

---

# PRIVACY AND PERSONAL DATA PROTECTION ISSUES AS REGARDS THE USE OF COOKIES ON THE EXAMPLE OF HEALTHCARE PROVIDERS IN SLOVAKIA

Laura Rózenfeldová – Pavol Sokol – Diana Fortunová

European Information Society Institute, o. z. / Univerzita Pavla Jozefa Šafárika v Košiciach

Address Štítová 1/ Šrobárova 2

040 01 Košice

laura.rozenfeldova@upjs.sk – pavol.sokol@upjs.sk - diana.fortunova@student.upjs.sk

**Abstract:** *This paper examines the application of the cookies' regulation, specifically as regards the legal requirements stipulated by legislation and further developed by case law, the fulfilment of which ensures the lawful employment and use of cookies towards users visiting different websites on the internet. The implementation of these legal requirements in practice is analysed on the example of websites operated by different healthcare providers within the territory of the Slovak republic, which utilize cookies for different purposes. In this regard the authors identify the common practice of healthcare providers as regards the use of cookies on their websites and the main issues that prevent the successful implementation of the regulation in practice.*

**Keywords:** *privacy, personal data, cookies, healthcare providers*

## 1. Introduction

The existence of specific challenges and threats to the protection of fundamental rights and freedoms of natural persons on the internet, specifically of the right to privacy and personal data protection, cannot be refuted.

Data collection may be executed in numerous ways. One of the most common methods is based on the use of cookies, which are defined as the state of information that passes between an origin server and user agent and is stored by the user agent [1]. In general, cookies are small data or text files that are employed at the time when users visit websites by their servers with the objective to collect selected information and send this information back to these servers.

The issue to be tackled in this regard is the fact that the information collected may either include personal data of the websites' users, therefore possibly interfering with their right to personal data protection, or may in other way interfere with their personal life with the possibility to infringe users' right to the protection of their privacy. Due to the importance of privacy and personal data protection in the digital environment, the use of cookies and other similar technologies is limited by the applicable legislation supported by the relevant case law. This paper follows primarily the regulation enacted by the European Union (hereinafter only as the "EU"), which includes primarily the ePrivacy Directive [2] and the General Data Protection Directive [3], and the relevant case law of the CJEU contained primarily in the judgement C-210/16 *Wirtschaftsakademie Schleswig-Holstein* [4] and the judgement C-673/17 *Planet 49* [5].

## 2. Related works

Kosta [6], Borgesius [7] and Markou [8] provide a critical legal analysis of the 2009 amendment to Article 5 (3) of the ePrivacy Directive that altered the approach as regards the provision of consent from the previously applied opt-out principle to the newly preferred opt-in principle. Cofone [9] further examines the different approaches of the selected Member States (UK and Netherlands) to the

implementation of this amendment in their national legislation. The impact of the recent General Data Protection Regulation on the use of cookies in practice, specifically as regards the issue of consent provision, and the initiatives of the EU in connection with the further modification of the ePrivacy Directive are investigated by Rózenfeldová et al. [10]. The issue of consent provision and its obtainment from the perspective of business companies is also analysed by Jackson [11]. The legal analysis of the relevant CJEU case law on the use of cookies from privacy and personal data protection perspective is provided by Rózenfeldová [12]. Large-scale empirical study of web cookies was realised by Cahn et. al. [13]. The authors collected over 3.2 million cookies from the top 100.000 Alexa websites within the period of 18 months. On this basis the authors discuss important privacy implications by examining specific cookie attributes and placement behaviour of the third-party cookies. The Cookiepedia [14] provide the Cookiepedia database that currently contains 31 250 808 cookies that are categorized into four different categories, namely strictly necessary cookies, functionality cookies, performance cookies and targeting or advertising cookies, and also provides a tool to scan the content of websites to detect cookies used on them.

## 3. Methodology

The primary research question for the analysis provided is stipulated as follows: "How do healthcare providers in the Slovak republic approach the issue of privacy and personal data protection as regards the use of cookies on their websites towards their users?" The authors consider the individual legal requirements stipulated by the EU legislation and supported by the relevant case law of the CJEU and their implementation in practice. The authors examine these legal requirements and study their application or the absence thereof on the websites operated by healthcare providers that provide their services within the territory of the Slovak republic.

The healthcare providers examined include both state-owned and operated institutions, as well as organizations

---

---

managed by private companies. The list of healthcare providers was formulated on the basis of the National Registry of Health Care Providers administered in accordance with the Act No. 153/2013 Coll. on the National Health Information Centre [15], which defines e. g. the scope of data included in the registry, particularly information enabling the identification of subjects authorized to provide healthcare services in the Slovak republic.

