Bulletin of the *Transilvania* University of Braşov
Series VII: Social Sciences • Law • Vol. 11 (60) No. 2 - 2018

A PARTIAL OVERVIEW OF THE DATA SUBJECTS' CONTROL OVER THEIR PERSONAL DATA UNDER THE GENERAL DATA PROTECTION REGULATION

Maria-Magdalena BÂRSAN[1]

Abstract: *The legal framework on data protection was updated recently by the 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. According to this new regulation natural persons should have control of their own personal data. As such, the effective protection of personal data throughout the Union required the strengthening and setting out in detail of the rights of data subjects. In view of the novel legal framework, this article aims to explore some of the data subjects' main rights as to the control over the processing of their personal data.*

Key words: *GDPR, right to be informed, right of access, right to be digitally forgotten, right to de-referencing.*

1. Introduction

In the words of The Economist: "The world's most valuable resource is no longer oil, but data". Since personal data emanates from individuals, it's only natural that recital 7 of the Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data provides that "natural persons should have control of their own personal data" and the legal and practical certainty for individuals should be enhanced.

In this context, the data subjects' control over their own data is achieved by a series of rights and the correlative obligations of those who process and determine the processing of personal data. As such, the exercise by the data subject of the rights conferred by the General Data Protection Regulation (GDPR) should ensure an effective protection of personal data throughout the Union.

In order to overview how these rights provide to the data subjects control over the digital processing of personal data, we chose to present some of those rights which in our view have the highest impact on the processing activities: the right to be informed (article 13-14 GDPR), the right of access (article 15 GDPR) and the right to be digitally forgotten (right to de-referencing) consecrated by the Court of Justice of the E.U.

[1] *Transilvania* University of Braşov, maria.m.barsan@unitbv.ro.

2. The Right to Be Informed (**articles 13-14 GDPR**)

The first condition for the data subjects to have control over personal data processing is to know if any data concerning them is processed. Usually, data subjects are informed about the processing activities as a result of the principle of transparency provided by article 5 paragraph (1) letter a) GDPR. The right to be informed, like the other rights of the data subjects, is the normative expression of the principle of control and the participation of the data subjects in the processing of their personal data (Zanfir, 2015, p. 81).

The principle of transparency establishes for the controller the obligation to take any appropriate measures in order to keep the data subjects (users, customers or clients) informed about how their data are being used (European Union Agency for Fundamental Rights, 2018, p. 120). The information about the processing activities are given to the data subjects either before the processing starts, or during the processing, or following a request of access to their own data.

In that regard, recital 39 states that "It should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed […]. That principle concerns, in particular, information to the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of the natural persons concerned and their right to obtain confirmation and communication of personal data concerning them which are being processed".

The Court of Justice of the European Union (CJEU) in Bara Judgement, paragraph 33, stressed that "the requirement to inform the data subjects about the processing of their personal data is all the more important since it affects the exercise by the data subjects of their right of access to, and right to rectify, the data being processed […], and their right to object to the processing of those data […]". Another point to remember from this decision is that, in principle, the data subject must be informed both by the controller performing a data transfer and also by the controller who received that data regarding the scope, extent, categories of data and other processing related issues (Lisievici, 2015, p. 127-128).

Therefore, the knowledge of the processing activities is the one that allows the data subjects to control if the processing is lawful and intervene as to the processing of their personal data. Because of its importance, the obligation to be informed is considered in doctrine as one of the pillars of personal data processing (Şchiopu, 2017b, p. 97), alongside the principles relating to processing of personal data and the lawfulness of processing.

The obligations to inform regulated in article 13 and 14 GDPR do not depend on a request from the data subject. The controller is required to "proactively comply with the obligation, regardless of whether the data subject shows interest in the information or not" (European Union Agency for Fundamental Rights, 2018, p. 120). Although the list of information to be provided to the data subject according to article 13 and 14 GDPR is divided into two paragraphs, this list is an exhaustive and mandatory one, the operator having the obligation to provide all this information (Șandru, S., 2017, p. 136).

However, there are situations when the controller doesn't have the obligation to inform the data subject about the processing, for example, if personal data have not been obtained from the data subject and the obtaining or disclosure of the personal data is expressly laid down by Union or Member State law to which the controller is subject. Nevertheless, even in such situations, Article 29 Working Party in paragraph 66 of the Guidelines on transparency under Regulation 2016/679 specify that the data controller should make it clear to data subjects that it obtains or discloses personal data in accordance with the law in question, unless, according to article 23 GDPR, there is a legal prohibition preventing the data controller from doing so.

3. The Right of Access (article 15 GDPR)

If the data subjects are in doubt whether a controller is processing their personal data, the right of access provided by article 15 GDPR allows them to obtain from the controller the confirmation as to whether or not personal data concerning him or her are being processed. Also, the data subjects have the right to obtain access to the personal data (a copy of the personal data undergoing processing).

