RSP • No. 49 • 2016: 66-76

ORIGINAL PAPER

Processing Personal Data by Cookies

Marioara Maxim*

Abstract
After the eradication of the communism, the processing of personal data has become a real topic, as the data privacy turned into a concrete fundamental right for Romanian citizens. In 2001, the Romanian Parliament adopted the Law no. 677/2001 on the protection of individuals with regard to the processing of personal data and the free movement of such data, as a response to the EU legislation by transposing Directive 95/46 EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Still, the processing of personal data by cookies is not visible for all stakeholders, especially for the data subjects, despite the fact that we access the Internet on a daily basis for social networking, for research, for shopping, or just for information. Whenever we access websites, several cookies might be placed on our computers temporarily or even permanently. Depending on the technical properties of the used cookies, this might imply a collection of personal data, accessing and usage of personal data, international transfer of personal data, etc., all of the above falling under the concept of processing personal data, as provided by the law. Consequently the study explains the legal conditions of processing personal data by cookies in the context of the national legal framework, with consideration of the European Union legislation, and in the light of Article 29 Data Protection Working Party's Opinions and Recommendations.

Keywords: *data protection, cookies, processing, legislation, networking*

* University of Bucharest, Faculty of Law, PhD School, Bucharest, Romania, Email: av.maria_maxim@yahoo.com

Introduction

According to article 4, paragraph 1) of the Law no. 506/2004 on the processing of personal data and the protection of privacy in the electronic communications sector, as amended by Law no. 235/2015 (Law no. 506/2004), *"the confidentiality of the electronic communication through a public communication network or publicly available electronic communications services, and the confidentiality of the traffic data is guaranteed". This legal guarantee is part of the protection to the private life of the individuals, right that is classified as inalienable, imprescriptible, and non-transferable to any other person (Ovidiu Ungureanu, Cornelia Munteanu, 2015).*

In this context, the same article of Law no 506/2004 establishes as a principle the *rule of consent* anytime the personal data or traffic data are subject of a processing operation, while the exemptions are expressly given in a very limitative register. Thus, the storage of personal data or traffic data for the purpose of making the communication functional, respectively for the performance of the electronical communications services, is allowed, including the case when this implies the usage of cookies technologies. Hence, the article 4, paragraph 6) of the Law no. 506/2004 which transposed the article 5) paragraph 3) of the Directive 2002/58, as modified by Directive 2009/136/EC of the European Parliament and of the Council in November 2009, establishes 2 (two) categories of exemptions, analyzed in one of the below sections referring to the exclusive purpose of the transmission of the electronic communication, and to the delivery of an electronic service required by the user/data subject (section no. 5). The study also includes the main categories of cookies as they have been analyzed by Article 29 Data Protection Working Party (WP), the processing requirements, such as consent validity, the rights and obligations of the main stakeholders, with the consequences for the data confidentiality breach in terms of sanctions provided by the law, and the civil liabilities of the data controllers or data processors.

Definition and categories of cookies

A cookie is a small text file that is downloaded onto 'terminal equipment' (e.g. a computer or smartphone) when the user accesses a website (UK Information Commissioner's Office). (Cookies indicate in fact specific technologies which use unique identifiers (an alphanumeric code - numbers, letters, randomly set) sent to the Internet user/data subject by the website/s accessed by that user while browsing, that are stored on the user terminal equipment (computer, mobile phone, tablet, etc.), and can access various information (e.g. the tracking cookies).

If the Cookies contain the personal data, or might be used as an identification element, or the information generated contains personal data, than the requirements of processing of personal data are also applicable (i.e. the IP address is accessed in setting the cookies). In this respect, according to Law no. 677/2001, *personal data* mean any data referring to an identified or identifiable natural person. Same article provides the references to the *identifiable person* which means any natural person who can be identified directly or indirectly, specifically by indication to an identification number or to one or several specific factors connected to his or her identification – physical, psychological, economic, cultural or social.

Article 3 of the Law no. 677/2001, defines the *processing of personal data* as "any operation or set of operations done upon the personal data, by automatic or non-

automatic means, such as collection, registration, organisation, storage, adaptation or amendment, extraction, consultation, usage, or by dissemination to a third party in any way, or by combination, blockage, erasing or destruction". As we can observe, practically any kind of operation towards personal data means processing of personal data and falls under the Law no. 677/2001, which means that only the access of personal data (such as IP of the user) is sufficiently enough for the application of the Law no.677/2001 and Law no. 506/2004 requirements.

