonomy-Preserving Protective Measures (APPMs)*, European Data Protection Law Review 4 (4) 2018, pp. 447-458.
– DOI: <https://doi.org/10.21552/edpl/2018/4/7>.
34. Jasmontaite, L., Kamara, I., Zanfir-Fortuna, G., Leucci, S.: *Data Protection by Design and by Default: Framing Guiding Principles into Legal Obligations in the GDPR*, European Data Protection Law Review 4 (2) 2018, pp. 168-189.
– DOI: <https://doi.org/10.21552/edpl/2018/2/7>.
35. Jasserand, C.: *Subsequent Use of GDPR Data for a Law Enforcement Purpose: The Forgotten Principle of Purpose Limitation?*, European Data Protection Law Review 4 (2) 2018, pp. 152-167.
– DOI: <https://doi.org/10.21552/edpl/2018/2/6>.
36. Karjalainen, T.: *All Talk, No Action? The Effect of the GDPR Accountability Principle on the EU Data Protection Paradigm*, European Data Protection Law Review 8 (1) 2022, pp. 19-30.
– DOI: <https://doi.org/10.21552/edpl/2022/1/6>
37. Koch, B. A.: *Liability for Emerging Digital Technologies: An Overview*, Journal of European Tort Law 11 (2) 2020, pp. 115-136.
– DOI: <https://doi.org/10.1515/jetl-2020-0137>.

38. Kuner, Ch., Bygrave, L. A., Docksey, Ch., Drechsler, L., Tosoni, L. (eds.): *The EU General Data Protection Regulation: A Commentary/Update of Selected Articles*, Oxford University Press, 2021, pp. 45-48, available at <https://ssrn.com/abstract=3839645>, accessed on 19/01/2023.
– DOI: <http://dx.doi.org/10.2139/ssrn.3839645>.
39. Li, Z.: *Affinity-Based Algorithmic Pricing: A Dilemma for EU Data Protection Law*, Computer Law & Security Review, Vol. 46 (2022), [<https://ssrn.com/abstract=4144571>] and [<https://www.sciencedirect.com/science/article/pii/S0267364922000528>], accessed on 28.11.2022.
40. Martial-Braz, N., Rochfeld, J.: *Droit des données personnelles. Les spécificités du droit français au regard du RGPD*, Dalloz, Paris, 2019.
41. Mattatia, F.: *RGPD et droit des données personnelles*, 5e édition, Eyrolles, Paris, 2021.
42. Maxim, M.: *Răspunderea civilă contractuală în domeniul protecției datelor cu caracter personal în contextul noului Regulament general (UE) privind protecția datelor 2016/679*, Universul Juridic, București, 2021.
43. Netter, E.: *Regards sur le nouveau droit des données personnelles*, Éditions du Centre de droit privé et de sciences criminelles d'Amiens, Amiens, 2019.
44. Ploșteanu, N.-D., Lăcătușu, V., Farcaș, D.: *Protecția datelor cu caracter personal și viața privată – Jurisprudența CEDO și CJUE*, Universul Juridic, Bucharest, 2018.
45. Rabagny-Lagoa, A.: *Fiches de droit du traitement et de la protection des données personnelles*, Ellipses, Paris, 2022.
46. Raimondo, L.: *La protection des données personnelles. 100 questions-réponses pour comprendre et mieux se protéger*, Ellipses, Paris, 2021.
47. Riccio, G. M., Scorza, G., Belisario, E. (eds.): *GDPR e normativa privacy. Commentato*, Editore IPSOA Gruppo di Wolters Kluwer Italia, 2018.
48. Săvescu, A. (ed.): *RGPD – Regulamentul general privind protecția datelor cu caracter personal. Comentarii și explicații*, Hamangiu, Bucharest, 2018.
49. Spiecker Genannt Döhmman, I., Tambou, O., Bernal, P., Hu, M., Molinaro, C. et al.: *Multi-Country – The Regulation of Commercial Profiling – A Comparative Analysis*, European Data Protection Law Review 2 (4) 2016, pp. 535-554.
– DOI: <https://doi.org/10.21552/EDPL/2016/4/12>.
50. van Alsenoy, B.: *Data Protection Law in the EU: Roles, Responsibilities and Liability*, Intersentia, Bruxelles, 2019.
– DOI: <https://doi.org/10.1017/9781780688459>
51. van Eijk, N., Hoofnagle, J. C., Kannekens, E., *Unfair Commercial Practices: A Complementary Approach to Privacy Protection*, European Data Protection Law Review 3 (3) 2017, pp. 325-337.
– DOI: <https://doi.org/10.21552/edpl/2017/3/7>.

52. Veale, M., Nouwens, M., Santos, C.: *Impossible Asks: Can the Transparency and Consent Framework Ever Authorise Real-Time Bidding After the Belgian DPA Decision?*, *Technology and Regulation*, 2022.
– DOI: <https://doi.org/10.26116/techreg.2022.002>.
53. Viterbo, F. G.: *The ‘User-Centric’ and ‘Tailor-Made’ Approach of the GDPR Through the Principles It Lays down*, *The Italian Law Journal* 5 (2) 2019, pp. 631-672.
54. Voigt, P., von dem Bussche, A.: *The EU General Data Protection Regulation (GDPR): A Practical Guide*, Springer International Publishing, 2017.
– DOI: <https://doi.org/10.1007/978-3-319-57959-7>.
55. Wachter, S., Mittelstadt, B.: *A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI*, *Columbia Business Law Review* (2) 2019, [<https://ssrn.com/abstract=3248829>], accessed on 28/11/2022.