Recital 63 states that if "the controller processes a large quantity of information concerning the data subject, the controller should be able to request that, before the information is delivered, the data subject specify the information or processing activities to which the request relates". However, according to one author, recital 63 does not allow the operator to impose on the data subject the obligation to specify the information or processing activities to which his application relates, unless processing a large amount of information about the data subject itself, not when the volume of personal data it processes is large generally speaking (Şchiopu, 2018c, p. 87). Also, the same author considers that, under the principle of fair and transparent processing, the operator cannot refuse to provide the data subject with all the information, even if there is a large volume of information, which is an opinion we agree with.

Much of the information to be provided to the data subject as a result of the exercise of the right of access or the fulfilment of the obligation to inform can be readily extracted by the controller from the records of processing activities provided by article 30 GDPR. The obligation to keep a record of processing activities does not apply to an enterprise or an organisation employing fewer than 250 persons, unless the processing is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data or personal data relating to criminal convictions and offences.

Since there will be rare cases in which the controllers will not have the obligation to keep the records of the processing activities, even with regard to companies or organizations with less than 250 employees, we agree with the opinion that the rule is the obligation to keep these records, with exceptions to be analyzed on a case-by-case basis (Şchiopu, 2018b, p 88). Furthermore we consider that the record of processing activities is a vital tool in terms of data traceability and implicitly as regards the control that the data subjects should have on their own data.

Of course, we could imagine situations when the controller does not inform the data subject about the processing activities despite the fact that he should do so. Also, in

response to an access request, the controller might not confirm that personal data concerning him or her are being processed, although such processing is carried out. In such cases, when the data subjects' rights under GDPR have been infringed as a result of the processing of their personal data in non-compliance with the GDPR, the data subjects have two options: they will either lodge a complaint with a supervisory authority, or will choose a judicial remedy. We consider that the first option is preferable given that the supervisory authority can investigate, to the extent appropriate, the subject matter of a complaint, according to article 57 paragraph (1) letter f) GDPR, and the investigation may reveal the details of the processing activities that the controller kept hidden despite the obligation of transparency regarding the data processing.

3. The Right to Be Digitally Forgotten (CJEU Judgement in Case C‑ 131/12, Google Spain)

The right to the protection of personal data derives from the right to private life (Șandru, S., 2016, p. 137) and, according to recital 4 "is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality". Also the doctrine mentions that "sometimes the right to data protection is less preferred among the social values protected in the legislation" (Şandru, D.-M., 2018, p. 18).

In this context, the Court of Justice of the European Union in Google Spain Judgement admitted that in order to comply with the rights of erasure and opposition, "the operator of a search engine is obliged to remove from the list of results displayed following a search made on the basis of a person's name links to web pages, published by third parties and containing information relating to that person, also in a case where that name or information is not erased beforehand or simultaneously from those web pages, and even, as the case may be, when its publication in itself on those pages is lawful".

Thus, by interpreting the provisions of Directive 95/46/EC, the Court of Justice of the European Union has enshrined a right of individuals to obtain that certain results no longer appear when their names are entered into an online search engine. The recognition of the right to be digitally forgotten is all the more important as the erasure directly from web pages doesn't always provide an effective and complete protection of the data subject, for example when the publisher may not fall under the E.U. data protection law or the publication is carried out for journalistic purposes.

The right to de-referencing tends to create the premises necessary for certain information to be forgotten (Şchiopu, 2017a, p. 190) when the excessive visibility resulting from the indexing of personal data is disproportionate to the data subject's fundamental rights to respect for privacy and the protection of personal data. These rights, according to the Google Spain Judgement, override, as a rule, not only the economic interest of the operator of the search engine but also the interest of the general public in having access to that information upon a search relating to the data subject's name.

According to the Guidelines issued by Article 29 Data Protection Working Party, the de-listing decisions should "be implemented in such a way that they guarantee the

effective and complete protection of data subjects' rights and that EU law cannot be circumvented. […] In practice, this means that in any case de-listing should also be effective on all relevant domains, including .com". However, Google considers that the right to be digitally forgotten resembles a bell that protects only the European territory by hiding certain search results, so that personal information can be freely processed on the Internet outside the EU.

In the near future, the Court of Justice of the European Union will issue a decision in case C-507/17 on the territorial effect of a de-listing decision. Strictly from the point of view of the effectiveness of the right to be digitally forgotten, any other way than the global implementation will undermine the protection of the data subjects' rights (Şchiopu, 2018a, p. 72) and implicitly the control of the data subjects over their digital footprint. So only time will tell if the right to de-referencing proves to be an effective control tool.

