KATARZYNA MORAWSKA

OBJECTION TO PROCESSING PERSONAL DATA AS AN EXPRESSION OF THE RIGHT TO PRIVACY[1]

INTRODUCTION

Steady technological development stems from ever larger body of data being processed; as a result profiles of service users – data subject may be created. In times when we more or less consciously decide to share our private sphere, the right to privacy must be specially protected. This right is inextricably linked with the need to exercise effective control over the transferred data, and hence awareness must be built on the purposes and method of personal data's possible processing by the controllers.

The need to ensure effective protection of personal data and to regain control over the processing of data by data subjects has been raised for many years as a key challenge for ensuring the right to privacy[2]. Cornerstone for national legislation until 25 May 2018, Directive 95/46/EC[3], had failed to address the needs of modern society and the challenges posed by modern technologies. A pan-European reform attempts to adapt EU legislation in personal data protection to these challenges.

Regulation (EU) 2016/679 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 and repealing Directive 95/46/EC (hereinafter "the GDPR")[4] imposes a number of new obligations on personal data controllers with a view to ensuring more effective

[1] Artykuł przetłumaczony ze środków finansowanych przez Ministerstwo Nauki i Szkolnictwa Wyższego na działalność upowszechniającą naukę (DUN), nr decyzji 810/P-DUN/2018. Article translated from funds financed by the Ministry of Science and Higher Education for the dissemination of science (DUN), Decision No. 810 / P-DUN / 2018.

[2] Communication from the Commission on Promoting Data Protection by Privacy Enhancing Technologies (PETs) Brussels 2017, access on 15.07.2019

[3] 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, OJ L 281, 23.11.1995, p. 31–50.

[4] 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, OJ L 119, 4.5.2016, p. 1–88.

protection and security of the data they process and provides for liability for breaches of the GDPR rules (criminal, administrative and civil liability).

Under the GPRD data subjects been considerably empowered to exercise their rights more effectively. The publication discusses empowering data subjects specified in the GDPR, a most important aspect of the data protection reform, vital for examining the privacy right particular the following, and illustrates it with the right to object.

The publication argues that the right to object to data processing expresses the right to privacy viewed as the right to control the processes of personal data processing and to exercise real control over how data controllers may use personal data.

However, neither the rights, including the right to object, nor other institutions protecting privacy under GDPR will be properly exercised and applied unless they strictly link the protection mechanisms - this is a novelty implemented by GDPR to make the regulatory rights and obligations more effective.

The publication will also consider the administrative sanctions that the supervisory authority may impose on personal data controllers or processors for non-compliance with the rules on data subjects' rights.

DATA SUBJECTS' RIGHTS AS AN EXPRESSION OF THE PROTECTION OF THE RIGHT TO PRIVACY

Under Article 1(2), GDPR also aims to implement the fundamental rights and freedoms of natural persons, in particular the right to the protection of personal data[5]. The postulate to empower data subjects necessities parallel strengthening the enforcement of their rights, which has been ensured by such instruments as high administrative penalties, but also by emphasizing informing data subjects about the catalogue of information that the data controller must provide.

This obligation is set forth in Articles 13 and 14 of the GDPR, which implement the principles of fair and transparent processing, whereby a data subject must be informed of the existence of the processing operation and its purposes, and of its rights (recital 60 of the GDPR).

[5] A. Grzelak, *Główne cele ogólnego rozporządzenia o ochronie danych*, [in:] ed. M. Kawecki, T. Osiej, *Ogólne rozporządzenie o ochronie danych - Wybrane zagadnienia*, p. 18.

The controller should provide the data subject with other necessary information, on considering the specific circumstances and the specific context of personal data processing. By way of illustration, the controller should inform the data subject of profiling and its consequences. An information obligation clause may be the appropriate place to implement the provisions of Article 22 of the GDPR.

