sciendo

The GDPR and the DGA Proposal: are They in Controversial Relationship?

Lusine Vardanyan & Hovsep Kocharyan*

Summary: At the end of 2020, the European Commission published a new European data strategy, which aims to create a new legal framework to promote the development of a single European data market. In the scope of the new strategy the European Commission has already proposed the Data Governance Act proposal (hereinafter – the "DGA"), which aims to strengthen the mechanism to facilitate data exchange. The proposal of the new legislative act has raised the question about the right balance between it and the existing EU legislative acts, which were adopted in the key of personal data protection, especially with the General Data Protection Regulation (hereinafter – the "GDPR"). We argue that there are a number of inconsistencies between the DGA proposal and the GDPR that may prevent the full implementation of mechanisms that allow achieving the EU's intended goals in this field within the framework of the new European strategy. The interaction of the DGA with the GDPR is characterized by conflict of laws and legal uncertainty, which can jeopardize the achievement of the objectives of the DGA itself and can reduce the level of personal data protection in the EU, compared to the GDPR. Besides, the examination of the relevant case-law of the Court of Justice of the European Union (hereinafter – the "CJEU" or the "Court") regarding the implementation of the GDPR identifies approaches that prevent the opening of data exchange as the DGA proposal requires.

Keywords: GDPR, data exchange, data protection, CJEU, new European strategy

* Lusine Vardanyan is a doctoral student at the Department of International and European Law, Faculty of Law, Palacký University Olomouc (Czech Republic). She participated in the work on this paper on behalf of the Project of specific research no. IGA_PF_2021_014 "Tackling the protection of the right to personal integrity and body-derived data in information society: new challenges for EU law". Email: lucyrossetti77@gmail.com
Hovsep Kocharyan is a doctoral student at the Department of International and European Law, Faculty of Law, Palacký University Olomouc (Czech Republic). He participated in the work on this paper on behalf of the Project of GAČR no. 20-27227S "The Advent, Pitfalls and Limits of Digital Sovereignty of the European Union" funded by the Czech Science Foundation. Email: hovsep.kocharyan01@upol.cz

Citation: VARDANYAN, L., KOCHARYAN, H. The GDPR and the DGA proposal: are they in controversial relationship? *European Studies – the Review of European law, Economics and Politics*. 2022, vol. 9, no. 1, pp. 91–109, DOI: 10.2478/eustu-2022-0004

1. Introduction

At the end of 2020, the European Commission published a new European data strategy, which aims to create a new legal framework to promote the development of a single European data market. As part of the new European strategy, the EU is already submitting proposals for new laws. Along with the Digital Services Act[1] (hereinafter – the "DSA") and the Digital Markets Act[2] (hereinafter – the "DMA"), the European Commission has proposed the Data Governance Act project, which aims to strengthen the governance mechanism to facilitate data exchange, and introduce new tools and mechanisms to implement the European data strategy. The DGA defines a special set of principles for managing the provision of data exchange services (Article 11), organizes a compliance system for exporting data outside the EU (Article 30), and introduces rights that should ensure the implementation of "data altruism" (Article 19). Even a cursory analysis of these projects shows an attempt by the EU to become an active player in promoting the monetization of personal data. This is a radical shift in the EU's focus from protecting privacy to promoting data sharing. However, this shift strictly raises the question of the correct balance between the new laws that will be adopted based on the new strategy and the existing EU laws that have been adopted or interpreted by the CJEU in the context of data protection of the person. Of particular importance is the problem of coordinating the GDPR and the DGA,[3] as indicated in the joint opinion of the EDPB and EDP.[4] The most important concern is the possibility of maintaining the level of protection of personal data and the problem of further application of the GDPR as the most

[1] Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC COM/2020/825 final [online]. Available at: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM:2020:825:FIN

[2] Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act) COM/2020/842 final [online]. Available at: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM%3A2020%3A842%3AFIN

[3] 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 [2016] OJ L 119/1.

[4] EDPB-EDPS Joint Opinion 03/2021 on the Proposal for a Regulation of the European Parliament and of the Council on European Data Governance (Data Governance Act). (2021), p. 14.

influential legal instrument that has provided individuals with enhanced protection of information confidentiality.[5]

As stated in the Explanatory memorandum to the DGA proposal: "(...) the interplay with the legislation on personal data is particularly important. With the General Data Protection Regulation (GDPR) and e-Privacy Directive, the EU has put in place a solid and trusted legal framework for the protection of personal data and a standard for the world".[6] Although the DGA will not modify existing data protection rules, however, the goal set for this document by the European Commission can be achieved only if there is insufficient mutual coordination of these acts, and in particular with the GDPR.

The objective of this paper is to analyze the DGA proposal and the GDPR to identify possible inconsistencies between these legislative acts that may prevent the full implementation of mechanisms that allow achieving the intended EU goals. In addition, we will examine the relevant case law of the EU Court of Justice regarding the GDPR to identify approaches that prevent the opening of data exchange.

To achieve the research objectives, the researchers use several approaches to meet the complex issues of the paper. As a starting point (working with the set of relevant data/documents) we will utilize the analytical approach (the desktop research) in order to identify, systematize and mutually compare the provisions of the DGA and GDPR, key case-law of CJEU, its impact and interpretations. The researchers also use deductive approach while testing the hypotheses against the assembled data; inductive method while formulating the models of interpretation; comparative method, while comparing the provisions of appropriate legislative acts and judicial cases; synthesis, while working on the conclusions; prediction in evaluation and extrapolation of the future developments.