In accordance to Opinion no. 4/2012 on Cookies Consent Exemption, Article 29 Data Protection Working Party refers to the following categories of cookies, depending on the purpose they are used, the technology of the cookies, or the way the consent is required (e.g. expressly, or by objection):

"Authentication cookies" which are meant to support the user to log in for the following times, after he previously registered on that specific site. Examples of websites that use this kind of cookies: on-line training courses, on-line banking services, various accounts on media, e-commerce sites, etc.

Flash cookies", based on tracking technology, which are used to store the information needed for video content or audio content, enabling the users to access them. These cookies usually are stored on the user terminal equipment just for the respective session, falling under the sub-category of "session cookies".

"User-input cookies" used for the storage of the input that the user sent to a website, typically in on-line shopping (for instance when the user sends items to his shopping basket), or for filling-in some on-line forms.

"First Party cookies" vs. "Third Parties cookies" are the cookies placed by the party who operates the accessed website, being typically revealed in the URL displayed to the user. Third Parties cookies are the ones placed by different entities than the ones that operate the website, or its processors, or sub-processors.

"Security cookies" can be connected to the system security requirements to safeguard it from abuses (when log in), or to the security of the services provided, or the security of the websites. They have a longer duration of time, to serve their purpose, and, depending on the case, they might be under special conditions related to the consent of the user, respectively if he/she does not expressly require them or if they are not directly connected to the functionality of the provided services (e.g. being related to an additional service that was not required by the user).

"User interface customisation cookies (UI cookies)" are meant to save specific preferences of the users such as language, currency, display related preferences, etc.

"Social plug-in content sharing cookies" are the cookies that are placed to enable sharing of the information between the friends of various social networks, identifying the members of that social network vs. the non-members visitors, etc. The cookies for the non-members can be placed only if the social network obtained priory their consent, and they need to be only session cookies opposed to permanent cookies.

"Tracking cookies" are used for instance in cases of on-line behavioural advertising or for research and market analysis, for fraud detection, and they are meant to monitor the users' browsing activity, and access the information relevant for the purpose, usually being also third party cookies. They require the consent of the users before the cookies are stored in their terminal equipment. Also, in this case is important to consider the situations when the terminal device is used by many users, and only one of them agreed to have the cookies stored on the terminal equipment (e.g. computer), as the accessed information might belong to the other users, too.

"Opt-in Cookies" vs. "Opt-out Cookies": the first are the cookies that include the consent of the users for various processing of data purposes (e.g. behavioural advertising) while the latter store the refusal of the users for processing of their data, such as on-line preferences**.** In the latter case, one of the problems that have been identified during the research refers to the possibility of the data controller (website owner, ad network provider) to place opt-out cookies on the user terminal equipment with the purpose to exclude him/her from the on-line processing of his/her preferences (opt-out cookies representing an identification code for that specific user), considering the requirements of a valid and freely express given consent.

Thus, the difficulty is related to the existence of a real option of the user in such cases, if the data controller does not provide other options to the end user except the opt-in cookie in case he/she would like to be tracked for on-line commercial ads, and opt-out cookie in case he/she does not accept to be tracked. Still, the opt-out cookie is stored on the terminal equipment of the user who refused to be subject of personal data processing.

Applicable legislation

In case the data storage or accessing the data by cookies implies personal data processing, the Law no. 677/2001 is applicable, with all the provided requirements: data subject consent, notification, information, data subject's rights, etc. Nonetheless, it is to be mentioned that even when processing of data by cookies refers to the data that do not represent personal data, Law no. 506/2004 is still applicable, as a general rule for electronic communication services, which means that in principle the consent is required to be obtained before the cookies are placed on the user terminal equipment, unless we are in the situation of one of the exceptions previously mentioned by article 4, paragraph 6).

Therefore, the main regulations in case of processing data by cookies are the following: Directive 95/46 EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Directive 95/46); 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 2002/58/EC), amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009; Regulation no. 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws; Romanian Law no. 677/2001 on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data (Law no 677/2001); Law no. 506/2004 on the processing of personal data and the protection of privacy in the electronic communications sector, as amended by Law no. 235/2015 (Law no 506/2004); Article 29 Data Protection Working Party Opinion 2/2010 on online behavioural advertising (WP 2/2010); Article 29 Data Protection Working Party Opinion 16/2011 on EASA/IAB Best Practice Recommendation on Online Behavioural Advertising (WP 16/2011); Article 29 Data Protection Working Party Opinion 04/2012 on Cookie Consent Exemption (WP np 04/2012); Article 29 Data Protection Working Party Opinion 02/2013 providing guidance on obtaining consent for cookies.