To answer the above-stated research question, the authors conducted the analysis of all of the websites provided and operated by the identified healthcare providers in the Slovak republic.

The analysis included the examination of 95 websites in total, from which only 77 were identified as functional and therefore were included in the analysis. Moreover, 5 more websites were later excluded from the analysis due to the fact that no cookies were employed on them. Therefore, 72 websites of the Slovak healthcare providers in total formed the basis for the authors' final analysis.

The analysis included the collection of numerous attributes defined with the objective to answer stipulated partial research questions. The relevant data was collected from the healthcare providers' websites, specifically from two sources, namely from the so-called 'cookie banners' (notifications shown on the website informing the user about the employment of cookies on the website) and from the cookies policies available on the website.

The first set of data, the objective of which is the examination of the method of consent provision, included the following data: (I) whether the user has the possibility to consent with the use of cookies (attributes: yes / no); (II) whether the user has the possibility to actively consent with the use of cookies (the application of the opt-in principle) (attributes: yes / no); (III) whether the user has the possibility to choose between different consent settings (e. g. consent provided for the use of all categories of cookies or only for the selected categories of cookies) (attributes: yes / no); (IV) whether cookies were applied notwithstanding the provision of consent, namely whether cookies were used even before the provision of consent (attributes: yes / no); (V) if cookies were applied notwithstanding the provision of consent, what types of cookies were employed, namely whether these cookies were limited to first-party cookies (attributes: yes / no).

The objective of the second set of data is to study the individual aspects that must be present to ensure the provision of an informed consent. In this respect, the authors examined, whether the following data was provided to users: (I) general information about cookies (attributes: yes / no); (II) information on the types of cookies used by the website (attributes: yes / no); (III) information regarding the purpose of cookies' use (attributes: yes / no); (IV) information specifying the scope of the data collected (attributes: yes / no); (V) information about the time period,

within which cookies are used (attributes: yes / no); (VI) information about the parties with access to data collected by cookies (attributes: yes / no); (VII) specification of countries, to which data is sent (attributes: yes / no); (VIII) information about the controller (attributes: yes / no); (IX) information about the data protection officer (attributes: yes / no).

#### **4. Consent as the authorization criterion**

The utilization of data collected and processed with tracking technologies such as cookies can provide numerous benefits to different subjects. These include not only websites' operators, but also individual users of their websites. However, to ensure the conformity of such collection and processing of data, whether personal or other, with the applicable legislation and case law, the websites' operators must identify the relevant legal requirements and adhere to them in their practice.

The legal basis that provides the necessary authorization for the accumulation and processing of data in this regard is consent. The determination of consent as the authorization criterion is based on the provisions of the relevant legislation applicable in this regard, namely on Article 5 (3) of the ePrivacy Directive and, after the relatively recent modification of personal data protection legislation, on Article 6 (1) (a) of the General Data Protection Regulation (hereinafter only as "GDPR").

Consent as the legal basis for data processing is defined in Article 4 (11) of GDPR 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." This definition and the subsequent provisions of GDPR regarding consent together with the relevant case law of the CJEU determine the individual legal requirements to be fulfilled in order for the provision of consent to be considered as valid.

The most important condition in this regard is the requirement of lawfulness. According to Article 6 (1) of GDPR, "processing shall be lawful only if and to the extent that at least one of the following applies: a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes." However, the provision of consent by the data subject (the affected natural person) for one or more specific purposes with the use of cookies on the website must fulfill certain conditions. Especially important is the obligation of controllers (website operators) to ensure that data subjects not only have the possibility to consent with the use cookies, but are also able to consent in an active manner. Active consent presents the application of the currently preferred opt-in principle in practice, which requires users to actively 'do something' to provide their consent, as opposed to the formerly accepted opt-out principle that presumed the provision of consent until users submitted or otherwise expressed their objection in this regard.

---

---

The provision of active consent seems to be one of the most problematic conditions to be exercised in practice. Many websites actively try to circumvent this demand or otherwise trick users into providing their consent with the use of cookies. Examples of such practices include general formulations according to which users consent with the use of cookies simply by visiting a website (without the need to actively consent), by providing pre-checked checkboxes in cookies notifications, which users must deselect to refuse their consent, or by highlighting ‘the accept buttons’ while limiting the visibility of or otherwise hiding ‘the deny buttons’ in cookies notifications.