The research will try to find the answers for the following questions:

1. Are there any inconsistencies between the DGA and the GDPR, and the relevant case law of the CJEU, and if so, which are the main ones?
2. Will the DGA strengthen individuals' control over their personal information, compared to the GDPR?

[5] See also KOCHARYAN, H., VARDANYAN, L., HAMUĽÁK, O., KERIKMÄE, T. Critical Views on the Right to Be Forgotten After the Entry Into Force of the GDPR: Is it Able to Effectively Ensure Our Privacy? International and Comparative Law Review. 2021, vol. 21, no. 2, pp.96–115. https://doi.org/10.2478/iclr-2021-0015

[6] Proposal for a Regulation of the European Parliament and of the Council on on European data governance (Data Governance Act) COM/2020/767 final [nline]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0767

2. Regulation of data exchange before the adoption of the new European strategy

In the area of data exchange regulation, the EU's legislative activity is quite modest. This is primarily the Directive (EU) 2019/1024[7] and the RNPR.[8] But in comparison with the GDPR, these acts are somewhat secondary in the formation of the digital environment. Moreover, these acts do not detract from the value of the GDPR and do not enter into conflict with it.

The Directive (EU) 2019/1024 does not revoke the GDPR in accordance with Article 1 (paragraph 4). But it applies only to non-personal data and the level of protection of personal data remains unchanged. The main objective of the Directive (EU) 2019/1024 is to allow the free reuse of data held by national public sector authorities. Article 1 of the Directive sets out a set of minimum rules governing reuse and practical measures to facilitate reuse:

a) existing documents administered by the public sector authorities of the Member States;
b) existing documents belonging to certain state-owned enterprises; and
c) certain types of research data.

According to Article 12 of the Directive (EU) 2019/1024, it also restricts the ability of public sector bodies to enter into exclusive reuse agreements with private partners. However, the scope of the Directive is rather limited. It allows Member States to enact exclusion laws and generally does not apply to documents whose intellectual property rights are held by third parties.

According to Article 1 of the Regulation (EU) 2018/1807 aims to ensure the free flow of non-personal data. Article 4 prohibits Member States from introducing data localization requirements. Data should move freely, like goods, capital, services and labor. However, due to the breadth of the definition of personal data in Article 4 of the GDPR, almost any data can potentially become personal data. This means that Regulation (EU) 2018/1807 has limited application. The

[7] Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector informationPE/28/2019/REV/1 [online]. Available at:https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2019.172.01.0056.01.ENG

[8] 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 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 (Text with EEA relevance.)
PE/53/2018/REV/1 [online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1807

above legal instruments are certainly not sufficient to ensure a free flow of data. It is the lack of effectiveness of existing tools for data exchange, as well as the consideration of data as a key asset for the European economy, that has led to the need for new regulation of this area.

3. Priority of the goal of protecting privacy in the GDPR in the case-law of the CJEU: will there be a review?

The CJEU plays a major role in personal data protection as their function is to interpret the EU law and thus also the EU legislation related to the personal data protection.[9] The shift in the EU's focus from protecting privacy to promoting data sharing means that it is possible to revise the approach developed in the EU's judicial practice to the interpretation of the GDPR with a key that provides a fundamental right to data protection. The Court will again face the difficult task of balancing the right to data protection and the free flow of data.

As is known the CJEU through its judicial practice has contributed to the transformation of the protection of personal data into a fundamental right, through the definition of the categorical apparatus used in the relevant legal acts,[10] obligations and responsibilities of the data processing parties, balancing data protection with other rights.[11] Many of the definitions used in the DGA, as in the GDPR, are broad and vague, thus giving the provisions a wide range of interpretation. There will be a clear need to clarify the basic definitions of the DGA.

In its judgments, in particular with regard to the laws governing the field of data protection, the Court has repeatedly emphasized, based on its case-law, that it considers the purpose and context to be the main principles of their interpretation.

---

[9] PAVELEK, O., ZAJÍČKOVÁ, D. Personal Data Protection in the Decision-Making of the CJEU Before and After the Lisbon Treaty. *Baltic Journal of European Studies.* 2021, Sciendo, vol. 11(2), p. 167.

[10] Judgment of the Court of 6 November 2003.Criminal proceedings against Bodil Lindqvist. Case C-101/01.EU:C:2003:596; Judgment of the Court (Second Chamber) of 19 October 2016 Patrick Breyer v Bundesrepublik Deutschland Case C-582/14 EU:C:2016:779; Joint cases C-141/12 and C- 372/12; YS and M. and S. v Minister of Immigration, Integration and Asylum [2016], ECLI:EU:C:2014:2081.

[11] Judgment of the Court (Grand Chamber) of 6 October 2015 Maximillian Schrems v Data Protection Commissioner Case C-362/14 EU:C:2015:650; Judgment of the Court (Second Chamber) of 9 March 2017 Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v Salvatore Manni Case C-398/15; EU:C:2017:197, Judgment of the Court (Grand Chamber) of 5 June 2018 Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH. Case C-210/16. EU:C:2018:388.