While examining the right to object, it is worth noting that the data subject is entitled to object to their personal data being profiled. To this end, the data subject should be informed of this form of personal data processing at the stage of data collection under the information requirement clause. Data subjects should be able to exercise their right not to be subject to a decision based solely on automated processing (including profiling) and which produces legal effects vis-à-vis them or similarly significantly affects them. It is emphasized that Article 21(4) of the GDPR commits the controller to inform the data subject of the right to object[6].

Furthermore, if the controller collects personal data directly from the data subject, the latter must be informed whether it is required to communicate the personal data and of the consequences of not doing so. On the other hand, if the data are obtained from a source other than the data subject, the controller must provide information about the categories of data received (for instance contact details, identification data) and about the source of the data (such as the employer of this person, referral person, entity from the capital group to which the data subject has consented).

Recital 61 points to the moment when the information obligation should be fulfilled both when the data are collected directly (Article 13 of GDPR) and indirectly (Article 14 of GDPR). The data subject should be informed of the processing of its personal data upon collection and, for the data from another source within a reasonable period, within one month at the latest. Where personal data are to feed into communication with the data subject, the clause should be communicated at the latest at the first communication with the data subject and where disclosure to another recipient is planned, the information obligation should be fulfilled at the latest at the first disclosure.

In the context of the examination of Articles 12, 13 and 14 of GDPR, the implementation of the right to privacy aims not only to build awareness of data subjects of their rights, but also

[6] P. Fajgielski, *Komentarz do art. 14 ogólnego rozporządzenia o ochronie danych*, [in:] Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz, p. 147.

to ensuring that data subjects' requests are respected under the procedure laid down in Article 12 of GDPR. This Article provides for transparent information and communication with data subjects. This provision refers to the general principle that the information obligation should be written in clear and simple language and specified the manner in which the controller should respond to the data subject's requests. In principle, requests should be responded within one month. Nonetheless, this time limit may be extended to a total of three months[7]. Where the controller fails to respond to the request or refuses to respond to it, the data subject may lodge a complaint with the supervisory authority against the controller or directly request an order to comply with the request[8].

Not only is the goodwill of the controllers of personal data or of the processors of data on their behalf a guarantee of the application of the GDPR, but above all the risk of severe administrative sanctions by national supervisory authorities. Under Article 83 of the GDPR, 'each supervisory authority shall ensure that the imposition of administrative fines (…) shall in each individual case be effective, proportionate and dissuasive'. For infringements of the provisions on the fulfilment of the information requirement and of the rights of data subjects, fines of up to EUR 20,000,000 are provided for in Article 83(5), or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year[9]. These obligations are nothing new, as they were effective in the previous legal situation, hence the risk of a fine is higher. On the other hand, for a breach of the obligations of a controller and processor introduced by a GDPR, such as those referred to in Articles 8, 11, 25 to 39, 42 and 43, or of the obligations of a certification body, the authority may impose a fine of up to EUR 10,000,000 and, in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year.

In view of the function to be performed by the fine, that is primarily to act as a deterrent, when mitigating the fine, the authority considers that the penalty be proportionate to the infringements and effective.

[7] P. Litwiński, *Komentarz do art. 12*, [in:] *ed*. P. Litwiński, M. Kawecki, P. Barta, *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz*,, (7).
[8] P. Fajgielski, *Komentarz do art. 12 ogólnego rozporządzenia o ochronie danych*, [in:] Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz, p. 99.
[9] J. Łuczak, *Artykuł 83 Ogólne warunki nakładania administracyjnych kar pieniężnych* [in:] ed. D. Lubasz, E. Bielak-Jomaa, *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, p.1054-1065.