#### **4.1 The lawfulness of consent provision**

The analysis confirmed the above-stated issues regarding the lawfulness of consent’s provision on the websites of the analysed healthcare providers. In this regard, the first partial research question was defined as follows: “Does the method of consent provision applied on the healthcare providers’ websites fulfil the condition of lawfulness in accordance with the applicable legislation and case law?” To answer this question, the authors investigated four issues.

Firstly, we considered, whether users visiting the websites of the healthcare providers had the ability to consent with cookies used on these websites. In this regard, from the 72 websites that form the basis for our analysis, only 9 of them employed a mechanism for consent’s provision.

Secondly, we investigated whether users were able to provide their consent with the use of cookies in an active manner, e. g. by clicking on the accept button. From the 9 websites that employed some form of mechanism for consent provision, almost all of them (8 out of 9) conformed to the condition of the active consent provision. The reason for this may be that fact that when websites’ operators realise the fact that the provision of users’ consent is necessary, and therefore a mechanism for consents’ provision must be created, they employ such a mechanism that adheres to the applicable legislation and case law that requires the provision of active consent.

Thirdly, the authors considered whether the user, that has the possibility to consent with the use of cookies, also has the opportunity to choose between different consent settings. Such an opportunity may be present in the creation of different categories of cookies used on a website (e. g. strictly necessary, functional, analytical, advertising or other types of cookies). In this regard, website operators may enable users to consent only with all types of cookies employed on their websites, or may provide users the option to choose the categories of cookies with the use of which they consent to. The authors consider that from the legal point of view, the latter option better suits the legal requirement, according to which consent for personal data processing shall be given for one or more specific purposes. This conclusion is based on the fact that users’ general consent with the employment of all categories of cookies may not be deemed as distinct enough to ensure the specificity of processing’ purposes. The authors’ analysis

demonstrates these issues, as only 6 from the analysed websites enabled users to determine the categories of cookies, with the use of which they consent to, whereas 66 of websites did not provide this option to their users.

Fourthly, the authors analysed the question, whether cookies were employed (e. g. stored in users’ terminal equipment) notwithstanding the provision of consent. In this regard the authors examined, whether cookies were engaged also in the incognito mode of web browsers.

The engagement of cookies before the obtainment of users’ consent with the use of cookies is, at first sight, in conflict with the principle of lawful processing of personal data, due to the absence of a legal basis that authorizes such processing. Our analysis has shown that the majority of the analyzed websites (69 from 72 websites) used cookies even before any consent was provided from users. These results may indicate that the website operators do not condition the use of cookies on the provision of consent. This conclusion is supported by the fact that in the case of 60 websites that used cookies before the provision of consent, no mechanism for consent obtainment was provided, and in the case of the remaining 9 websites, that implemented such a mechanism, none of them ensured the non-employment of cookies before consent provision.

In conclusion, the answer to the first partial research question of whether the method of consent provision applied on the healthcare providers’ websites fulfils the condition of lawfulness in accordance with the applicable legislation and case law must be (with minor exceptions) no. As was stated above, the majority of the analysed websites do not provide any mechanism for consent provision. From those websites that provide such a mechanism, only 8 websites in total fulfilled the requirement of active consent provision and only 6 websites provided the users with the possibility to choose between different categories of cookies to consent to and therefore ensured the provision of specific consent. Furthermore, the majority of websites did not condition the use of cookies on the consent provision (on average 5 cookies were used on every website before the provision of consent). Despite of the fact that some websites provided a mechanism for consent provision, none of them ensured the non-employment of cookies before obtaining such consent.

#### **4.2 The possibility to withdraw consent**

Article 7 (3) of GDPR also conditions the validity of consent’s provision on the right of data subjects that previously provided their consent with data processing to withdraw their consent at any time. Therefore, the authors stipulated their third partial research question as follows: “Do healthcare providers ensure the application of the right to consent withdrawal as regards the use of cookies on their websites?”

In this regard, the authors considered, firstly, whether the analyzed healthcare providers informed their users about their right to withdraw their previously provided consent

---

---

with the use of cookies. This obligation is stipulated directly in Article 7 (3) of GDPR (2016), according to which data subjects shall be informed of this right “prior to giving consent”. Despite of the clear wording of the regulation, the authors identified only 21 websites that provided their users with this information in contrast with 51 websites that did not contain such information. Therefore, more than 70 % of the analyzed healthcare providers were identified as directly infringing the applicable regulation in this regard.