In the judgement of the case of *Sergejs Buivids* (in paragraph 49) the Court states: "It must be observed, as a preliminary point, that, according to settled case-law of the Court, the provisions of a directive must be interpreted in the light of the aims pursued by the directive and the system which it establishes".[12] This also applies to the interpretation of the GDPR. But GDPR has a "Janusian" two-face goal: to ensure an equal level of protection of natural persons and the free flow of personal data throughout the EU and thus contribute to the functioning of the internal market. But the goal of promoting the formation of the internal market in the adopted hybrid model of the GDPR should still be considered secondary in the light of the case-law of the CJEU, as it gives priority to the goal of protecting the rights of individuals over the free flow of data.

In the cases of Schrems II,[13] *Wirtschaftsakademie*,[14] FashionID[15] and others the Court has already formed approaches for the predictability of subsequent enforcement and interpretation of the GDPR in the contest, namely, the purpose of protecting the rights of individuals. The Court's judgment in the case of *Google v. CNIL*[16] even allows for the further worldwide application of the right to be forgotten and is seen as an attempt to develop progressive case law to protect human rights in the digital age.[17] The enviable consistency of the CJEU interpretation in the context of the protection of the fundamental right to data protection should be pointed out. However, this predictability in a situation where the DGA will come into force can greatly hinder the enforcement of the DGA. The DGA has as its legal basis the article 114 of the TFEU. In accordance with this article, the EU must take measures to bring together the provisions established by law, regulation or administrative actions in the Member States

[12] Judgment of the Court (Second Chamber) of 14 February 2019. Sergejs Buivids v. Datu valsts inspekcija (C-345/17, EU:C:2019:131.

[13] Judgment of the Court (Grand Chamber) of 16 July 2020 Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems Case C-311/18 ECLI:EU:C:2020:559.

[14] Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH C-210/16, EU:C:2018:388.

[15] Judgment of the Court (Second Chamber) of 29 July 2019 Fashion ID GmbH & Co.KG v Verbraucherzentrale NRW eV Request for a preliminary ruling from the Oberlandesgericht Düsseldorf Case C-40/17, ECLI:EU:C:2019:629.

[16] Judgment of the Court (Grand Chamber) of 24 September 2019 Google LLC, successor in law to Google Inc. v Commission nationale de l'informatique et des libertés (CNIL).

[17] HAMUĽÁK, O., VARDANYAN, L., KOCHARYAN, H. The Global Reach of the Right to be Forgotten through the Lenses of the Court of Justice of the European Union. *Czech Yearbook of Public and Private International Law*. 2021, vol. 12, p. 211. See also HAMUĽÁK, O., KISS, L. N., GÁBRIŠ, T., KOCHARYAN, H. "This Content is not Available in your Country" A General Summary on Geo-Blocking in and Outside the European Union. *International and Comparative Law Review*. 2021, vol. 21, no. 1, pp. 153–183, https://doi.org/10.2478/iclr-2021-0006

that aim to establish and operate an internal market in the EU. At first glance, it may seem that this sets different goals for the GDPR and DGA. Maybe, but the GDPR enshrines individual rights, such as the right of access by the data subject (Article 15), the right to rectification (Article 16) and the right to erasure ("the right to be forgotten") (Article 17), which, together with the data protection rules, form a framework for protecting individual control over their data. The memorandum indicates that "Allowing personal data to be used with the help of a 'personal data-sharing intermediary', designed to help individuals exercise their rights under the General Data Protection Regulation (GDPR)".[18] It states: "Since personal data falls within the scope of some elements of the Regulation, the measures are designed in a way that fully complies with the data protection legislation, and actually increases in practice the control that natural persons have over the data they generate."[19]

The DGA is essentially supposed to create a human-centric approach for the digital single market and the data economy, by fostering data sharing mechanisms that benefit society and by allowing the sharing of public sector data for the common good. In this way, it should differ from DSA and DMA and approach the GDPR. Their identical protective approach for individuals can be observed in the mimesis of the GDPR in the DGA, as noted by Vagelis Papakonstantinou and Paul de Hert.[20] Especially when Article 2 of the DGA introduces a new unique set of terms: "data holders", "data users", "data" or "data sharing", which however correspond in many ways to "data subjects", "controllers", "personal data" and "processing" of the GDPR (Article 4). And it is quite easy to identify the "parallelism" of the DGA proposal text with the GDPR text. This suggests that it may also be aimed at promoting the fundamental right to data protection. Again, the same "two-faced" feature of the legal act, which transfers the weight of the choice of telos on the shoulders of the case-law of the CJEU. This is especially difficult in conditions where the DGA does not give an exact meaning and scope of itself.

After the entry into force of the DGA, the version currently proposed may also raise the question of reviewing this unambiguous choice of one goal by the Court out of the two proposed in the GDPR. In future, the Court will have to find a solution to reconcile the two almost mutually exclusive goals. The new policy

[18] *Explanatory memorandum of the proposed DGA* [online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0767

[19] Ibid.

