

# CONSENT IN THE DECISION-MAKING PRACTICE OF THE SLOVAK DPA<sup>1</sup>

## SÚHLAS V ROZHODOVACEJ ČINNOSTI ÚRADU NA OCHRANU OSOBNÝCH ÚDAJOV SLOVENSKEJ REPUBLIKY

*Laura Bachňáková Rózenfeldová<sup>2</sup>*

<https://doi.org/10.33542/SIC2024-1-02>

### ABSTRACT

*Consent in personal data regulation presents one of the legal bases that legitimizes personal data processing realised by the controller. Despite the controller's frequent referral to consent as a legal basis for such processing, the fulfilment of legal conditions for valid consent provision can prove challenging to many controllers. In this regard, the paper examines the existing decision-making practice of the national data protection authority – the Office for Personal Data Protection of the Slovak Republic – concerning the deficiencies regarding data subject's consent provision that resulted in the initiation of administrative proceedings before this office and in the issuance of sanctions for the infringement of the applicable regulation on consent provision.*

### ABSTRAKT

*V kontexte právnej úpravy ochrany osobných údajov predstavuje súhlas jeden z právnych základov, ktorý legitimizuje spracúvanie osobných údajov prevádzkovateľom. Napriek častému odkazovaniu prevádzkovateľov na súhlas ako na právny základ takéhoto spracúvania, zostáva naplnenie právnych podmienok stanovených pre platné poskytnutie súhlasu problematickým pre mnohých prevádzkovateľov. V tejto súvislosti skúma predkladaný príspevok existujúcu rozhodovaciu prax vnútroštátneho dozorného orgánu – Úradu na ochranu osobných údajov Slovenskej republiky – týkajúcu sa nedostatkov súhlasu poskytnutého dotknutou osobou, ktoré vyústili do začatia administratívneho konania pred týmto úradom a do uloženia sankcií za porušenie aplikovateľnej právnej úpravy týkajúcej sa poskytnutia súhlasu.*

### I. INTRODUCTION

The applicable regulation of personal data protection contained in the General Data Protection Regulation<sup>3</sup> (hereinafter only referred to as 'GDPR') is based on different legal principles, the observance of which aims to ensure the achievement of the desired level of protection of the data subjects' personal data in practice. One of the most important legal principles in this regard present the principle of lawfulness. To ensure the lawfulness of personal data processing, the controller is required to demonstrate the legal basis applicable for

---

<sup>1</sup> This paper is funded by the Slovak Research and Development Agency on the basis of the Contract No. APVV-21-0336 within the scope of the project 'Analysis of judicial decisions using artificial intelligence' and the Contract No. VEGA 1/0431/23 within the scope of the project 'Competition for the interests of consumers and traders in the provision of digital content and digital services in the Digital Single Market, with an emphasis on legal and economic aspects'.

<sup>2</sup> JUDr., PhD., Univerzita Pavla Jozefa Šafárika v Košiciach, Právnická fakulta, Slovenská republika  
Pavol Jozef Šafárik University in Košice, Faculty of Law, Slovak Republic.

<sup>3</sup> Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), *OJ L 119*, 4.5.2016, p. 1–8.

different processing operations executed by it in practice. The individual legal bases for personal data processing are defined in Article 6 (1) GDPR and include, *inter alia*, the provision of the data subject's consent to the processing of their personal data for one or more specified purposes.

Data subject's consent presents one of the most commonly referred to legal bases for personal data processing.<sup>4</sup> Consent is often preferred by controllers, as its provision by the data subject may seem like the easiest legal basis to obtain in practice, especially considering the possible legal uncertainty that may be connected with the application of other legal bases in this regard. Nonetheless, the preferred practice of acquiring consent even in cases where other legal bases may be applicable is in direct conflict with the current personal data protection regulation, that recognizes consent as only one of the possible legal bases for personal data processing, the application of which should not be the first, but often the last option legitimizing controller's processing operations. The controller is, therefore, obligated to properly consider the applicability of other legal bases, and only in case of their unsuitability should consent of the data subject be obtained.

If controller concludes that consent presents the suitable legal basis for personal data processing, it is obligated to ensure the validity of consent provision. Article 4 (11) GDPR defines consent of the data subject as "*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.*" In this regard, the following elements of valid consent provision can be distinguished – consent is

- a) freely given,
- b) specific,
- c) informed and
- d) presents an unambiguous indication of data subject's wishes.

These criteria must be fulfilled cumulatively, which "*creates a high threshold for valid consent. Also contributing to this high threshold is the data protection authorities' tendency to interpret each of the criteria strictly.*"<sup>5</sup> Given the fact that the objective of this paper is not to provide a comprehensive overview of these elements, we refer to the explanation provided in this regard by the European Data Protection Board in its Guidelines 05/2020 on consent under Regulation 2016/679<sup>6</sup> (hereinafter referred to only as "Guidelines 05/2020 on consent"). Selected elements are also examined in more details in the following chapters of this paper.

As Bygrave states, "*rules requiring data subject consent also make up and manifest a general core principle of data protection law, namely the principle of data subject influence, which holds that individuals should be able to participate in, and have a measure of influence over, the processing of data on them by others.*"<sup>7</sup> The objective to strengthen the data subject's control over his or her personal data was also one of the main objectives of the GDPR, reflecting the need to unify the differing approaches to consent interpretation in different Member States. Its achievement, however, required a new approach to the interpretation of consent and provision of clearer instructions regarding conditions ensuring its validity.

Additional conditions for valid consent provision include the obligation of the controller to be able to demonstrate that the data subject has consented to personal data processing and the

---

<sup>4</sup> Other commonly applied legal bases in practice include, e.g. the compliance with legal obligations of the controller (Article 6 (1) (c) GDPR) and processing necessary for the performance of the contract (Article 6 (1) (b) GDPR).

<sup>5</sup> BYGRAVE, L. A. Commentary to Article 4 (11) GDPR. In: Kuner, Ch. et al. The EU General Data Protection Regulation (A Commentary). Oxford: Oxford University Press, 2020. ISBN: 978-0-19-882649-1. P. 181.

<sup>6</sup> European Data Protection Board. Guidelines 05/2020 on consent under Regulation 2016/679. Version 1.1. Adopted on 4. May 2020.