Pursuant to Article 83(2) of the GDPR, when measuring the penalty, the authority shall consider the nature, gravity and duration of the infringement taking into account the nature, scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them. It also assesses the categories of personal data affected by the infringement, that is whether the infringement concerned sensitive data referred to in Article 9 of the GDPR or the so-called ordinary data. Moreover, the authority assesses the intentional or negligent character of the infringement and any previous infringements by the controller or processor. The authority may also take into account any action taken by the controller or processor to mitigate the damage suffered by data subjects. It also assesses the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32 of the GDPR (that is data protection by design and by default under Article 25 and security of processing under Article 32 of the GDPR). It is also important that the supervisory authority takes into account the degree of cooperation with the supervisory authority in order to remedy the breach and mitigate its possible negative consequences. Aside of the degree of cooperation, the manner in which the infringement became known to the supervisory authority is important, in particular whether, and if so to what extent, the controller or processor notified the infringement. It is also assessed whether the measures referred to in Article 58(2) of the GDPR (i.e. "the controller or processor concerned" have been previously applied to the controller or processor in the same case. corrective powers of supervisory authorities, such as: to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of this Regulation, to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation, to order the controller or the processor to comply with the data subject's requests, to order the controller to communicate a personal data breach to the data subject or to impose a temporary or definitive limitation including a ban on processing).

The catalogue of factors that the supervisory authority may take into account when imposing a sanction is open. As the last one, the EU legislator referred to 'any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement'.

It follows from the above that the proposal to exercise the rights of data subjects has been guaranteed by the EU legislator first of all by defining the way in which the controller should communicate the rights to data subjects (fulfilment of the information obligation) and secondly by ensuring appropriate sanctions for non-compliance.

The approach of the national supervisory authority to this postulate is illustrated by the decision issued by the President of the Office for Personal Data Protection awarding the first administrative fine[10] under GDPR, for default on information obligation. In its decision ZSPR.421.3.2018, the authority stated, among others, that the breach was of a serious nature as it concerned the fundamental rights and freedoms of persons whose data the Company had processed (processed). The Company's activity also violated the fundamental principle of fairness and transparency as regards personal data processing (Article 5(1)(a) of the GDPR). The breach by the Company of the obligation to provide basic information on the processing and the instructions on the rights to which data subjects are entitled in relation thereto (specified in Articles 15-21 of the GDPR) was considered by the authority as entailing such effects as the risk of stripping data subjects of these rights[11].

RIGHT TO OBJECT TO PROCESSING DATA

The right to object to the processing of data is set out in Article 21 of the GRPD. The provision explicitly specifies prerequisites entitling the data subject to exercise this right and the consequences of lodging an objection. This provision also enumerates the data controller's obligations regarding the proper transfer of information to data subjects as to the manner of exercising this right.

One could already object to the processed data under the previous legal regime, however, significant changes have been introduced in the GDPR, in particular with respect to the rules of exercising the right pointed out in Article 21. First of all, the right to object is applied depending on the ground for processing personal data. This right may therefore be exercised when processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller and when processing is necessary for the purposes of legitimate interests pursued by the controller or by a third party. Therefore, the right to object may not be exercised when data are processed under a consent,

[10] The President of the Office of Personal Data Protection (UODO) has awarded the first fine of over PLN 943 thousand, source: https://uodo.gov.pl/pl/138/786, access on 15.07.2019.
[11] Decision of the President of the Office for the Protection of Personal Data ZSPR.421.3.2018, source: https://uodo.gov.pl/pl/324/787, access on 15.07.2019.

contract or legal obligation and when the data are necessary to protect the vital interests of the data subject[12].

As becomes clear from this consideration, the right to object derived from the need to ensure equivalent protection of data subjects whose data are processed on a legal ground which does not require their active involvement, such as the expression of a declaration of intent - consent in the form of a check box.