[20] PAPAKONSTANTINOU, V., DE HERT, P. Post GDPR EU laws and their GDPR mimesis. DGA, DSA, DMA and the EU regulation of AI/ 1 April 2021 [online]. Available at: https://europeanlawblog.eu/2021/04/01/post-gdpr-eu-laws-and-their-gdpr-mimesis-dga-dsa-dma-and-the-eu-regulation-of-ai/

will require a delicate balance between unleashing the economic potential of data use while respecting personal data and other fundamental rights of EU citizens.

It is possible, of course, that a shift in the EU's focus from protecting privacy to promoting data sharing may force the CJEU to reconsider the human rights focus of the GDPR and revive its telos as a data market regulator. But this would mean crossing out the EU's already established judicial practice, which seems an unlikely scenario. In addition, such a change may have a negative impact on the level of privacy protection in the EU – a circumstance that the EU has always been proud of.

It should be noted that the text of the GDPR itself does not consider the protection of individuals as a restriction on the movement of personal data: "the free movement of personal data within the Union should not be restricted or prohibited for reasons related to the protection of individuals with respect to the processing of personal data" (Article 1). This provision may be one of the key loopholes for the Court to form an approach that approves the priority of data turnover over the protection of human rights in the digital sphere. But the task for the Court in any case will not be easy. Although the provisions of the GDPR concerning, for example, data security or data portability obligations directly contribute to the creation of data economy, the GDPR nevertheless restricts the processing of data and this is based on Article 5, on the principles of processing. According to the principle of purpose limitation, data may only be collected for certain, explicit and legitimate purposes, and may not be further processed in a manner inconsistent with the original purposes for which it was collected. In addition, the data minimization principle restricts processing to data that is adequate, up-to-date, and limited to what is necessary for the purposes of processing. These data protection principles are not easily reconciled with the idea of open data flows.

It seems that the appearance of a second human rights document regulating, among other things, the sphere that is already regulated by the provisions of the GDPR, should be aimed at improving the effectiveness and level of protection of personal data *inter alia* and the degree of control of the individual over their data, compared to the GDPR. But does the DGA increase the degree of protection that is provided through the implementation of the GDPR provisions? It appears that there is not, which will be shown in later in this paper.

And although it is impossible to understand its clear interaction with the GDPR from the text of the DGA proposal, it can already be stated that the judicial practice of the CJEU may also become an obstacle to the full application of the DGA and the achievement of its goals.

4. Introduction of the concept of "data altruism": there is no good without a hood

In Article 2(10) of the project of the DGA the term "data altruism" is defined as "(…) the consent by data subjects to process personal data pertaining to them, or permissions of other data holders to allow the use of their non-personal data without seeking a reward, for purposes of general interest, such as scientific research purposes or improving public services". From the definition from the very beginning, it can be concluded that data altruism is one of the specific models of consent to the processing and use of data, at least for data subjects. It is also clear that the drafters, through increased "data donation", wanted to prevent the commercialization of data exchange in the context of the expansion of the data market. At first glance, this is an expression of the EU's basic approach to the protection of personal data, and a continuation of the main meaning embedded in the GDPR and antitrust laws, through which the EU fights the commercial exploitation of private information.

But the picture changes if we point out the following. Firstly, the content of the legal definition of altruism is not disclosed in the DGA or in any other EU legislation. Secondly, the provision of Article 2 may also become a loophole for the commercialization of private information or the deception of data subjects in the field of personal data exchange, if it is considered in conjunction with Article 3 of the DGA, which makes it possible to reuse personal data without obtaining the consent of the data subject itself. The data obtained may then be commercialized by third parties without the knowledge of the individual providing the data. Third, regulation will further exacerbate the issue of the balance between respecting the fundamental right to protect personal data and sharing personal data for general "public interest" purposes. Fourth, according to the DGA, personal data can also be transferred and processed "altruistically" on the basis of an individual's consent, an area that is already regulated by the provisions of the GDPR with even stricter rules. In conditions where the provisions of the DGA do not provide for other additional rules that would increase the security of the processing of "altruistically" transferred personal data, this means that there is no duplication of the scope of competing data management regimes. In addition, the DGA may reduce the protection and guarantees provided for in the GDPR for personal data by creating *lex specialis* provisions that allow circumventing the strict provisions of the GDPR. This reduces the level of control of the individual over the use of personal information: the latter is known to be the main idea of the GDPR, which is considered an act that provides information self-determination of a person. The desire of the DGA to create an adequate mechanism by which

an individual can ensure that his/her data is used for the public good, and not just turned into a commodity for private profit, can only be called an aspiration.

5. A new model of consent?

The DGA introduces a single form of consent for altruism in relation to data. Article 22(3) states that: "When providing personal data, the European Data Altruism Consent Form must enable data subjects to give consent and withdraw consent to a specific data processing operation in accordance with the requirements (GDPR)". The advantages of this model include the possibility of harmonizing legislation in the EU Member States and facilitating the exchange of data within the EU. But the DGA does not specify, whether this consent mechanism should be considered as another requirement for the legitimate exchange of data and their processing of personal data, or should become an alternative model of consent – *lex specialis* – when the data is used for general interest purposes. It should be noted that in contrast to the DGA, the concept of consent established in the GDPR is clearly defined. So, Article 4(11) of the GDPR establishes that ""consent" of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her".