<sup>7</sup> BYGRAVE, L. A. Data Protection Law: An International Perspective. Oxford: Oxford University Press, 2014. ISBN: 9780191758904. P. 158.

provision of relevant information prior to consent provision, including informing the data subject about their right to withdraw previously given consent. Consent should cover all processing activities carried out for the same purpose and when the processing has multiple purposes, consent should be given for all of them.<sup>8</sup>

Specific conditions for consent provision apply in the following situations:

- a) if consent is provided for scientific research purposes (Article 89 GDPR),
- b) with regard to the provision of information society services<sup>9</sup> to children (Article 8 GDPR)
- c) in relation to the processing of special categories of personal data (Article 9 GDPR).

As regards personal data processing for scientific research purposes, Article 89 GDPR subjects such processing operations to appropriate safeguards for the rights and freedoms of the data subjects, the objective of which is to ensure that technical and organizational measures are in place, in particular to ensure compliance with the data minimization principle. Specific conditions for consent provision may relate in this regard to the obligation to obtain specific consent, given the fact that it may not be possible to fully identify the purpose of personal data processing at the time of data collection;<sup>10</sup> in this case, the purpose of personal data processing may be described in a more general manner. However, this possibility does not exclude the need for specific consent provision. EDPB specifies in its Guidelines 05/2020 on consent multiple methods that may be employed by the controllers to compensate for the more general specification of processing purposes in practice.

As Article 8 GDPR specifies, processing of personal data in relation to the provision of information society services to children below the age of 16 years “*will be lawful only if and to the extent that consent is given or authorized by the holder of parental responsibility over the child,*” and the controllers have the obligation to make reasonable efforts to verify the fulfilment of this condition, taking into consideration available technology.

Processing of special categories of personal data is, in principle, prohibited. However, Article 9 (2) (a) provides an exception to this rule, as it allows for processing of special categories of personal data on the basis of *inter alia* an explicit consent of the data subject for one or more specified purposes. Here, consent provides an exemption from the primarily prohibited processing of concerned categories of data. As Georgieva and Kuner specify in this regard, „*this is a higher threshold than in Article 6 (1) (a) GDPR, which mentions ‘consent’ as a legal basis for data processing without requiring that it be explicit.*“<sup>11</sup>

## II. METHODOLOGY

From a methodological point of view, this paper employs a systematic content analysis that can be defined as a methodical, replicable technique for compressing many words of text into fewer content categories based on explicit coding rules<sup>12</sup>. In this regard, the following stages of systematic content analysis in legal research can be distinguished:

---

<sup>8</sup> Recital 32 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), *OJ L 119, 4.5.2016, p. 1–8.*

<sup>9</sup> In this regard, see the analysis of the newly adopted Digital Services Act regulating the new obligations of information society service providers provided by RUDOHRADSKÁ, S. – TREŠČÁKOVÁ, D. Proposals for the Digital Markets Act and Digital Services Act – broader considerations in context of online platforms. In: EU 2021 – the future of the EU in and after the pandemic: International Scientific Conference: Conference book of proceedings. Osijek: Sveučilište Josipa Jurja Strossmayera u Osijeku, 2021. ISBN 24599425. S. 487-500.

<sup>10</sup> See Recital 33 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), *OJ L 119, 4.5.2016, p. 1–8.*

<sup>11</sup> GEORGIEVA, L. - KUNER, CH. Commentary to Article 9 GDPR. In: Kuner, Ch. et al. The EU General Data Protection Regulation (A Commentary). Oxford: Oxford University Press, 2020. ISBN: 978-0-19-882649-1. P. 377.

<sup>12</sup> WEBER, R. : Basic content analysis. SAGE Publications, Inc., Vol. 49, 1990.

1. determination of a suitable research question or hypothesis,
2. collection of data for analysis;
3. coding of the data,
4. drawing conclusions and observations, and
5. discussion of findings in a manner understandable to the legal community.<sup>13</sup>

As regards the first step in the systematic content analysis, we stipulate the following research questions:

RQ1: *What factual circumstances defined the examined infringements of controller's obligations concerning consent provision?*

RQ2: *What was the nature of these infringements, specifically the infringement of which specific obligations were determined?*

RQ3: *How severe were the sanctions imposed on infringing controllers by the DPA?*

To answer these research questions and to examine the controller's adherence to the obligations ensuring valid provision of consent in practice, this paper analyses the decisions of the national data protection authority – the Office for Personal Data Protection of the Slovak Republic (hereinafter referred to as the 'DPA') that stated the infringement of different requirements regarding consent provision. In Slovakia, no official database of decisions adopted by the DPA has been established. The analysis provided in this paper is, therefore, based on a dataset of decisions obtained directly from the DPA based on a freedom of information request in accordance with the Slovak Act No. 211/2000 Coll. on free access to information ('Freedom of Information Act'). The decisions obtained from the DPA included 180 decisions adopted in the time period from November 2018 to October 2022. The decisions provided therefore reflect the emerging enforcement practices of the DPA after GDPR adoption. In total, 13 decisions concerning the infringement of obligations regarding consent provision have been identified from the total of 180 decisions provided by the DPA.

The objective of the data coding stage is to create a suitable representation of individual decisions in a code representing individual attributes. In this paper we use three types of attributes, namely numerical (e.g., amount of fine), categorical (e.g., type of operator), and binary. Binary attributes represent the occurrence or the absence of a specific attribute. To illustrate, binary attributes specify whether a fine was issued by the DPA as a result of the proceedings or not, or, in case of different possibilities for proceedings' beginning, the specific form of proceedings' initiation (e.g., proceedings is or is not initiated on the basis of the DPA' initiative).

The analysis resulted in the selection and collection of a set of attributes classified into the following categories:

- a) decision identification - attributes: decision number, adoption date, identification of the controller, nature of the controller, nature of the proceeding;
- b) the initiative for the proceedings beginning – attributes: the initiative of the DPA, controller's infringement notice, motion of a third party, nature of the third party (if identified);
- c) type of infringement – attributes: the provisions of GDPR infringed, factual description of the infringement, categorization of the infringement into selected categories;
- d) the sanction imposed, specifically the amount of fine issued and/or obligations imposed on the controller by the DPA.

The attributes identified in this regard were used for statistical analysis of the DPA's decisions, the results of which are provided in the following chapters of this paper.