It is to be mentioned that in April 2016, after 4 years of consultation, the European Parliament approved the new Regulation on the protection of personal data and on the free movement of such data, and repealing Directive 95/46/EC (called General Data Protection Regulation - GDPR) that will be directly applied in all EU member states in 2 years after

its publication. At the same time, the Directive 2002/58/EC remains valid, most probably under the revision in the next period. Likewise, the main requirements for the cookies technologies remain the same, as identified in this research, including the requirements for consent validity, and the rights and obligations provided to the main parties, at least until new amendments might be provided to the current framework in the electronical communication services. The relevant aspects brought by GDPR will be mentioned accordingly in the following sessions, if applicable.

Parties: Rights and Obligations

In case of personal data processing by cookies, Law. 677/2001 and Law no. 506/2004 sets forth specific rights and collateral obligations for the following parties: data subject that in most of the time is the user of the terminal equipment, even in cases when there might be multiple data subjects (i.e. the terminal devise has multiple users/accounts), the data controller that can be the network operator, the owner of the website, the ad network provider, the data processor that might be the representative of the data controller, or the publisher in case of the behavioural advertising, and the third parties who are very present in the processing of data by cookies, as most of the cookies fall under the category of "third parties cookies".

Data subject/user's rights refer in the first place to the requirements of the consent that he/she has to express before any cookie is stored on the individual terminal equipment, and clearly before the cookie can access any data stored in the terminal.

In this respect, the consent validity requires the option to be given "expressly and unequivocally". Therefore, we are in a case of an opt-in concept (opposed to opt-out). The consent rule is provided by article 4 paragraph 5) of Law no. 506/2004 in corroboration with article 5, paragraph 1) of Law no. 677/2001. Furthermore, the consent is valid only if the data subject was thoroughly informed about the purpose of the cookies, the entity that accesses the data (first party cookies vs. third party cookies); their duration, the data accessed, including the special personal data; the technology used, if there is any international transfer of the accessed data, etc.. The Article 29 Data Protection Working Party provides in its opinion the obligation for the data controller (the website administrators or owners) to inform the data subject using appropriate tools which have to be very visible and clear, (visible banners, specific box, additional links, etc.), and not hidden terms and conditions, written down with very small letters. The consent has to be also freely given, in the meaning that the data subject has to perform an action, and be active by either clicking on an opt-in button, or accessing a specific link, or by setting his browser configuration, etc. *"If the browser settings were predetermined to accept all cookies, such consent would not comply with Article 5 paragraph 3 of Directive 2002/58/CE"* (WP 2/2010 on online behavioral advertising), respectively article 4 of Law no.506/2004 which transposed the above mentioned Directive. In such an option, it would mean that the data subject accepts also future personal data processing before he/she knows the adequate information about it. In this regards, the Opt-out cannot be considered as a valid consent, but rather as a method for revoking the given consent at a later stage. It is to be also added that the consent of children is expressly regulated in the new GDPR in article 8, paragraph 1) which provides that "in relation to offer of information society services directly to a child, the processing of personal data of a child shall be lawful where the child is at least 16 years old", with the possibility for the member states to provide a lower age. The same article requires the parent's consent if the child is below the established minimum age.

Nonetheless, in case the cookie processes personal data (as for instance the IP or the preferences of the data subject in terms of tracking the accessed websites), the data subject has all the rights provided by Law no 677/2001 in chapter IV, such as: articles 13, 14, 15, 17 and 18: the right to object (article 15), the right to access his/her personal data (article 13), the right to have the data erased/corrected (article 14), the right to address the complaints to authorities or to Courts (article 18). It has to be mentioned that all the rights and obligations have been preserved by the new GDPR.

Data Controller / Data Processor: In order to exercise his/her rights, the data subject can address directly the data controller, which might be depending on the case the website owner, the network operator, or the ad network operator (in some cases the publisher for the on-line behavioural advertising). Thus, according to Law no. 677/2001, the data controller is the individual or the legal entity (in private or public sector) who establishes the purpose and the methods of personal data processing.