The EDPB also emphasizes the importance of detail in this matter: "If the controller has conflated several purposes for processing and has not attempted to seek separate consent for each purpose, there is a lack of freedom. This granularity is closely related to the need of consent to be specific".[21] In accordance with the GDPR, where Article 5(1)(b) establishes the principle of limiting the purpose of protecting data subjects, there are restrictions on the use of data by controllers. Personal data must be collected for specific, explicit and legitimate purposes and must not be further processed in a manner incompatible with them. Re-processing for other purposes is possible if the data subject again consents to it, as well as if the second purpose is compatible with the first. In this second case, a compatibility assessment must be carried out, requiring an assessment of very many circumstances, such as, for example, the context of the collection of personal data, the reasonable expectations of the data subjects regarding the reuse of the submitted data, the impact of the re-processing of the data on the data

[21] *Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1 Adopted on 4 May 2020* [online]. Available at: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf

subject itself, the safeguards adopted by the controller to ensure fair processing and to prevent any undue influence on the data subjects.[22] The DGA introduces a mechanism for reusing "protected public sector data". Moreover, such reuse is also possible in the case of personal data. Here again, one can see the overlap DGA with the GDPR, since the reuse of personal data is already regulated by the relevant provisions of the GDPR. The DGA allows data intermediaries to determine the purpose of data exchange and for personal data. However, this truncates to some extent the institution of consent. By allowing the reuse of personal data without clearly providing the same GDPR guarantees, the DGA weakens the protection provided by the GDPR. This is especially dangerous when one considers that the purpose of use may also be commercial, and according to article 6 public sector authorities may charge a fee for allowing the reuse of data. In addition, the DGA talks about consent in the context of altruism, but does not contain details, as does the GDPR, and increases the likelihood that in practice, when reused, the companies will have the opportunity to choose a model of the least detailed consent, as well as a goal different from the original, including commercial. Moreover, this may be acceptable for personal data. Therefore, we can agree with the view that the DGA does not properly take into account the need to ensure and guarantee the level of protection of personal data provided for by EU law and raises serious concerns from the point of view of fundamental rights.[23]

There is one more thing to be pointed out. Among the new definitions that the GDPR introduces, we would like to highlight the category of "permission of the data holder". At the same time, the DGA defines in Article 5 that ""data holder" means a legal person or data subject who, in accordance with applicable Union or national law, has the right to grant access to or to share certain personal or non-personal data under its control". Such a notion is problematic. First, it can be easily seen that a systematic interpretation of these rules can lead to a situation where the "permission" of the DGA and the "consent" of the GDPR become competing concepts. Besides, the joint opinion of EDPB and EDPS looks at the qualification of "permission" under art 6(1)(c) and (e) of the GDPR, which means that it would allow for the sharing/processing of data insofar as it constitutes a legal basis in the meaning of this article. But the concept of "permission" does not fulfil the criteria of Article 6(3) GDPR in order to qualify as a legal basis under Article 6(1)(c) and/or (e) of the GDPR.[24] Such inconsistency

[22] *Article 29 Data Protection Working Party, Opinion 03/2013 on Purpose limitation* [online]. Available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

[23] Ibid 7.

[24] EDPB-EDPS Joint Opinion 03/2021 on the Proposal for a Regulation of the European Parliament and of the Council on European Data Governance (Data Governance Act). (2021), p. 14.

in the models of consent in human rights documents may reduce their potential to protect fundamental human rights. The purpose of data exchange should be clear from the beginning and data should only be collected to answer clear and pre-defined questions. In addition, data subjects should be able to dynamically consent to the collection/use of their data, as well as provide/withdraw consent as necessary. The role of a person should not be limited to consent to the use of their personal data. The initial consent may not be a sufficient condition for the subsequent exchange of data.

6. Problematic differentiation of personal and non-personal data

The correct definition of the relationship between personal and non-personal data is crucial for the application of EU legal instruments, as EU law involves the application of various legal acts to regulate the scope of personal data and non-personal data. The difference between personal data and non-personal data is also due to the material scope of the GDPR and the EU Regulation on the Free Flow of Non-Personal Data (hereinafter – the "RNPR"). The differentiation of personal and non-personal data was almost always problematic even before the DGA, for example, because of the extreme breadth of the concept of personal data specified in the GDPR, because of the "transitivity" of non-personal data to personal data, as indicated by the European Commission.[25] The researchers point out that a meaningful distinction between identifiable and unidentifiable information could not be more robust.[26] The same conclusion can be seen in the additional opinion of WP29: data is not identified, that is, anonymous, only when anonymization is irreversible.[27] The DGA has not resolved the issue of the ratio of personal and non-personal data. Moreover, the analysis of art 2(3) DGA shows that this difference is taken as the basis of DGA.[28] Based on this distinction, it

[25] European Commission, 'Communication from the Commission to the European Parliament and the Council: Guidance on the Regulation on a Framework for the Free Flow of Non-Personal Data in the European Union COM(2019) 250 Final' (2019), pp. 7, 10.

[26] NARAYANAN, A. and FELTEN, Ew. *No Silver Bullet: De-Identification Still Doesn't Work. 2014* [online]. Available at: https://freedom-to-tinker.com/2014/07/09/no-silver-bullet-de-identification-still-doesnt-work/; OHM, P. Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization. *UCLA Law Review*. 2010, Vol. 57, p. 1701 [online]. Available at: www.epic.org/privacy/reidentification/ohm_article.pdf

[27] Article 29 Working Party opinion 05/2014 on Anonymisation Techniques, 10 April 2014 (WP 216), pp. 3, 5–7.