---

<sup>13</sup> M. SALEHIJAM: The value of systematic content analysis in legal research. *Tilburg Law Review*, 23(1-2), 2018. <<https://tilburglawreview.com/articles/10.5334/tilr.5>> Accessed 21. November 2023.

### III. RELATED WORKS

The definition of consent and validity of its provision in relation to personal data protection regulation remains a highly debated issue in the academic literature. Breen et al<sup>14</sup> explored the philosophical background of consent and attempted to develop an understanding of it in the context of the growing influence of information systems and the data-driven economy. Other authors examined the notion of consent and the procedure for its provision in relation to the use of cookies that enable collection and processing of personal data of users visiting a website – an issue also highly relevant for this paper. The relevant studies include papers analysing the notion of consent prior to GDPR adoption provided e.g., by Koops<sup>15</sup> that investigated new personal data protection intentions in the EU law including proposed changes in the consent definition. On the other hand, Aladeokin et. al.<sup>16</sup> examined cookies from the perspective of privacy protection laws of different Commonwealth countries. Authors' report contains a study of adherence to privacy protection laws by different categories of websites (e.g., e-commerce, news and media) when setting cookies on users' computer systems. Moreover, Jackson<sup>17</sup> focuses on consent and its obtaining from the perspective of business companies. Other authors discussed the issues regarding the regulation of the right to be forgotten and the right for revoking consent under the GDPR<sup>18</sup>. Some papers dealt with the issue of consent in specific areas (IoT<sup>19</sup>, Big Data, etc.). Similarly, the paper of de Matos et al.<sup>20</sup> examined the consumer consent requirements and evaluated the effect of enhanced consent on consumer opt-in behavior and on firm behavior and outcomes after consent is solicited. Nonetheless, no comprehensive studies examining the decision-making practice of national DPAs regarding consent provision have been identified in this regard. To overcome this deficiency, this paper examines the existing decision-making practice of the national DPA and provides an overview of the relevant case-law, distinguishing different categories of infringements relating to consent provision in this regard.

### IV. CONSENT IN THE DECISION-MAKING PRACTICE OF THE DPA

The objective of the DPA's proceedings on personal data protection that resulted in the issuance of the decisions analysed in this paper, was to determine whether the personal data protection rights of natural persons regarding the provision of their consent were infringed and, in the event of infringement detection, to sanction these infringements through the adoption of corrective measures or a fine, if these were deemed reasonable and effective.

The administrative proceedings analysed in regard were initiated either by the motion of the concerned person (6 decisions) or by the DPA itself (7 decisions). The subjects, against which these proceedings were directed, included primarily private companies (12 decisions), and in one decision a state authority (the Slovak Office of Standards, Metrology and Testing).

The analysis of the individual decisions of the DPA concerning infringements of consent conditions revealed the most common types of infringements related to data subject consent

---

<sup>14</sup> BREEN, S. - OUAZZANE, K. - PATEL, P. GDPR: Is your consent valid? *Business Information Review*, Vol. 37, No. 1, 2020. P. 19-24. DOI: <https://doi.org/10.1177/0266382120903254>.

<sup>15</sup> KOOPS, B. J. The trouble with European data protection law. *International Data Privacy Law*, 4(4), 2012. P. 250-261. DOI: 10.1093/idpl/ipu023.

<sup>16</sup> ALADEOKIN, A. - ZAVARSKY, P. - MEMON, N. Analysis and compliance evaluation of cookies-setting websites with privacy protection laws. In *Digital Information Management (ICDIM), 2017 Twelfth International Conference on Digital Innovation Management (ICDIM)*, pp. 121-126. DOI: 10.1109/ICDIM.2017.8244646.

<sup>17</sup> JACKSON, O. Businesses retreating from consent under GDPR. *International Financial Law Review*. 2018.

<sup>18</sup> See, e.g., POLITOU, E. - ALEPIS, E. - PATSAKIS, C. Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions. *Journal of Cybersecurity*. Vol. 4, Issue 1, 2018. ISSN: 2057-2093. DOI: 10.1093/cybsec/tyy001.

<sup>19</sup> O'CONNOR, Y. - ROWAN, W. - LYNCH, L. - HEAVIN, C. Privacy by Design: Informed Consent and Internet of Things for Smart Health. *Procedia Computer Science*, Vol. 113, 2017. P. 653-658. DOI: 10.1016/j.procs.2017.08.329.

<sup>20</sup> DE MATOS, M.G. – ADJERID, I. Consumer consent and firm targeting after GDPR: the case of a large Telecom provider. *Management Science*, Vol. 68, No. 5, 2021. DOI: 10.1287/mnsc.2021.4054.

provision. These infringements can be categorized into the following categories (provided with decreasing incidence):

1. the formulation of consent did not include all of the required information and/or provided incorrect information to the data subject,
2. the provision of consent by the data subject was not free,
3. the consent was not provided in an active manner,
4. the controller continued the processing of data subject's personal data even after the withdrawal of the previously given consent to such processing,
5. the consent was not a suitable legal basis for personal data processing.

Closer examination of these infringement categories is provided in the following chapters of this paper.

### **1. Deficiencies as regards the provision of an informed consent**

One of the conditions for valid provision of data subject's consent is that the consent provided is informed. This condition is closely connected to the transparency principle that requires personal data to be processed in a transparent manner in relation to the data subject (Article 5 (1) (a) GDPR). In general, information to be provided to the data subject should be provided prior to any personal data processing so as to ensure that the data subject can make informed decisions, understand the nature of personal data processing, and retain control over it. In the event that the consent provided by the data subject is considered as not informed, such consent provision will be invalid and may result in the infringement of the lawfulness principle (Article 6 GDPR), if no other legal bases for personal data processing are applicable in a given case.