4. Conclusions

While the obligation to inform and the right of access have the purpose of revealing the processing of personal data, the right to be digitally forgotten tends to hide a data processing activity by limiting the excessive visibility that online search engines give to personal data. Thus, the data subjects' rights enshrined in the General Data Protection Regulation may have a divergent effect over the data processing, but they are all intended to strengthen the control that individuals should have over their own personal data. However, the effectiveness of these rights is not always guaranteed, especially when the right to the protection of personal data is balanced against other fundamental rights.

References

- CJEU, Judgment of 13 May 2014, *Google Spain*, Case C‑ 131/12, ECLI:EU:C:2014:317, published in the electronic Reports of Cases (Court Reports - general).
- CJEU, Judgment of 1 October 2015, *Bara*, C-201/14, ECLI:EU:C:2015:638, published in the electronic Reports of Cases (Court Reports - general).
- *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, published in the Official Journal of the European Communities L 281 from 23rd of November 1995.
- European Union Agency for Fundamental Rights, Council of Europe (2018). *Handbook on European data protection law*. Luxembourg: Publications Office of the European Union.
- *Guidelines on the implementation of the Court of Justice of the European Union Judgment on "Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" C-131/12*, WP 225 - Article 29 Data Protection Working Party, adopted on 26 November 2014, Retrieved from http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf, Accessed 29th September 2018.

*** *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), published in the Official Journal of the European Union L 119 from 4th of May 2016.

Lisievici, A. (2015). Monitorul Protecţiei Datelor cu Caracter Personal [Personal Data Protection Monitor]. *Revista română de drept al afacerilor*, no.*10*, p.121-139.

Şandru, D.-M. (2018). Punerea în aplicare a Regulamentului General privind Protecţia Datelor 2016/679. Experienţe din România [The Implementation of the General Data Protection Regulation 2016/679. Romanian Practice]. In D.-M. Şandru, I. Alexe (eds.), *Legislaţia Uniunii Europene privind protecţia datelor*[European Union Data Protection Legislation] (pp. 7-24). Bucharest: Universitară.

Șandru, S. (2016). *Protecția datelor personale și viața privată* [Personal Data Protection and Privacy]. Bucharest: Hamangiu.

Șandru, S. (2017). Transparența prelucrărilor de date personale, între drept și obligație. O nouă configurare europeană a dreptului de informare [The Transparency of personal data processing, between right and obligation. A new European configuration of the right to be informed]. In I. Alexe, N.-D. Ploeșteanu, D.-M. Șandru (coord.), *Protecţia datelor cu caracter personal. Impactul protecţiei datelor personale asupra mediului de afaceri. Evaluări ale experienţelor româneşti şi noile provocări ale Regulamentului (UE) 2016/679* (p. 128-143). Bucharest: Universitară.

Şchiopu, S.-D. (2017a). Efectivitatea dreptului de a fi uitat [The effectiveness of the right to be forgotten]. In I. Alexe, N.-D. Ploeșteanu, D.-M. Șandru (eds.), *Protecţia datelor cu caracter personal. Impactul protecţiei datelor personale asupra mediului de afaceri. Evaluări ale experienţelor româneşti şi noile provocări ale Regulamentului (UE) 2016/679* (p. 188-203). Bucharest: Universitară.

Şchiopu, S.-D. (2017b). Pilonii prelucrării datelor cu caracter personal [The pillars of personal data processing]. *Revista Universul Juridic*, no.6, p.87-102.

Şchiopu, S.-D. (2018a). Aplicarea teritorială a dreptului la uitare digitală (dreptul la înlăturare) în lumina cererii de decizie preliminară introdusă de Conseil d'État (Franța) la 21 august 2017 - Google Inc./CNIL (Cauza C-507/17) [The territorial scope of the right to be forgotten (right to de-referencing) in the light of the request for a preliminary ruling from the Conseil d'État (France) lodged on 21 August 2017 — Google Inc. v CNIL (Case C-507/17)]. *Pandectele române*, no.1, p. 61-72.

Şchiopu, S.-D. (2018b). Obligația de păstrare a evidenței activităților de prelucrare a datelor cu caracter personal [The obligation to keep a record of processing activities for personal data]. *Revista română de drept al afacerilor*, no.1, p.85-94.

Şchiopu, S.-D. (2018c). Scurte considerații asupra dreptului de acces al persoanei vizate în lumina Regulamentului (UE) 2016/679 [Short Considerations on the Right of Access by the Data Subject under Regulation (EU) 2016/679]. *Revista Universul Juridic*, no. *5*, p. 86-93.

Zanfir, G. (2015). *Protecţia datelor personale: drepturile persoanei vizate* [Personal Data Protection the Rights of the Data Subject]. Bucharest: C.H. Beck.