[28] DGA, art 2(3).

often provides for different rules regarding personal data and personal data.[29] This is not a simple adoption of the legal approach already more or less established in EU law. This can be seen as the result of a growing awareness that data is a valuable resource, and the DGA, as the first EU legal instrument reflecting the EU's political trend towards a data economy, should seek to reflect the concept of data as things as deeply as possible, in order to unlock key innovations and promote economic growth within the EU. After all, as Charlotte Ducuing points out, with the recognition of different regulatory regimes for personal and non-personal data, the concept of "data as a thing".[30] Therefore, it is not logical to demand from the DGA an unambiguous solution to this problem. But the DGA does not just adopt the provisions that already exist in existing laws, but rather tries to redraw those provisions of the GDPR that are key, ideological for this document and for which this division between the regulation of personal and non-personal exists in EU law. For example, the DGA allows the reuse of data, including personal data, and at the same time allows, in accordance with article 6, public sector authorities to charge a fee for allowing the reuse of data, including personal data – a circumstance that was key for the adoption of the GDPR as a tool to prevent the commodification of personal data and protect privacy. But any new framework for data must take into account that data is not just an economic resource that needs to be turned into a commodity, and not an instrument of pressure against private players. It is inextricably linked with data subjects. And the DGA, which focuses on disclosing the economic value of data, ignores this fact. Meanwhile, in any case, data subjects should control their data, and it should not be considered simply as a resource for fueling "innovation".

It should be noted that it is difficult to determine when a part of the data will become personal and, therefore, when the regulatory regime should change.[31] This means that the DGA can contradict two legislative acts at once: the data can first be subject to the DGA in conjunction with the RNPR, and then be subject to the DGA in conjunction with the GDPR.

And there is one more thing. In nature, there are mixed data sets – these are data that consist of personal and non-personal data. They are not regulated as a single entity in EU law, but are regulated by different legislative acts – RNPR

[29] Articles 5(3), 5(11)-(13), 30 of the DGA.

[30] DUCUING, Ch. *The regulation of 'data': a new trend in the legislation of the European Union?* 06 April 2021 [online]. Available at: https://www.law.kuleuven.be/citip/blog/the-regulation-of-data-a-new-trend-in-the-legislation-of-the-european-union/

[31] GRAEF, I., GELLER, R., HUSOVEC, M., *Towards a Holistic Regulatory Approach for the European Data Economy: Why the Illusive Notion of Non-Personal Data Is Counterproductive to Data Innovation.* (September 27, 2018). TILEC Discussion Paper No. 2018-029 [online]. Available at: https://ssrn.com/abstract=3256189

and GDPR. The DGA also ignores the existence of the specified data category: it does not contain the concept of mixed data and does not provide guidance for the demarcation of data within a single data set. But ignoring the problem does not mean that it does not exist: the problem of the demarcation of personal and non-personal data within the same data set is still unresolved. The new European strategy is limited to a reference to the European RNPR Guidelines, without defining what a "mixed data set" means.[32] This link can be considered as "empty" because this concept is also absent in RNPR.[33] If the DGA is intended to regulate the data economy, it must necessarily contain strict legislative rules in this regard, especially when, as the European Commission points out, mixed datasets will make up the majority of data sets in the data economy.[34]

The absence of special rules in the DGA for mixed data does not mean that the DGA will not apply to this set. One can reason "by analogy": RNPR indicates that: "In the case of a data set composed of both personal and non-personal data, this Regulation applies to the non-personal data part of the data set. Where personal and non-personal data in a data set are inextricably linked, this Regulation shall not prejudice the application of Regulation (EU) 2016/679".[35] The data set is "inextricably linked" if their separation would be either impossible or considered by the controller to be economically inefficient or technically impracticable.[36] In the text, you can also find the provision that the DGA is without prejudice to GDPR. But what does it give the law enforcement officer to "change" one legal act to another, if the DGA does not contain any additional provisions regarding the use of non-personal or mixed data? Unfortunately, nothing. In addition, the provision under consideration from the very beginning makes it unclear whether the phrase "without prejudice" is solely a priority of the GDPR in the event of a conflict of its provisions with the DGA, if so, is the GDPR a priority in any situation of a conflict of the GDPR with the DGA? These are the questions to which the answer will not be found as a result of the analysis of the provisions of the DGA. The EDPB-EPDS joint opinion emphasizes that such a formulation of the DGA of the provision in question does little to avoid in practice a conflict

[32] European Commission, 'Communication from the Commission to the European Parliament and the Council, the European Economic and Social Committee and the Committee of the Regions: A European Strategy for Data' (2020), p. 6.

[33] European Commission, 'Communication from the Commission to the European Parliament and the Council: Guidance on the Regulation on a Framework for the Free Flow of Non-Personal Data in the European Union COM(2019) 250 Final' (2019), pp. 8–9.

[34] Ibid., p. 8.

[35] Article 2(2) of the RNPR.