The European Data Protection Board provides in its Guidelines 05/2020 on consent the minimum content requirements for consent for it to be considered as informed. These include:

- a) "the controller's identity,
- b) the purpose of each of the processing operations for which consent is sought,
- c) what (type of) data will be collected and used,
- d) the existence of the right to withdraw consent,
- e) information about the use of the data for automated decision-making in accordance with Article 22 (2) (c) where relevant, and
- f) on the possible risks of data transfers due to absence of an adequacy decision and appropriate safeguards as described in Article 46."<sup>21</sup>

In this regard the European Data Protection Board also notes that "*depending on the circumstances and context of a case, more information may be needed to allow the data subject to genuinely understand the processing operations at hand.*"<sup>22</sup>

The form for the provision of information regarding the data subject consent is not defined in the applicable legislation. Consent should be given "by a clear affirmative act, e.g., by a written statement, including by electronic means or an oral statement" (Recital 32 GDPR). Further clarification is provided in Article 7 (2) GDPR, according to which "*if the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented (...) in an intelligible and easily accessible form, using clear and plain language.*" The formulation of the data subject's consent and information provided within it should be easily understandable to an average person, easily accessible and distinguishable from other matters (not hidden in lengthy privacy or personal data policies) and must allow the data subject to understand the nature of the personal data processing to which they agree to.

---

<sup>21</sup> European Data Protection Board. Guidelines 05/2020 on consent under Regulation 2016/679. Version 1.1. Adopted on 4. May 2020. pp. 15-16.

<sup>22</sup> Ibid. p. 16.

As regards the analysis provided in this paper, the deficiencies relating to the provision of an informed consent proved to be the most common types of issues identified by the DPA in its case-law concerning consent provision. Specifically, 7 decisions included infringements that can be classified into this category of consent infringement types. The individual infringements are described below.

The first decision of the DPA (No. 00049/2022-Os-14)<sup>23</sup> concerned the provision of incorrect information to the data subject by the controller on its website. The controller in question published on its website (in relation to the information about the data subject's right to withdraw previously given consent with personal data processing provided for the purposes of sending commercial notifications, i.e., for direct marketing purposes) inactive email address, through which data subjects could have contacted the company with inquiries about the processing of their personal data. The DPA stated in this regard that by referring to inactive email address the controller failed to act transparently towards data subjects and misled them. This conduct was evaluated by the DPA as the infringement of the transparency principle (Article 5 (1) (a) GDPR) that was sanctioned with a fine in the amount of 1.000,- Eur. The DPA also imposed specific measures to rectify the infringement, specifically by stipulating an obligation of the controller to provide data subjects with all information necessary, including correct information regarding the data subject's right to withdraw its consent with personal data processing and a suitable method to do so.

The second decision of the DPA (No. 00006/2021-Os-2)<sup>24</sup> sanctioned the non-provision of concise, understandable, and explicit information about the purposes of personal data processing in the registration form provided by the controller, specifically in relation to the consent to be provided for the data subject's registration in the controller's customers' club. The purpose omitted from the registration form concerned, specifically, targeted offer of goods and services to the registered members of the controller's customers' club. The DPA classified this infringement as the infringement of the transparency principle (Article 5 (1) (a) GDPR). The summary amount of fine imposed on the controller was 2.900,- Eur. It must be, however, noted that this fine was issued for the combination of multiple infringements committed by this controller and not only for the infringement of obligations relating to consent provision. The controller was also obligated to adopt measures to rectify the infringement, specifically to amend the registration form in accordance with the transparency principle so as to inform the data subject about the absenting purposes for personal data processing.

The third decision of the DPA (No. 00374/2022-Os-3)<sup>25</sup> identified the infringement of Article 12 (1) and 13 (1, 2) GDPR, the nature of which consisted of the failure to provide relevant information to data subjects regarding consent, the provision of which was requested for the purpose of sending information about products and news to data subjects. According to the DPA, the controller was obligated to provide, i.e., information about the purposes of personal data processing, the scope of personal data processed, duration of personal data storage and data subject rights related to personal data processing based on consent. This infringement (committed in this case by a state authority) was sanctioned with the imposition of a fine in the amount of 200,- Eur (the lowest fine imposed by the DPA on controllers in this regard). No specific measures were imposed by the DPA due to the removal of identified deficiencies by the controller.

Another decision of the DPA (No. 00517/2020-Os-10)<sup>26</sup> sanctioned the infringement of the transparency principle (Article 5 (1) (a) GDPR) and Article 13 (2) (a, b) GDPR committed by the controller's failure to provide information to data subjects about the legal basis for personal

<sup>23</sup> Decision of the Office for Personal Data Protection of the Slovak Republic No. 00049/2022-Os-14 adopted 29.9.2022.

<sup>24</sup> Decision of the Office for Personal Data Protection of the Slovak Republic No. 00006/2021-Os-2 adopted 4.1.2021.

<sup>25</sup> Decision of the Office for Personal Data Protection of the Slovak Republic No. 00374/2022-Os-3 adopted 8.2.2022.

<sup>26</sup> Decision of the Office for Personal Data Protection of the Slovak Republic No. 00517/2020-Os-10 adopted 13.8.2020.

data processing based on data subject's consent and information about data subject's rights, including the right to withdraw consent. The infringement was sanctioned with the fine in the amount of 2.100,- Eur (similarly this fine encompassed multiple different infringements of the controller in question). No other measures were imposed as all identified deficiencies were removed by the controller.

Further decision of the DPA (No. 00705/2020-Os-21)<sup>27</sup> concerned the non-provision of relevant information to data subjects that visited the controller's website about personal data collected and processed with the help of cookies<sup>28</sup>. Specifically, the controller did not inform data subjects about personal data collected and about the necessity of such collection for the functioning of the website prior to consent provision. Only after consenting the data subject gained access to the document titled 'Personal data protection' that defined purposes for the processing of personal data collected through cookies and the duration of consent validity. This approach is, however, in conflict with the controller's obligation to provide relevant information about personal data processing prior to such processing or, at the latest, at the time of personal data collection (infringement of the transparency principle – Article 5 (1) (a) in connection with Article 13 GDPR). The fine issued in this regard by the DPA reached the amount of 700,- Eur. The controller was also obligated to ensure that the document titled 'Personal data protection' is accessible on its website even without the data subject's consent with the processing of personal data through cookies.

Another decision of the DPA (No. 00770/2020-Os-1)<sup>29</sup> regarded the infringement of the transparency principle (Article 5 (1) (a) GDPR) committed by the provision of inaccurate information about personal data processing, specifically by referencing the previously applicable personal data protection legislation (Act No. 122/2013 Coll. on personal data protection as amended) in the formulation of consent with personal data processing. The fine imposed was in the amount of 500,- Eur.