Typically, the first party cookies are established by the data controller, the entity that administrates the website, and appears in the URL address (for instance anspdcp.ro).

Nonetheless, the data controller in case of on-line behavioural advertising is the ad network provider, who rent the space from the publisher of the website to use it for commercial advertisements. They establish the purpose of personal data processing, the methods, and have complete control over the cookies technology, or over the behavioural data captured by the cookie. Even if technologically, they use a provider for the equipment, this is under the control and direct guidance of the ad network operator. The website publisher can be as well a data controller, having a jointly responsibility with the ad network provider, as the publisher is the one to have access to IP, collect the IP, and relishes the alphanumerical code / cookies. Therefore, in case the publisher will use the data for a different purpose, or for additional purpose, he will have the role and the responsibilities of the data controller, too. Nevertheless, the website publisher has in general the role of the data processor (a case by case analysis needs to be done, as the circumstances of the situation may differ).

The data controller has thus the obligations meant to ensure the data subjects rights, and to safeguard their personal or traffic data. The main obligations are the following: a. observing the data subject rights and implement technical solution to ensure the proper information, the validity of the consent (e.g. appropriate settings of the application); b. notification of the National Supervisory Authority for Personal Data Processing in certain cases as profiling for on-line behavioural advertising (ANSPDCP Decision no. 200/2015), and notifications of the amendments done during the processing (Bojincă, Basarabescu, Săvoiu, 2013); c. implementation of the technical and organisational measures: data privacy by design / by default; audit rights, etc. (Ombudsman Order 52/2002 on the minimum security requirements applicable for the personal data processing).

In the meaning that the processing of data is performed by the intermediaries, such as providers of electronic communications services, they will have the role and responsibilities of the data processors. The data processors have the obligation to fully observe the data subject rights, to act according to the data controller instructions, to accept to be audited by the data controller, to cooperate with the data controller in case of data breach, and notify immediately the data controller upon any data incidents, and eventually towards the National Supervisory Authority For Personal Data Processing. It is to be mentioned the fact that, as mentioned expressly in the new GDPR (recital 42), "when processing is based on the data subject's consent, the controller should be able to

demonstrate that the data subject has given consent to the processing operation". This means that the obligation to prove that the legal requirements have been fulfilled belongs to the data controller, the data processor remaining of course responsible for fulfilling the data controller instructions.

Third Parties: As the third party cookies are statistically more that the first party cookies, it is very important to distinguish between the data controller, data processor, and third parties' roles and responsibilities.

Thus, according to Law no. 677/2001(article 3), the third parties are defined *"as any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the person who, under the direct authority of the controller or the processor, are authorized to process the data".*

As mentioned by the WP 4/2012, in case of data processing by cookies, the third party will be than the natural person or the legal entity who is not a first party cookie, meaning that it does not appear in the URL address, and thus the third parties cookies *"are cookies that are set by websites that belong to a domain that is distinct from the domain of the website visited by the user…, regardless of any consideration whether that entity is a distinct data controller or not".*

An illustrative example: in the behavioral advertising when the cookie is placed for the purpose to create profiles, and enables the user identification in all the websites accessed by him/her in that browser session or in the following ones. Thus, in such a case, the third party will get access to the personal data of the data subjects. Consequently, it will take actually the role of the data controller, as it has the possibility to define the purpose of the data processing, the methods of accessing information, or the means by placing the cookies.

If the third party becomes a data controller, it has all the related rights and obligations.

Cookies excepted from the Consent

According to article 4), paragraph 6) of Law no. 506/2004, 2 main types of cookies do not require the data subject consent, but continue to imply a complete information of the data subject who maintains his/her rights provided by Law no. 677/2001 (e.g. right to oppose). Thus, the exemptions refer to the following situations:

a) Cookies that are used for ***"the sole purpose of carrying out the transmission of a communication over an electronic communication network"*** (article 5, paragraph 3 of Directive 2002/58/EC)**.**

WP 04/2012 identifies 3 examples that can fall under this category: the cookies that *"route the information over the network, and identify the communication endpoints", the cookies that determine the network "errors or data loss", and the cookies that "exchange the data items in their intended order, by numbering data packets".*

b) Cookies that are ***"strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service"*** (same article of law) include the cookies that are meant to enable a functionality of the website – such is for on-line shopping, video display set-ups, the language preferences, etc.

