https://doi.org/10.22364/iscflul.7.43

Elīna Muciņa, *Mg. iur.*
Latvia

DATA SUBJECTS' CONTROL OVER THEIR PERSONAL DATA

DATU SUBJEKTU KONTROLE PĀR VIŅU PERSONAS DATIEM

Kopsavilkums

Atsaucoties uz vienu no datu aizsardzības reformas mērķiem, šis raksts veltīts analīzei, kā datu subjekti īsteno kontroli pār saviem personas datiem. Autore identificē personas datu apstrādes principus un pārskata Vispārīgajā datu aizsardzības regulā, kura nosaka šo kontroli, paredzētos instrumentus. Apskatot regulas prasības un to, kā ES tirgus dalībnieki īsteno šīs prasības, autore sniedz šīs kontroles raksturojumu.

Atslēgvārdi: dati, personas datu aizsardzība, privātums, cilvēktiesības

Summary

Referring to one of the objectives of the data protection reform, this article is dedicated to the analysis of the ways data subjects execute control over their personal data. The author identifies the personal data processing principles and examines tools provided by the General Data Protection Regulation that mandate this control. Following the overview of the requirements of the Regulation and their implementation by the EU market participants the author describes the features of this control.

Keywords: data, personal data protection, privacy, human rights

Introduction

Establishing data subjects in control of their personal data was one of the key objectives of the adoption of the new General Data Protection Regulation[1] (hereinafter – Regulation).

In 2012, the European Commission published a communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Region "Safeguarding Privacy in a Connected World. A European Data Protection Framework for the 21st Century",[2] where it informed of its intentions

[1] 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): Official Journal of the European Union, Volume 59, 4 May 2016.

[2] Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Region. Safeguarding Privacy in a Connected World. A European

regarding the personal data reform. The aim of the new legislative acts proposed by the Commission was to strengthen rights, to give people efficient and operational means to make sure they are fully informed about what happens to their personal data and to enable them to exercise their rights more effectively.[3] Moreover, it was intended to strengthen the individuals' ability of control their personal data by ensuring that, when their consent is required, it is given explicitly and freely, equipping internet users with an effective right to be forgotten in the online environment, guaranteeing easy access to one's own data and a right to data portability, reinforcing the right to information so that individuals fully understand how their personal data is handled, particularly when the processing activities concern children.[4]

In the proposal for the Regulation[5] – explanatory memorandum – the European Commission presented further detail of the proposed new legal framework. The European Commission expressed will to build a stronger and more coherent data protection framework in the EU, backed by strong enforcement that would allow the digital economy to develop across the internal market, put individuals in control of their own data and reinforce legal and practical certainty for economic operators and public authorities.[6]

Recitals 6 and 7 of the Regulation state that natural persons should have control of their own personal data in the context of technological developments and globalisation, and how it has changed the routines of personal data processing worldwide. Those developments require a strong and more coherent data protection framework and equally strong enforcement, as it is important to create the trust allowing digital economy to develop across the internal market.

The Regulation, was adopted on 14 April 2016 and, pursuant to Article 99, para. 2 of the Regulation it applies from 25 May 2018.

In this article, the author discusses the concept of control in the context of personal data and identifies the personal data processing principles and examines tools provided by the Regulation that mandate control of data subjects over their personal data.

1. Concept of control

The control is defined as the ability or power to decide or strongly influence the particular way in which something will happen or someone will behave, or the

Data Protection Framework for the 21st Century. Available at: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0009:FIN:EN:PDF [last viewed on May 7, 2019].

3 Ibid.

4 Ibid.

5 Proposal for a Regulation of the European Parliament and of the Council 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). Available at: http://www.europarl.europa.eu/registre/docs_autres_institutions/commission_europeenne/com/2012/0011/COM_COM(2012)0011_EN.pdf [last viewed on May 9, 2019].

6 Ibid.

condition of having such ability or power.[7] Traditionally, the concept of control involves monitoring of factual circumstances and, if the received information does not provide satisfaction or contains deviations from the expected result, deciding on further actions, such as adjusting or taking corrective action.

Therefore, having control in the context of personal data means being properly informed about one's personal data processing, as well as having the opportunity to take effective action in case the received information shows that the personal data are not handled in line with the statutory requirements.

Thus, in order to understand how data subjects can control their personal data, one should first examine the availability of information on the personal data processing and, second, actions data subjects can take if the obtained information does not meet their reasonable expectations.

2. Right to be informed

The right to be informed in personal data protection law is derived from the principles relating to processing of personal data stipulated by Article 5 of the Regulation. Most importantly, it is the principle of transparency that gives power to the individual to enforce the right to be informed. As Advocate General Cruz Villalon rightly stated in the Bara case, the requirement to inform the data subjects about the processing of their personal data guarantees transparency of all processing.[8]

Specifically, transparency applies to three central areas: (1) the provision of information to data subjects related to fair processing; (2) how data controllers communicate with data subjects in relation to their rights under the Regulation; and (3) how data controllers facilitate the exercise by data subjects of their rights.[9] Therefore, the principle of transparency forms an essential basis for the right to be informed.