The last decision of the DPA (00387/2022-Os-3)<sup>30</sup> identified the infringement of the fairness principle (Article 5 (1) (a) GDPR) committed through the provision of inaccurate information to data subject by the controller, specifically by obtaining consent with the processing of biometric data (biometric signature) for individual identification of natural persons for longer period of time than such data was actually processed. This infringement was sanctioned with a fine in the amount of 4.000,- Eur and the DPA imposed an obligation on the controller to ensure the consistency of the period of time for which consent was provided by the data subject with the actual duration of personal data processing (in relation to the fulfilment of obligations stemming from the contract on the provision of public services).

The above-specified deficiencies relating to the provision of an informed consent demonstrate that the most commonly occurring types of violations regarding consent provision are classified by the DPA as the infringement of the transparency principle, and not the lawfulness principle. This confirms the close connection between these principles, also considering the content of the transparency principle as defined in Articles 13 (1) (c) and 14 (1) (c) GDPR that require the provision of information on the purposes of the processing for which the personal data are intended as well as the legal basis for the processing to the data subject. Nonetheless, a reference to the lawfulness principle is advisable given the fact that these violations primarily relate to the failure to ensure one of the conditions for valid consent provision, therefore invalidating the legal basis for personal data processing selected by the controller. Such an approach is also in line with the EDPB Guidelines 05/2020 on consent that

---

<sup>27</sup> Decision of the Office for Personal Data Protection of the Slovak Republic No. 00705/2020-Os-21 adopted 12.11.2020.

<sup>28</sup> See RÓZENFELDOVÁ, L. Protection of privacy and personal data as regards the use of cookies. In: *STUDIA IURIDICA Cassoviensia*, Vol. 8, No. 1, 2020. ISSN: 1339-3995.

<sup>29</sup> Decision of the Office for Personal Data Protection of the Slovak Republic No. 00770/2020-Os-1 adopted 20.5.2020.

<sup>30</sup> Decision of the Office for Personal Data Protection of the Slovak Republic No. 00387/2022-Os-3 adopted 28.3.2022.



specify that the consequence of not complying with the requirements for informed consent is that consent will be invalid and the controller may be in breach of Article 6 of the GDPR.<sup>31</sup> Moreover, these deficiencies relate either to the controller's failure to provide the relevant information to data subjects required by the applicable legislation, or the provision of inaccurate information. The short summary of the above-described case-law is provided in Table 1.

*Table 1 Decisions identifying deficiencies in relation to the provision of an informed consent*

Decision No.	Infringement	Description of the infringement	Fine
00049/2022-Os-14	Article 5 (1) (a) GDPR	provision of incorrect information to the data subject by a private company on its website	1.000,-€
00006/2021-Os-2	Article 5 (1) (a) GDPR	non-provision of concise, understandable, and explicit information about the purposes of personal data processing in the registration form	2.900,-€
00374/2022-Os-3	Article 12 (1) and 13 (1, 2) GDPR	failure to provide relevant information to data subjects regarding consent provision	200,-€
00517/2020-Os-10	Article 5 (1) (a) and 13 (2) (a, b) GDPR	failure to provide information to data subjects about the legal basis for personal data processing based on data subject's consent and information about data subject's rights, including the right to withdraw consent	2.100,-€
00705/2020-Os-21	Article 5 (1) (a) in connection with Article 13 GDPR	non-provision of relevant information to data subjects regarding personal data collected	700,-€
00770/2020-Os-1	Article 5 (1) (a) GDPR	provision of inaccurate information about personal data processing	500,-€
00387/2022-Os-3	Article 5 (1) (a) GDPR	provision of incorrect information to the data subject about the duration of personal data processing	4.000,-€

## 2. Free provision of consent

Another condition to be applied in relation to consent provision determines that any consent of the data subject with personal data processing should be freely given. This condition ensures real choice and control of the data subject over their decision to consent with personal data processing. Recital 42 GDPR stipulates that consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment. As highlighted by the WP29 in several Opinions, "consent can only be valid if the data subject is able to exercise a real choice, and there is no risk of deception, intimidation, coercion, or significant negative consequences (e.g., substantial extra costs) if he/she does not consent. Consent will not be free in cases where there is any element of compulsion, pressure, or inability to exercise free will."<sup>32</sup>

Article 7 (4) GDPR specifies circumstances to be considered when assessing whether consent was freely given in relation to the performance of a contract. These include whether the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract. Article 7 (4) GDPR is, however, only relevant where the requested data are not necessary for the

<sup>31</sup> European Data Protection Board. Guidelines 05/2020 on consent under Regulation 2016/679. Version 1.1. Adopted on 4. May 2020. p. 63.

<sup>32</sup> Ibid. P. 9.

performance of the contract, and the performance of that contract is made conditional on the obtaining of these data on the basis of consent.<sup>33</sup>

The failure to ensure the free provision of data subject's consent was determined in five decisions of the DPA. These decisions are examined in more detail below.

The first relevant decision (No. 01107/2020-Os-7)<sup>34</sup> concerned the infringement of the fairness and transparency principle (Article 5 (1) (a) GDPR) committed by the controller by the inclusion of consent with personal data processing by third parties (for the purpose of confirming data subject's solvency) in the document titled 'General conditions' that formed an inseparable part of the vehicle rental agreement to be concluded between the controller and the data subject. In line with the EDPB Guidelines 05/2020 on consent, "if consent is bundled up as a non-negotiable part of terms and conditions, it is presumed not to have been freely given."<sup>35</sup> This infringement was sanctioned with a fine in the amount of 2.300,- Eur. No additional obligations were imposed given the removal of the identified deficiencies by the controller.

Another DPA's decision (No. 00296/2020-Os-17)<sup>36</sup> identified the infringement of Article 7 (4) GDPR that concerned the conditioning of any further communication of the controller with the data subject on the provision of their consent with personal data processing, which was, however, not necessary for the possible future conclusion of a contract of sale. As explained by the EDPB, Article 7 (4) GDPR "seeks to ensure that the purpose of personal data processing is not disguised nor bundled with the provision of a contract of a service for which these personal data are not necessary. In doing so, the GDPR ensures that the processing of personal data for which consent is sought cannot become directly or indirectly the counter-performance of a contract."<sup>37</sup>

Further relevant decision of the DPA (No. 00705/2020-Os-21)<sup>38</sup> sanctioned the controller for its practice of obtaining data subject's consent with the use of cookies on its website. The controller conditioned the data subject's access to the document containing information on personal data processing on the provision of consent with personal data processing by the data subject, therefore infringing Article 4 (11) GDPR requiring that consent is freely given. The fine issued in this regard by the DPA reached the amount of 700,- Eur. As explained in this previous chapter, the controller was also obligated to make the documentation accessible on its website without the need for the provision of the data subject's consent with the processing of personal data through cookies.