It is to be mentioned that usually these are first party cookies, as the third party cookies are connected to additional information, and they are not strictly necessary to the functionality of the accessed website, being not related to a service required by the data subject. By these 2 main exemption the law maker ensured that the functionality of the service required by the data subject or the user is preserved, as long as the data controller

or data processor access only the needed data for the user identification (or security matters), so that the service to be provided at an adequate level.

Retention period for the data collected

The duration of the cookies has to be part of the data subject/user information.

One of the principles provided by the data privacy legislation refers to the principle of proportionality in the meaning that the data shall be processed only for a duration proportional with the declared purpose of the collection and storage. This principle has been maintained further on by article 5) paragraph 1) letter e) of the GDPR.

As we before mentioned, some of the cookies (the "session cookies") shall be meant to be stored only for the respective browsing session, so that they should be automatically erased when the session ends. Contrary to this, the so called "persistent cookies" are stored for a longer period of time, until the moment that the set-up period expires. Some cookies have a longer duration for the benefit of fulfilling their legitimate purpose, such as security cookies or authentication cookies. Persistent cookies can technically be set for days, but also minutes or many years (e.g. 7985 years as shown in the Cookies Sweep Combined Analysis – Report issued by WP in 2015), when the longer duration not proportional to the scope of data processing is not legitimate, being contradictorily to the principles provided by the data protection legislation, including the new GDPR. Furthermore, as we identified from the WP Opinion no. 4/2012, there are also cookies that cannot be erased despite the effort of the data subjects / users. This type of cookie is called "zombie-cookie", and it is illegal, being considered disproportionate to the legitimate usage of the cookies, per se. The legislation does not provide certain duration for the storage of the data by cookies, or a timeline for the existence of the cookies placed into the terminal equipment of the data subject/user. Hence, based on the article 14) paragraph 2) of the GDPR, the user / data subject has to be informed about the "*period for which the personal data is stored, or if that is not possible, the criteria used to determine that period*". Still the WP, in its opinion on cookies consent exemption consider that the reasonable duration for the persistent cookies shall be "limited to a few hours" (WP 04/2012), but definitely we also considered that in specific cases shall not exceed 1 year, and the consent shall be re-obtained.

Statistical data

One of the recently performed studies on the cookies was adopted on February 3, 2015, by Article 29 Data Protection Working Party in its Report – Cookies Sweep Combined Analysis. The study was performed in 8 European Countries (United Kingdom, France, Denmark, Netherlands, Spain, Slovenia, Greece and Check Republic), by automatically means, and by manually research, on 478 websites used by the data subjects in 3 sectors: e-commerce, media and public. The main findings, relevant for our research, confirmed the fact that almost every time when the Internet users access an website, several cookies are placed on their terminal equipment, majority of them without being visible, and with no opt-in consent. Thus, the WP report revealed that a number of 16555 cookies were found in all 478 investigated sites (an average of 34.6 cookies/per site). Considering this overall number – 16,555, the following findings have been considered in our research: 3 times more third-party cookies as opposed to first-party cookies; 2302 session cookies and 14,253 persistent cookies; 22 sites used more than 100 cookies (in media and e-commerce sectors); 3 first party cookies with 7,985 years duration (expiry

date in 9999); 415 sites set 8,472 third-party cookies; only 7 web sites were with no cookies (public sector); 59% used the banner to notify the users, while 39% used the link method, and 29% (116 websites) used no notification means; 57% of the websites provided sufficient level of information to the data subjects/users. As the number of third parties cookies are 3 times more that first cookies, and as they are usually not needed for the service functionality, it has to be considered the browser settings that prevent the third parties cookies to be stored on the terminal devise, or access the information stored on the equipment, especially when the consent is not required, and the processing of personal data is not legitimate. European Commission stated as well on its website that *"most browsers support cookies, but users can set their browsers to decline them and can delete them whenever they like"*.

Sanctions and Civil Liabilities

The data subjects has the right to object to the data processing by cookies, and the data controller has the obligation to provide an answer to the data subject's complaint in the deadline provided by Law no. 677/2001, respectively in 15 days respectively, or to erase the cookie or to guide the data subject to perform the deletion of the cookies by itself. In additional to this, the Law 506/2004 provides that serious fines that can be applied by the National Supervisory Authority on Personal Data Processing, respectively between RON 5,000 – 100,000, up to 2% of the turnover, depending on the circumstances of the cases. Likewise, the processing of personal data by breaching the data subjects rights established in articles 4-10, and articles 12-15 or article 17, represents an administrative offence being sanctioned between RON 1000 to 25,000, if the offence does not represent a criminal offence by itself (article 32 of Law 677/2001).