Other personal data protection principles that strengthen the right to be informed are the principle of fairness and the principle of accountability.

According to the principle of fairness controllers should notify data subjects and the general public that they will process data in a lawful and transparent manner and must be able to demonstrate the compliance of processing operations with the Regulation. Processing operations must not be performed in secret and data subjects should be aware of potential risks.[10]

---

[7] Cambridge Dictionary. Available at: https://dictionary.cambridge.org/us/dictionary/english/control [last viewed on May 11, 2019].

[8] Opinion of Advocate General Cruz Villalón. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62014CC0201 [last viewed on May 10, 2019].

[9] Article 29 Data Protection Working Party. Guidelines on transparency under Regulation 2016/679. Available at: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227 [last viewed on May 6, 2019].

[10] Handbook of European Data Protection Law. Luxembourg: Publications Office of the European Union, 2018, p. 118.

The principle of accountability means that the controller is responsible for, and shall be able to demonstrate compliance with the general data protection principles.[11] Thereby the controller is put in an active position to prove compliance with the general data protection principles at any time, including compliance with the principles of transparency and fairness.

In order to ensure transparency and fairness, the Regulation requires to inform data subjects on several occasions. First of all, every controller has a general duty to inform data subjects on the intended personal data processing in accordance with Articles 13 and 14 of the Regulation. Furthermore, the controller is obliged to inform the data subjects as a part of the right of access[12], as a part of notification obligation regarding rectification or erasure of personal data or restriction of processing[13], on the essence of the joint controllers' arrangement[14], in case of personal data breach if it is likely to result in a high risk to the rights and freedoms of natural persons[15], in personal data transfer situations – where transfer is based on data subject's explicit consent or controller's compelling legitimate interests[16].

As it follows from the Regulation, the obligation to inform the data subject on most occasions is proactive – the controller should provide the information without a request or other action on behalf of the data subject. Only on limited occasions the information is given on the basis of a specific request of a data subject. It confirms the importance of providing data subjects with the information on their personal data processing.

Besides, the Regulation sets the requirements in regard to the form and quality of information to be provided to data subjects. The principle of transparency requires that any information and communication relating to the processing of personal data be easily accessible and easy to understand, and that clear and plain language be used.[17] According to Article 12, paras 1 and 5 of the Regulation, the information or communication shall be in line with the following rules:

- it shall be concise, transparent, intelligible and easily accessible;
- it shall be in clear and plain language;
- it shall be in writing or provided by other means, including, where appropriate, by electronic means;
- when requested by the data subject the information may be provided orally; and
- it shall be provided free of charge[18].

[11] Article 5, para. 2 of the Regulation.

[12] Article 15 of the Regulation.

[13] Article 19 of the Regulation.

[14] Article 26, Para 2 of the Regulation.

[15] Article 34 of the Regulation.

[16] Article 49 of the Regulation.

[17] Recital 39 of the Regulation.

[18] The controller may charge a reasonable fee if requests from data subjects are manifestly unfounded or excessive, in particular because of their repetitive character.

The information needs to be presented to data subjects in a way that it can be properly understood, as opposed to information that is formally compliant with personal data protection rules, but turns out to be useless for individuals due to its complicated formulation.

Nevertheless, most of the data controllers seem to have taken cautious approach in informing the data subjects. Lengthy and complicated privacy policies are drafted in order to ensure that all the required information is given. Thus, there exists an obvious difficulty to combine the need to be transparent, fair and accountable, from one side, and the need to provide data subjects with the necessary information "in an easily visible, intelligible and clearly legible manner"[19] from the other side. Some market participants have found a solution by providing layered documents, drafting overviews of long documents and providing information in an interactive way, for example, in video format, however, the tendency to draft long informative documentation shows that the fear of the Regulation's penalties prevails.

3. Rights to interfere

Articles 15–22 of the Regulation provide the following data subjects' rights which, in essence, allow to interfere with the existing personal data processing: right of access[20], right to rectification[21], erasure ("right to be forgotten")[22], restriction of processing[23], right to data portability[24], right to object to data processing[25], right not to be subject to a decision based solely on automated processing, including profiling[26]. While each of these rights provides data subjects with possibilities to execute control over their personal data, such as rectify inaccurate personal data., in this article the author focuses specifically on the right of access.