In all of the above examined cases, the DPA identified deficiencies that related to the conditioning of certain activities (access to documentation or conclusion of contractual relations) on the provision of data subject's consent – practices, that are in clear conflict with the requirement of free provision of data subject's consent with personal data processing. However, the infringement of the requirement of free consent provision can also be committed in a different manner, specifically by the controller's failure to distinguish different purposes, for which consent is provided. Recital 43 GDPR specifies in this regard that consent is also presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case. Therefore, if personal data is to be processed for different purposes, the controller is obligated to obtain consent for each purpose (if consent is selected as the applicable legal basis for such processing) and not bundle all processing purposes into one consent formulation. As the EDPB

---

<sup>33</sup> Ibid. P. 11.

<sup>34</sup> Decision of the Office for Personal Data Protection of the Slovak Republic No. 01107/2020-Os-7 adopted 14.12.2020.

<sup>35</sup> European Data Protection Board. Guidelines 05/2020 on consent under Regulation 2016/679. Version 1.1. Adopted on 4. May 2020. P. 7.

<sup>36</sup> Decision of the Office for Personal Data Protection of the Slovak Republic No. 00296/2020-Os-17 adopted 30.11.2020.

<sup>37</sup> European Data Protection Board. Guidelines 05/2020 on consent under Regulation 2016/679. Version 1.1. Adopted on 4. May 2020. P. 10.

<sup>38</sup> Decision of the Office for Personal Data Protection of the Slovak Republic No. 00705/2020-Os-21 adopted 12.11.2020.

states, “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. When data processing is done in pursuit of several purposes, the solution to comply with the conditions for valid consent lies in granularity, i.e. the separation of these purposes and obtaining consent for each purpose.”<sup>39</sup>

The issues with consent granularity were identified in two further decisions of the DPA. In the first decision (No. 00006/2021-Os-2)<sup>40</sup>, the DPA examined the infringement of the lawfulness principle (Article 5 (1) (a) GDPR) committed by the bundling of two different purposes (marketing and communication purpose and personal data processing in the scope defined in the document titled ‘Principles of personal data processing’) in one consent declaration contained in the registration form of the controller. Similarly, in the DPA’s decision (No. 00517/2020-Os-10)<sup>41</sup>, the DPA identified the infringement of the lawfulness principle consisting of the controller’s failure to provide the data subject with the possibility to consent with the processing of photographs used for different processing purposes. This infringement was sanctioned with the fine of 2.100,- Eur.

### 3. Inactive provision of consent

The legal definition of consent provided in Article 4 (11) GDPR emphasises that consent presents an unambiguous indication of the data subjects’ wishes, by which they, by a statement or by a clear affirmative action, agree to the processing of personal data relating to them. This provision specifies another condition for valid consent provision, specifically the need to ensure that the consent provided by the data subject is provided in an active manner, meaning that data subject have taken a deliberate action to consent to particular processing operations. Active provision of consent may include consenting through a written statement, including by electronic means, or an oral statement. Recital 32 GDPR specifies in this regard that “this could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject’s acceptance of the proposed processing of their personal data. Silence, pre-ticked boxes, inactivity of the data subject or merely proceeding with a service cannot constitute an active indication of the data subject’s choice”.

The infringement of this condition for valid consent provision was identified in three decisions of the DPA. The individual infringements are described below.

The first decision of the DPA (No. 00296/2020-Os-17)<sup>42</sup> concerned the infringement of Article 7 (4) GDPR committed by the controller by its failure to obtain consent of the data subject in an unambiguous confirmatory act, as the consent provided was included in a pre-ticked box in the controller’s consent form. As specified above, consent expressed through a pre-ticked box cannot constitute an active demonstration of the data subject’s consent to personal data processing. As DPA further clarified, valid provision of consent necessitates the application of measures excluding any doubts about the data subject’s objective to consent, specifically in an online environment, where the use of default options that the data subject must change in order to refuse personal data processing cannot constitute the provision of an unambiguous consent. The DPA sanctioned this infringement with a fine in the amount of 1.100,- Eur and imposed an obligation on the controller to ensure the compliance of consent provision with GDPR. In this regard, a referral to the infringement of Article 4 (11) GDPR

---

<sup>39</sup> European Data Protection Board. Guidelines 05/2020 on consent under Regulation 2016/679. Version 1.1. Adopted on 4. May 2020. P. 12.

<sup>40</sup> Decision of the Office for Personal Data Protection of the Slovak Republic No. 00006/2021-Os-2 adopted 4.1.2021.

<sup>41</sup> Decision of the Office for Personal Data Protection of the Slovak Republic No. 00517/2020-Os-10 adopted 13.8.2020.

<sup>42</sup> Decision of the Office for Personal Data Protection of the Slovak Republic No. 00296/2020-Os-17 adopted 30.11.2020.

would be more suitable, as Article 7 (4) focuses on freely given consent and not on the active manner of consent provision.<sup>43</sup>

Another DPA's decision relevant in this regard (No. 00374/2022-Os-3)<sup>44</sup> regarded the infringement of the transparency principle (Article 5 (1) (a) GDPR) committed by the controller by the inclusion of consent with personal data processing in a pre-ticked box (without provision of any further information on processing operations to be realized). This decision concerned the infringement of the state authority and was sanctioned with the imposition of a fine in the amount of 200,- Eur. No specific measures were imposed due to the removal of identified deficiencies by the controller. Similarly as in the previous decision, a referral to the infringement of Article 4 (11) GDPR would be more suitable with regard to the description of this infringement.

The last decision of DPA (No. 00704/2020-Os-1)<sup>45</sup> sanctioned the infringement of the lawfulness principle (Article 5 (1) (a) GDPR) committed by the controller's failure to demonstrate that consent of data subjects (unregistered visitors of the controller's website) was provided in an active manner. Consistently with the previously examined decisions, the controller used a pre-ticked box to obtain data subject's consent with personal data processing. This infringement was sanctioned with a fine in the amount of 2.500,- Eur. No additional obligations were imposed considering the removal of the identified deficiencies by the controller.