[36] European Commission, 'Communication from the Commission to the European Parliament and the Council: Guidance on the Regulation on a Framework for the Free Flow of Non-Personal Data in the European Union COM (2019) 250 Final' (2019), pp. 9, 10.

between the GDPR and specific provisions of the DGA that may contradict the GDPR.[37] Note that fixing the unambiguous priority of the provisions of the GDPR in the event of a conflict is also not justified, since it will detract from the very meaning of the DGA and expand the already wide material scope of the GDPR, which will hinder the achievement of the goal that was set for the DGA. This is also problematic for achieving the goals of the DGA. The solution is development and legislative consolidation of conflict-of-laws rules regarding certain provisions and legal institutions.

7. The problem of the uncertainty of the concept of "common interest"

The DGA aims to establish a mechanism to encourage the development of the EU data space, where individuals and businesses should more effectively control the data they generate. At the heart of the DGA is the idea that access to data, and thus control over it will be facilitated by third-party "data sharing service providers". According to the DGA, these service providers must put in place procedures to ensure that data sharing preserves the public interest, including those related to data protection. If the protection of the public interest is an important duty for service providers, then the definition of what is the "public interest" becomes important both in terms of evaluating the proper performance of this duty, and in terms of implementing data exchange. Intermediaries thus have the opportunity to assess a particular interest as a public one, since the DGA does not define what is meant by a common interest and there are no legally established criteria for checking the presence or absence of such a "common interest". The only requirement in determining the "common interest" in this case may be the requirement of neutrality put forward in the DGA. But even this may not protect against practices that may be presented as having a public purpose, but in fact also have a commercial element, such as in the use of data as a result of the commercialization of research results.

In addition, it is somewhat problematic how data intermediaries will act when the public interests themselves will conflict. The next problem that arises from the ambiguity of the concept of public interest is related to the prohibition of an agreement or other practices related to the reuse of "protected data" held by public sector bodies that would grant exclusive rights or restrict the availability of data for reuse by entities that are not parties to such agreements. Having provided

[37] 'EDPB-EDPS Joint Opinion 03/2021 on the Proposal for a Regulation of the European Parliament and of the Council on European Data Governance (Data Governance Act)' (2021), pp. 6, 9.

for this provision, the DGA provides for a derogation, according to which the exclusive right to re-use data can be granted to the extent necessary to provide a service or product "in the general interest". This can create an exception that is too broad. Therefore, we suggest defining the concept of "common interest" or a list of criteria that must be met in order for a service or product to be considered "in the common interest" and can use this exception.

8. Conclusion

The paper shows that the EU legislation adopted before the new European Strategy did not sufficiently stimulate the creation of data market and extensive data exchange. This was also due to the CJEU's particularly sensitive attitude to the problem of protecting confidentiality and personal data, which is also indicated by the choice of the protection of personal data as the GDPR's telos. The shift in the EU's focus from protecting privacy to promoting data sharing, outlined in the new European Strategy, could seriously affect the CJEU's already established precedent practice. In order to reconcile the objectives of these two regimes, consistent work is needed, which may be carried out, among others, in the legal practice of the CJEU. Despite the desire through the DGA to adopt a human-centric approach for the digital single market, the risk of a collision between the DGA and the GDPR regimes may reduce the level of individual control over the use of personal data compared to the GDPR.

The paper also shows that the DGA's interaction with the GDPR is problematic and is characterized by a number of legal uncertainties that can jeopardize the achievement of the DGA's goals. These are the divergence of definitions between the GDPR and the DGA, the problematic demarcation of personal and non-personal data, which is not solved by the DGA, but is taken as the basis of regulation, the lack of a clear basis for the processing and reuse of personal data in accordance with the DGA, etc. A more precise legislative definition of the conceptual framework used, or the development and consolidation of appropriate criteria for evaluating broad legal categories, will be a significant step towards a clearer relationship between the GDPR and the DGA. The uncertainty of the legal concepts used in the DGA, such as "data altruism" or "common interest", and the problematic relationship of consent models, can reduce the protection and guarantees provided for in the GDPR for personal data and make it possible to circumvent the strict provisions of the GDPR, thereby weakening the guarantees for the implementation of the information self-determination of a person. As a recommendation in this case, it can be proposed to exclude the possibility of re-use of personal data from the scope of Article 3 of the DGA.

It remains to be seen whether Europe's vision of becoming a digital leader in the face of the potential conflicts that have arisen between the DGA and the GDPR can actually be achieved. But it is clear that Europe should become a digital leader while maintaining strong protection of rights and fundamental values and retreat from its leading role in the field of data protection.

List of references

Article 29 Data Protecton Working Party, Opinion 03/2013 on Purpose limitation: [online]. Available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

Article 29 Working Party opinion 05/2014 on Anonymisation Techniques, 10 April 2014 (WP 216).

Charter of Fundamental Rights of the European Union OJ C 326, 26.10.2012, pp. 391–407.

Consolidated version of the Treaty on the Functioning of the European Union OJ C 326, 26.10.2012, pp. 47–390.

Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector informationDirective (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information PE/28/2019/REV/1.

DUCUING, Ch. *The regulation of 'data': a new trend in the legislation of the European Union?* 06 April 2021 [online]. Available at: https://www.law.kuleuven.be/citip/blog/the-regulation-of-data-a-new-trend-in-the-legislation-of-the-european-union/

European Commission, 'Communication from the Commission to the European Parliament and the Council, the European Economic and Social Committee and the Committee of the Regions: A European Strategy for Data' (2020) 6.