Secondly, the authors examined whether it was possible for users to withdraw their consent directly on the website, on which the consent was previously provided. In this regard, only 2 websites provided such an opportunity. Specifically, one website enabled the consent withdrawal through an email and the other website provided this option directly in the cookies’ notification.

The availability of the option to withdraw consent to websites’ users may be difficult to ensure in practice, if specific methods for consent withdrawal are to be created for individual websites. This is supplemented by another legal requirement stipulated in Article 7 (3) of GDPR (2016), according to which “it shall be as easy to withdraw as to give consent,” which can be interpreted as the possibility to withdraw consent in the same or similar manner as it was provided (e. g. if consent was provided by clicking on the accept button, the withdraw button should also be made available). In this regard it may be preferable for the website operators to provide their users with information regarding the possibility to delete cookies directly from their web browsers rather than to create specific mechanisms for consent withdrawal.

### Conclusion

This paper discusses the issues connected with the use of cookies as regards the privacy and personal data protection of users visiting websites operated by healthcare providers in the Slovak republic. The authors focused predominantly on the individual aspects of consent provision that has been identified as the primary legal basis for the collection and processing of users’ data through cookies. The results of the analysis conducted on the healthcare providers’ websites confirm the absence of a common approach to consent provision and highlights the individual deficiencies of consent obtainment, such as the absence of a specific mechanism for consent provision, non-fulfilment of conditions required for the provision of informed consent, as well as the absence of consent withdrawal mechanisms required by the applicable legislation. In this regard, the authors conclude that the websites of the analysed healthcare providers that provide services in the Slovak republic do not sufficiently ensure privacy and personal data protection of their users, whose personal or other data may be collected and processed in a way that does not correspond to their interests.

### Acknowledgements

This paper was supported by project no. 314011L790 - Friendly data environment in healthcare in the Operational Program "Effective Public Administration".

### References

- [1] Barth A. (2011) Request For Comments 6265: HTTP State Management Mechanism. Available from: <https://tools.ietf.org/html/rfc6265>
  - [2] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). OJ L 201, 31.7.2002, p. 37–47.
  - [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 (General Data Protection Regulation). OJ L 119, 4.5.2016, p. 1–88.
  - [4] Judgement of the Court of 5 June 2018 in the case C-210/16 *Wirtschaftsakademie Schleswig-Holstein*. ECLI:EU:C:2018:388.
  - [5] Judgement of the Court of 1 October 2019 in the case C-673/17 *Planet 49*. ECLI:EU:C:2019:801.
  - [6] Kosta, E. Peeking into the cookie jar: the European Approach towards the regulation of cookies. In: *International Journal of Law and Information Technology*, Vol. 21, No. 4 (2013), pp. 380–406.
  - [7] Borgesius, F. J. Personal data processing for behavioural targeting: which legal basis? In: *International Data Privacy Law*, 2015, Vol. 5, No. 3. pp. 163-176.
  - [8] Markou, Ch. Behavioural Advertising and the New ‘EU Cookie Law’ as a Victim of Business Resistance and a Lack of Official Determination. In: *Data Protection on the Move. Current Development in ICT and Privacy/Data Protection*. Dordrecht: Springer, 2016. pp. 213 – 248..
  - [9] Cofone, I. N. The way the cookie crumbles: online tracking meets behavioural economics. In: *International Journal of Law and Information Technology*, 2017, 25 pp. 38–62.
  - [10] Rózenfeldová, L. – Sokol, P. New Initiatives and Approaches in the Law of Cookies in the EU. In: *IDIMT-2018 Strategic Modeling in Management, Economy and Society 26th Interdisciplinary Information Management Talks*. Linz: Gerhard Chroust, 2018. pp. 303-310.
  - [11] Jackson, O. (2018). Businesses retreating from consent under GDPR. *International Financial Law Review*.
  - [12] Rózenfeldová, L. Protection of Privacy and Personal Data as regards the Use of Cookies. In: *STUDIA IURIDICA Cassoviensia*, vol. 8, no. 1, 2020. pp. 60-72.
  - [13] Cahn, A., Alfeld, S., Barford, P., & Muthukrishnan, S. (2016). An empirical study of web cookies. In *Proceedings of the 25th International Conference on World Wide Web* (pp. 891-901). International World Wide Web Conferences Steering Committee.
  - [14] Cookiepedia: <https://cookiepedia.co.uk/>
  - [15] Act No. 153/2013 Coll. on the National Health Information Centre.
-