Considering the above examined decisions, the common deficiency occurring in all of them with regard to active consent provision concerns the use of pre-ticked boxes by controllers on their websites that do not provide the data subject with the opportunity to express their unambiguous agreement (or disagreement) with personal data processing. Presuming data subject's consent is, however, in direct conflict with the applicable opt-in principle requiring active provision of consent. The previously applicable opt-out principle (presuming the provision of consent unless different indication of the data subject's wishes is provided) is no longer acceptable under current legislation.

The use of pre-ticked boxes for consent provision presents an ongoing issue for controllers that continue to include such boxes in their forms for consent collection, particularly in the online environment. However, the issue persists also in the written form, e.g. in contractual agreements, as was demonstrated in the case of the controller – telecommunications services provider Orange România SA - sanctioned by the Romanian DPA for the inclusion of a pre-ticked boxes in its contractual forms. The case was also considered by the CJEU, that stated in its decision C-61/19 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 the 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 (...).”*<sup>46</sup>

#### **4. Failure to end personal data processing after consent withdrawal**

Whereas the first three categories of deficiencies related directly to the nature of consent provided by the data subject, this category examines the controller's behavior after consent provision, specifically the consistency of its personal data processing operations with the content of the consent provided and the limitation of its duration through consent withdrawal. As Article 7 (3) GDPR prescribes, the data subject possesses the right to withdraw his or her

---

<sup>43</sup> This aspect is examined in the previous chapter of this paper.

<sup>44</sup> Decision of the Office for Personal Data Protection of the Slovak Republic No. 00374/2022-Os-3 adopted 8.2.2022.

<sup>45</sup> Decision of the Office for Personal Data Protection of the Slovak Republic No. 00704/2020-Os-1 adopted 1.6.2020.

<sup>46</sup> Judgement of the Court of Justice of the European Union C-61/19 of 11 November 2020 Orange Romania. ECLI:EU:C:2020/901. P. 52.

consent at any time. Any personal data processing realized prior to consent withdrawal remains lawful in this regard if it was based on valid consent of the data subject. In this respect, the examined case law included two decisions sanctioning the controller's failure to adhere to the agreed duration of personal data processing by continuing the processing operations even after the data subject's consent withdrawal. The first decision (No. 00051/2021-Os-16)<sup>47</sup> concerned the controller's failure to cease personal data processing after consent withdrawal, specifically by continuing to send marketing communication to data subject's personal email address. This constituted the infringement of the lawfulness principle (Article 5 (1) (a) GDPR), as after consent withdrawal, the controller lacked any legal basis that would legitimize such processing operations. The controller was sanctioned with a fine in the amount of 500,- Eur. The identical infringement was also sanctioned in another DPA's decision (No. 00052/2021-Os-16)<sup>48</sup>, where the same sanction was imposed on the controller.

### **5. Consent as an unsuitable legal basis for personal data processing**

The last category identified focuses on the issues connected with the selection of the applicable legal basis legitimizing personal data processing. The lawfulness principle requires the selection of a suitable legal basis prior to the commencement of any personal data processing operations. The responsibility to choose the correct legal basis for processing lies on the controller. If consent is selected as the basis for personal data processing, the controller must also be able to demonstrate that the data subject has consented to the processing of their personal data (Article 7 (1) GDPR).

In the examined case-law, only one decision stipulated that consent did not constitute the appropriate legal basis for personal data processing. This DPA's decision (No. 01339/2021-Os-10)<sup>49</sup> concerned the infringement of the lawfulness, fairness and transparency principle (Article 5 (1) (a) GDPR), where the controller has chosen the incorrect legal basis for the processing and evaluation of personal characteristics of different data subjects (psychodiagnostics, psychometric). Specifically, the controller realized a survey, the objective of which was to collect data and analyse personal characteristics of its employees and jobseekers, including profiling, without suitable legal basis. The controller based its processing operations on consent, however the DPA stated in its conclusion that the appropriate legal basis applied should have been the legitimate interest (Article 6 (1) (f) GDPR). The reason for this conclusion was the recognition of the existing imbalance of power between the data subjects concerned and the controller (making any consent to be provided not free). In this regard, considering the dependency resulting from the employer – employee relationship, it is unlikely that the data subject is able to deny their employer consent to data processing without experiencing the fear or real risk of detrimental effects as a result of a refusal.<sup>50</sup> This infringement (and other related infringements identified) resulted in the issuance of a 40.000,- Eur fine to the controller. No other measures were imposed, as all identified deficiencies were removed by the controller.

## **V. CONCLUSION**

The analysis of the DPA's case law regarding consent provision identified issues connected with this process in practice. These issues included not only the controller's failure to ensure the fulfilment of legal conditions for valid consent provision (provision of an informed, free and active consent), but also issues concerning the selection of an appropriate legal basis for personal data processing by the controller and the failure to cease processing operations after consent withdrawal by the data subject. The individual sub-chapters of this paper closely

---

<sup>47</sup> Decision of the Office for Personal Data Protection of the Slovak Republic No. 00051/2021-Os-16 adopted 19.9.2021.

<sup>48</sup> Decision of the Office for Personal Data Protection of the Slovak Republic No. 00052/2021-Os-16 adopted 10.9.2021.

<sup>49</sup> Decision of the Office for Personal Data Protection of the Slovak Republic No. 01339/2021-Os-10 adopted 20.12.2021.

<sup>50</sup> European Data Protection Board. Guidelines 05/2020 on consent under Regulation 2016/679. Version 1.1. Adopted on 4. May 2020. P. 9.

examined the factual circumstances of the analysed decisions, specified provisions, the infringement of which led to the administrative proceedings before the DPA, and the sanctions imposed by it. The majority of the infringements identified in this regard concerned the violation of principles relating to personal data processing (Article 5 GDPR), specifically the lawfulness principle and the transparency principle, including conditions for consent provision (Article 7 GDPR). Considering the fact that GDPR allows to sanction these infringements with administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher (Article 83 (5) GDPR), the sanctions imposed by the national DPA seem insufficient. This may impede the deterring effect, the imposition of administrative sanctions for personal data infringements should aspire to achieve in practice. It must be noted, however, that the practice of imposing symbolic fines for the infringement of personal data protection regulation is not exclusive for the infringements relating to consent provision but can be distinguished with respect to the results of all of the remaining administrative proceedings before the DPA.