European Commission, 'Communication from the Commission to the European Parliament and the Council: Guidance on the Regulation on a Framework for the Free Flow of Non-Personal Data in the European Union COM(2019) 250 Final' (2019).

EDPB-EDPS Joint Opinion 03/2021 on the Proposal for a Regulation of the European Parliament and of the Council on European Data Governance (Data Governance Act) (2021).

EDPB-EDPS Joint Opinion 03/2021 on the Proposal for a Regulation of the European Parliament and of the Council on European Data Governance (Data Governance Act)' (2021).

GRAEF, I., GELLER, R., HUSOVEC, M. *Towards a Holistic Regulatory Approach for the European Data Economy: Why the Illusive Notion of Non-Personal Data Is Counterproductive to Data Innovation.* (September 27, 2018). TILEC Discussion Paper No. 2018-029 [online]. Available at: https://ssrn.com/abstract=3256189

HAMUĽÁK, O., VARDANYAN, L., KOCHARYAN, H. The Global Reach of the Right to be Forgotten through the Lenses of the Court of Justice of the European Union. *Czech Yearbook of Public and Private International Law*. 2021, vol. 12, p. 211.

HAMUĽÁK, O., KISS, L. N., GÁBRIŠ, T., KOCHARYAN, H. "This Content is not Available in your Country" A General Summary on Geo-Blocking in and Outside the European Union. *International and Comparative Law Review*. 2021, vol. 21, no. 1, pp. 153–183, https://doi.org/10.2478/iclr-2021-0006.

KOCHARYAN, H., VARDANYAN, L., HAMUĽÁK, O., KERIKMÄE, T. Critical Views on the Right to Be Forgotten After the Entry Into Force of the GDPR: Is it Able to Effectively Ensure Our Privacy? *International and Comparative Law Review*. 2021, vol. 21, no. 2, pp. 96–115. https://doi.org/10.2478/iclr-2021-0015.

NARAYANAN, A. and FELTEN, Ew. *No Silver Bullet: De-Identification Still Doesn't Work.* (9 July 2014) [online]. Available at: https://freedom-to-tinker.com/2014/07/09/no-silver-bullet-de-identification-still-doesnt-work/

OHM, P. Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization, UCLA Law Review, Vol. 57, 2010, p. 1701 [online]. Available at: www.epic.org/privacy/reidentification/ohm_article.pdf

PAPAKONSTANTINOU, V., DE HERT, P. Post GDPR EU laws and their GDPR mimesis. DGA, DSA, DMA and the EU regulation of AI/ 1 April 2021 [online]. Available at: https://europeanlawblog.eu/2021/04/01/post-gdpr-eu-laws-and-their-gdpr-mimesis-dga-dsa-dma-and-the-eu-regulation-of-ai/

PAVELEK, O., ZAJÍČKOVÁ, D. Personal Data Protection in the Decision-Making of the CJEU Before and After the Lisbon Treaty. Baltic Journal of European Studies. Sciendo, vol. 11(2), 2021, p. 167.

Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC COM/2020/825 final.

Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act) COM/2020/842 final.

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 [2016] OJ L 119/2016.

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 (Text with EEA relevance.) PE/53/2018/REV/1OJ L 303, 28.11.2018, pp. 59–68.

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 (Text with EEA relevance.

Judgment of the Court of 5 June 2018. Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH. C-210/16, EU:C:2018:388.

Judgment of the Court of 6 November 2003. Criminal proceedings against Bodil Lindqvist. Case C-101/01.EU:C:2003:596.

Judgment of the Court (Grand Chamber) of 24 September 2019 Google LLC, successor in law to Google Inc. v Commission nationale de l'informatique et des libertés (CNIL). Case C-507/17, ECLI:EU:C:2019:772.

Judgment of the Court (Grand Chamber), 13 May 2014 Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González. C-131/12, EU:C:2014:317.

Judgment of the Court (Grand Chamber) of 6 October 2015. Maximillian Schrems v Data Protection Commissioner Case C-362/14, EU:C:2015:650.

Judgment of the Court (Second Chamber) of 19 October 2016. Patrick Breyer v Bundesrepublik Deutschland Case C-582/14. EU:C:2016:779.

Judgment of the Court (Second Chamber) of 9 March 2017. Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v Salvatore Manni Case C-398/15, EU:C:2017:197.

Judgment of the Court (Grand Chamber) of 5 June 2018. Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH. Case C-210/16, EU:C:2018:388.

Judgment of the Court (Second Chamber) of 14 February 2019. Sergejs Buivids v. Datu valsts inspekcija .C-345/17, EU:C:2019:131.

Judgment of the Court (Second Chamber) of 29 July 2019. Fashion ID GmbH & Co.KG v Verbraucherzentrale NRW eV Oberlandesgericht Düsseldorf Case C-40/17, ECLI:EU:C:2019:629.

Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1 Adopted on 4 May 2020 [online]. Available at: https://edpb.europa.eu

Judgment of the Court (Grand Chamber) of 16 July 2020. Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems C-311/18, ECLI:EU:C:2020:559.