The right of access consists of: (1) the right to obtain from the controller confirmation as to whether or not personal data concerning data subject are being processed; (2) if personal data are being processed, then additional right to access the personal data and certain information on the personal data processing; (3) the right to obtain a copy of the personal data undergoing processing.[27]

The acquired information provides data subjects with an overview of the relevant personal data processing. It allows them to evaluate the personal data processing in the necessary detail and enables to exercise other rights[28] stipulated in Articles 16–22 of

[19] Article 12, Para 7 of the Regulation.
[20] Article 15 of the Regulation.
[21] Article 16 of the Regulation.
[22] Article 17 of the Regulation.
[23] Article 18 of the Regulation.
[24] Article 20 of the Regulation.
[25] Article 21 of the Regulation.
[26] Article 22 of the Regulation.
[27] Article 15 of the Regulation.
[28] Court of Justice of European Union judgement of 7 May 2009 in case No. C-553/07.

the Regulation, as data subjects can interfere and challenge handling of their personal data only if sufficient information is at their disposal. Therefore, in the context of possibilities to control the personal data, the right of access should be evaluated as a primary right compared to all the remaining rights stipulated in Articles 16–22 of the Regulation.

Contrary to the right to be informed, the right of access and other rights listed above are reactive, since they can be enforced only if the data subject submits a request to the controller. It means that data subjects are given the authority to decide whether to use their rights provided by Articles 15–22 of the Regulation.

In order to strengthen these rights, the Regulation imposes certain obligations on the data controller. Namely, Article 12, para. 2 of the Regulation requires the controllers to facilitate the exercise of data subjects' rights under Articles 15–22. It is left to the controllers to decide what measures should be implemented in order to comply with this provision. Moreover, the controllers can refuse to act on the request of the data subject for exercising their rights under Articles 15–22 only in two occasions: either the controller demonstrates that it cannot identify the data subject or the request is manifestly unfounded or excessive.

When the controller receives the request of the data subject regarding the enforcement of his rights provided in Articles 15–22 of the Regulation, the following shall be observed in order to comply with the Regulation:

- the response on action taken on a request shall be given without undue delay and in any event within one month of receipt of the request. An opportunity to extend the response period by two months is available, informing the data subject of such extension within one month of receipt of the request, explaining the reasons for the delay[29];
- if the controller decides not to take action on the request, it shall inform the data subject without delay and at the latest within one month of receipt of the request, stating the reasons and the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy[30];
- response shall be free of charge[31];
- the same rules regarding information form and quality as provided in the previous section apply[32];
- where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject[33].

By setting out clear rules of handling data subjects' requests, the Regulation provides effective process of enforcement of their rights.

---

[29] Article 12, para. 3 of the Regulation.

[30] Article 12, para. 4 of the Regulation.

[31] Except cases of manifestly unfounded or excessive requests, then reasonable costs might be applied (or, alternatively, the controller may refuse to act on the request).

[32] Article 12, para. 1 of the Regulation.

[33] Article 12, para. 3 of the Regulation.

Overall, the controllers treat the obligation to respond to the requests of data subjects seriously and implement procedures for effective and timely processing of data subjects' requests. The most common feature seen on the market is designation of a contact point for receipt of the requests, for instance, a specific e-mail account in order to ensure that all data subjects' requests are received and responded on time. It is also common to draft internal policies describing detailed procedures for handling data subject requests and to include instructions in the trainings on application of the Regulation.

4. Consent

Data subject's consent is one of the legal grounds that allow personal data processing. This legal ground focuses on the self-determination of the data subject as a ground for legitimacy. All the other grounds, in contrast, allow processing in situations where irrespective of consent, it is appropriate and necessary.[34]

Although in personal data protection law a consent is traditionally viewed as a separate concept, it forms an essential part of data subjects' control: consent can only be an appropriate lawful basis for personal data processing if the data subject is offered control and a genuine choice with regard to accepting or declining the terms offered or declining them without detriment. If obtained in full compliance with the Regulation, consent is a tool that gives data subjects control over whether or not personal data concerning them will be processed.[35]

Article 4, para. 11 of the Regulation defines consent of the data subject as 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 addition, Article 7 states certain obligations that shall be fulfilled in order to obtain legally valid consent.

With regard to consent, the control of a data subject arises in connection with the requirement for a controller to obtain freely given consent. The element 'free' implies a real choice and control of the data subjects. As a general rule, the Regulation prescribes that, if the data subject has no real choice, feels compelled to consent or will endure negative consequences if they do not consent, then consent will not be valid.[36]

---

[34] Article 29 Data Protection Working Party. Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC. Available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf [last viewed on May 7, 2019].

[35] Article 29 Data Protection Working Party. Guidelines on consent under Regulation 2016/679. Available at: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051 [last viewed on May 8, 2019].

[36] Article 29 Data Protection Working Party. Guidelines on consent under Regulation 2016/679. Available at: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051 [last viewed on May 8, 2019].