### KEÚČOVÉ SLOVÁ

súhlas, osobné údaje, rozhodovacia činnosť, GDPR, DPA

### KEY WORDS

consent, personal data, case-law, GDPR, DPA

### BIBLIOGRAPHY

1. ALADEOKIN, A. - ZAVARSKY, P. - MEMON, N. Analysis and compliance evaluation of cookies-setting websites with privacy protection laws. In Digital Information Management (ICDIM), 2017 Twelfth International Conference on Digital Innovation Management (ICDIM), pp. 121-126. DOI: 10.1109/ICDIM.2017.8244646.
2. BREEN, S. - OUZZANE, K. - PATEL, P. GDPR: Is your consent valid? Business Information Review, Vol. 37, No. 1, 2020. P. 19-24. DOI: <https://doi.org/10.1177/0266382120903254>
3. BYGRAVE, L. A. Data Protection Law: An International Perspective. Oxford: Oxford University Press, 2014. ISBN: 9780191758904.
4. BYGRAVE, L. A. Commentary to Article 4 (11) GDPR. In: Kuner, Ch. et al. The EU General Data Protection Regulation (A Commentary). Oxford: Oxford University Press, 2020. ISBN: 978-0-19-882649-1.
5. Decision of the Office for Personal Data Protection of the Slovak Republic No. 00006/2021-Os-2, adopted 4.1.2021
6. Decision of the Office for Personal Data Protection of the Slovak Republic No. 00049/2022-Os-14, adopted 29.9.2022
7. Decision of the Office for Personal Data Protection of the Slovak Republic No. 00051/2021-Os-16, adopted 19.9.2021
8. Decision of the Office for Personal Data Protection of the Slovak Republic No. 00052/2021-Os-16, adopted 10.9.2021
9. Decision of the Office for Personal Data Protection of the Slovak Republic No. 00296/2020-Os-17, adopted 30.11.2020
10. Decision of the Office for Personal Data Protection of the Slovak Republic No. 00374/2022-Os-3, adopted 8.2.2022
11. Decision of the Office for Personal Data Protection of the Slovak Republic No. 00387/2022-Os-3, adopted 28.3.2022
12. Decision of the Office for Personal Data Protection of the Slovak Republic No. 00517/2020-Os-10, adopted 13.8.2020

13. Decision of the Office for Personal Data Protection of the Slovak Republic No. 00704/2020-Os-1, adopted 1.6.2020
14. Decision of the Office for Personal Data Protection of the Slovak Republic No. 00705/2020-Os-21, adopted 12.11.2020
15. Decision of the Office for Personal Data Protection of the Slovak Republic No. 00770/2020-Os-1, adopted 20.5.2020
16. Decision of the Office for Personal Data Protection of the Slovak Republic No. 01107/2020-Os-7, adopted 14.12.2020
17. Decision of the Office for Personal Data Protection of the Slovak Republic No. 01339/2021-Os-10, adopted 20.12.2021
18. DE MATOS, M. G. – ADJERID, I. Consumer consent and firm targeting after GDPR: the case of a large Telecom provider. *Management Science*, Vol. 68, No. 5, 2021. DOI: 10.1287/mnsc.2021.4054.
19. European Data Protection Board. Guidelines 05/2020 on consent under Regulation 2016/679. Version 1.1. Adopted on 4. May 2020.
20. GEORGIEVA, L. - KUNER, CH. Commentary to Article 9 GDPR. In: Kuner, Ch. et al. *The EU General Data Protection Regulation (A Commentary)*. Oxford: Oxford University Press, 2020. ISBN: 978-0-19-882649-1.
21. JACKSON, O. Businesses retreating from consent under GDPR. *International Financial Law Review*. 2018.
22. Judgement of the Court of Justice of the European Union C-61/19 of 11 November 2020 *Orange Romania*. ECLI:EU:C:2020/901.
23. KOOPS, B. J. The trouble with European data protection law. *International Data Privacy Law*, 4(4), 2012. P. 250-261. DOI: 10.1093/idpl/ipu023.
24. O'CONNOR, Y. - ROWAN, W. - LYNCH, L. - HEAVIN, C. Privacy by Design: Informed Consent and Internet of Things for Smart Health. *Procedia Computer Science*, Vol. 113, 2017. P. 653-658. DOI: 10.1016/j.procs.2017.08.329.
25. POLITOU, E. - ALEPIS, E. - PATSAKIS, C. Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions. *Journal of Cybersecurity*. Vol. 4, Issue 1, 2018. ISSN: 2057-2093. DOI: 10.1093/cybsec/tyy001
26. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1–8.
27. RÓZENFELDOVÁ, L. Protection of privacy and personal data as regards the use of cookies. In: *STUDIA IURIDICA Cassoviensia*, Vol. 8, No. 1, 2020. ISSN: 1339-3995. DOI: <https://doi.org/10.33542/SIC2020-1-06>
28. RUDOHRADSKÁ, S. – TREŠČÁKOVÁ, D. Proposals for the Digital Markets Act and Digital Services Act – broader considerations in context of online platforms. In: *EU 2021 – the future of the EU in and after the pandemic: International Scientific Conference: Conference book of proceedings*. Osijek: Sveučilište Josipa Jurja Strossmayera u Osijeku, 2021. ISBN 24599425. S. 487-500. DOI: <https://doi.org/10.25234/eclic/18317>
29. SALEHIJAM, M. The value of systematic content analysis in legal research. *Tilburg Law Review*, 23(1-2), 2018. <<https://tilburglawreview.com/articles/10.5334/tilr.5>> Accessed 21. November 2023. DOI: 10.5334/tilr.5
30. WEBER, R. *Basic content analysis*. SAGE Publications, Inc., Vol. 49, 1990.

**CONTACT DETAILS OF THE AUTHOR**

**JUDr. Laura Bachňáková Rózenfeldová, PhD.**

Researcher

Pavol Jozef Šafárik University in Košice,

Faculty of Law, Institute of Theory of Law of Gustav Radbruch

Kováčska 26, 040 75 Košice, Slovakia

Phone number: +421 55 234 4176

E-mail: [laura.rozenfeldova@upjs.sk](mailto:laura.rozenfeldova@upjs.sk)