In this regards, based on the jurisprudence in the field of cybercrimes, there might be additional technologies used for accessing the personal data, as VoIP, where "VoIP refers to the voice packages send through the electronic networks which uses IP protocol", and the crimes implies illegal usage of the VoIP accounts by other persons than the direct owners (Trancă, 2011). Furthermore, the data subjects have the right to address their case in the Courts, being entitled to have all the damages covered by the data controller or the data processors (article 18 of Law no. 677/2001). "Depending on the existence of the possibility to financially assess the damage, the injury might be patrimonial or non-patrimonial", considering the "emotional suffering" as well, such as in cases of profiling, and pursued adds. (Boroi, Stănciulescu, 2012).

Conclusions

The research performed on the legal regime of the data processing by cookies revealed that there is a legal framework established in the field of the data processing by technological means, without referring expressly to the cookies technologies. Thus, there is no reservation that the regulations of Law no. 506/2004 (article 4) and Directive 2002/58/EC (article 5) apply for personal data processing by cookies, as mentioned by the Article 29 Data Protection Working Party. Nevertheless, from the perspective of the new EU Regulation on data the protection of natural persons with regard to the processing of personal data and on the free movement of such data adopted in April 2016 by the European Parliament that will replace the existing framework (Directive 95/46/EC) in 2 years from its publication (2018), it is the time for Directive 2002/58/EC to be reviewed in the next period of time, and up-dated to the digital age, and to the new legal frame sets forth by GDPR.

References:

Bojincă M., Basarabescu G., Săvoiu A. (2015). *Dreptul la Protectia Datelor cu Caracter Personal*, Bucharest, Universul Juridic Publishing House.

Boroi G., Stănciulescu L. (2012). *Instituții de Drept Civil îî Reglementarea Noului Cod Civil*, Bucharest: Hamangiu Publishing House.

Ungureanu O., Munteanu C. (2015). *Drept Civil. Persoanele în Reglementarea Noului Cod Civil*, Bucharest, Hamangiu Publishing House.

Trancă A., (2011*). Infracțiuni Informatice*, Bucharest, Hamangiu Publishing House.

Directive 95/46 EC (1995) of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, published in the Official Journal of the European Communities L 281/31, 23.11.1995.

Directive 2002/58/EC (2002) 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, amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009, published in Official Journal of the European Communities L 201/43(1) OJ L 108, 24.4.2002.

Regulation no. 2006/2004 (2004) on cooperation between national authorities responsible for the enforcement of consumer protection laws, Published in the Official Journal of the European Union L 364/1, 9.12.2004.

Regulation of the European Parliament and of the Council (2016) on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), published on http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf, last time accessed on 21st of April, 2016.

Romanian Law no. 677/2001 on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data, published in the Romanian Official Journal no. 790, Part I, 12.12.2001.

Law no. 506/2004 on the processing of personal data and the protection of privacy in the electronic communications sector, as amended by Law no. 235/2015, .published in the Romanian Official Journal, Part I, no. 1101, 25.11.2004.

Article 29 Data Protection Working Party Opinion 2/2010 on online behavioral advertising, published on http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_en.pdf, last time accessed on 1st of March, 2016;

Article 29 Data Protection Working Party Opinion 16/2011 on EASA/IAB Best Practice Recommendation on Online Behavioral Advertising, published on http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp188_en.pdf, last time accessed on 1st of March, 2016.

Article 29 Data Protection Working Party Opinion 04/2012 on Cookie Consent Exemption, published on http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion -recommendation/files/2012/wp194_en.pdf, last time accessed on 1st of March, 2016.

Article 29 Data Protection Working Party Opinion 02/2013 on apps on smart devices, published on http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf, last time accessed on 21st of April, 2016.

Article 29 Data Protection Working Party (2015), Report – Cookies Sweep Combined Analysis, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2015/wp229_en.pdf, accessed last time on 16th of April, 2016

European Commission, http://ec.europa.eu/ipg/basics/legal/cookies/index_en.htm, last time accessed on 1 of April, 2016.

Information Commissioner's Office (2016). UK, https://ico.org.uk/for-organisations/guide-to-pecr/cookies-and-similar-technologies, last time accessed on 21 of April, 2016.

Article Info

Received: December 2 2015
Accepted: April 19 2016