Accordingly, the consent cannot be considered free if the data subject is unable to refuse without any detriment.[37]

Therefore, the right to give consent or refuse is an important tool for execution of the data subjects' control. In fact, the element 'free' also gives an important insight into the concept of control – in order to execute control, the data subjects shall have a real choice.

Furthermore, the Regulation stipulates two different forms of consent: consent can either be simple, or explicit. I.e., on some occasions it is sufficient to obtain consent, given that the requirements of Article 4, Para 11 and Article 7 of the Regulation are met. On other occasions, the Regulation requires the controller to obtain an explicit consent. It has been explained that the latter is required in situations where particular data protection risks may emerge, and thus, a high individual level of control over personal data is required, as in the case of the processing of special category data and automated decisions. Such particular risks also appear in the context of international data transfers.[38] As a result, when giving consent, different levels of control may apply.

An important component of consent is the right to withdraw it. Pursuant to Article 7, Para 3 a data subject is entitled to withdraw his or her consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal. The Regulation requires to ensure that the withdrawal of consent is as easy as giving consent.

Thereby, the Regulation ensures full control over data subjects' consent: if the data subject changes his mind and no longer wishes his personal data processing, he can easily refuse it at any time.

If consent is withdrawn, all data processing operations based on consent that took place before the withdrawal, if performed in accordance with the Regulation, remain lawful, however the controller must stop the processing actions concerned. Moreover, if there is no other lawful basis justifying the processing of the personal data, they should be deleted by the controller.[39]

As a result, consent as a legal basis is used rarely, fearing the unexpected withdrawals. Since the personal data processing is allowed only if a lawful basis determined by the Regulation exists, controllers first assess whether any alternative legal ground may apply for the intended personal data processing. And only on those occasions when other legal grounds cannot be applied, it is evaluated whether consent might be an option, considering its requirements and potential consent withdrawals.

---

[37] Ibid.

[38] European Data Protection Board. Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679. Available at: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf [last viewed on May 11, 2019].

[39] Article 29 Data Protection Working Party. Guidelines on consent under Regulation 2016/679. Available at: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051 [last viewed on May 8, 2019].

Conclusions

Having control in the context of personal data means being properly informed of one's personal data processing, as well as having opportunity to take effective action in case the received information shows that the personal data are not handled in line with the statutory requirements.

Data subject's control means that the data subject has a genuine choice. For instance, it can choose whether to give the consent or not, whether to interfere with the existing processing or not, which right to enforce towards the data controller, etc.

The right to be informed stems from the principles of transparency and fairness and is reinforced by the principle of accountability. The enforcement of the right to be informed forms a precondition for fulfilment of all the other rights of data subjects.

The right of access should be evaluated as a primary right of the data subjects provided for in Articles 15–22 of the Regulation, as it provides the possibility to obtain the necessary details of personal data processing and then decide on the need to pursue further action.

In addition to data subject rights provided for in Articles 13–22 of the Regulation, an important tool for executing control is the data subjects' consent. Depending on the risks related to personal data processing, either a simple or an explicit consent might be required.

The Regulation provides data subjects with more control over their personal data than ever. However, the effective execution of this control is determined by the controller.

The market participants have power to boost the control of the data subject. However, the fear of fines remains high and a formal approach in ensuring the data subjects' rights prevails.

BIBLIOGRAPHY

Literature

1. Handbook of European Data Protection Law. Luxembourg: Publications Office of the European Union, 2018.

Normative acts

2. 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): Official Journal of the European Union, Volume 59, 4 May 2016.

Court practice

3. Court of Justice of European Union judgment of 7 May 2009 in case No. C-553/07.

Internet sources

4. Article 29 Data Protection Working Party. Guidelines on consent under Regulation 2016/679. Available at: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051 [last viewed on May 8, 2019].
5. Article 29 Data Protection Working Party. Guidelines on transparency under Regulation 2016/679. Available at: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227[last viewed on May 6, 2019].
6. Article 29 Data Protection Working Party. Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC. Available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf [last viewed on May 7, 2019].
7. Cambridge Dictionary. Available at: https://dictionary.cambridge.org/us/dictionary/english/control [last viewed on May 11, 2019].
8. Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Region. Safeguarding Privacy in a Connected World. A European Data Protection Framework for the 21st Century. Available at: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0009:FIN:EN:PDF [last viewed on May 7, 2019].
9. European Data Protection Board. Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679. Available at: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf [last viewed on May 11, 2019].
10. Opinion of Advocate General Cruz Villalón delivered on 9 July 2015. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62014CC0201[last viewed on May 10, 2019].
11. Proposal for a Regulation of the European Parliament and of the Council 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). Available at: http://www.europarl.europa.eu/registre/docs_autres_institutions/commission_europeenne/com/2012/0011/COM_COM(2012)0011_EN.pdf [last viewed on May 9, 2019].