Within this power, there are some differences in the additional requirements that the data subject has to demonstrate. The distinction is based on the circumstances, in which the data are processed, whereby the data subject must in some cases demonstrate additionally that the objection is supported by the specific situation of the data subject. This will be the case when data are processed under the above legal ground, as set out in Article 6(1)(e) and Article 6(1)(f), when personal data are processed in the performance of public tasks, exercise of public authority and on the grounds of the controller's legitimate interest. In the area of new technologies, we will most often have to deal with legitimate interests, and this ground may underpin such processing as sending a newsletter, actions taken under the controller's own marketing, or liaision with consumers in the provision of services under the binding contract. Apart from the Internet environment, processes based on this premise may include CCTV monitoring, annual assessment of employees and collaborators, use of the employee's image under the consent given by the employee to disseminate the image.

As a result of a reasoned objection, the controller is not allowed to process such personal data, unless it proves that there are legitimate grounds for further processing. These grounds shall prevail over the interests, rights and freedoms of the data subject or the grounds for the establishment, exercise or defence of legal claims. That said, according to recital 69, it should be for the controller to demonstrate that its compelling legitimate interest overrides the interests or the fundamental rights and freedoms of the data subject.

However, as P. Fajgielski emphasizes, already in the previous regime, a view prevailed that where the data processing is based on more than one condition of admissibility (for instance the same data used for contract performance and for marketing), lodging an objection may not result in data being erased (the contract would then become inoperative), but only in

[12] P. Fajgielski, *Komentarz do art. 21 ogólnego rozporządzenia o ochronie danych*, [in:] Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz, p. 144.

discontinuation of their use for marketing[13]. In other words, after having objected to the receipt of marketing materials, the data subject should no longer receive these materials, whereas if the parties are for instance bound by a service contract, personal data may continue to be processed by the controller and used solely for that purpose.

In certain circumstances, in addition to raising objections, the data subject has to demonstrate a special situation. It is worthwhile to discuss here what this particular situation of the data subject may be. A specific situation may link to the disclosure by processing of data related to a private or family sphere[14]. Moreover, a specific situation should be considered a factual situation which was either absent at the collection of personal data (if these were collected directly) or which persisted during collection but was not known to the controller (indirect data collection). When assessing the specific situation of the data subject, it should be taken into account that this situation should affect the processing of personal data in such a way as to strike interests of the data subject and the controller into disequilibrium[15].

No specific situation must be invoked by persons who object to the processing for marketing purposes, namely in direct marketing. According to Article 21(2) of the GDPR, 'where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing'. By objecting to the processing of data for the purposes of direct marketing, the controller is not positioned to demonstrate, as above, that it needs the data, for example, for the protection of claims. The right to object is particularly applicable in relation to the use of information society services. These services are not defined in the GDPR as the provision of the Regulation refers in this respect to Directive (EU) 2015/1535 of the European Parliament and of the Council laying down a procedure for the provision of information in the field of technical regulations and of rules on information society services[16]. An information society service is therefore any service normally provided for consideration, at a distance, by electronic means and on an

[13] P. Fajgielski, *Komentarz do art. 14 ogólnego rozporządzenia o ochronie danych*, [in:] Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz, p. 146.
[14] J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych. Komentarz*, p. 531.
[15] P. Litwiński, *Komentarz do art. 21*, [in:] *ed.* P. Litwiński, M. Kawecki, P. Barta, *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz.*(4).
[16] Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services, OJ L 241, 17.9.2015, p. 1–15.

individual basis[17]. In accordance with Article 21(5), the GPRD requires that the right of objection may be exercised by automated means involving the use of technical specifications. According to the doctrine, this requirement may be interpreted as a necessity for a controller processing data on a website to ensure that the right of objection may be exercised as a functionality available on that website[18].

In conclusion, it is worth highlighting the differences between objection and withdrawal of consent. While the effects of filing both requests will, as a rule, be very similar to each other, for the former, the controller may, in specific cases, continue to process personal data. It can be done where the objection does not relate to marketing tasks and where the controller can demonstrate that its important legitimate interests override the interests or fundamental rights and freedoms of the data subject. On the other hand, if a consent constitutes the only ground for the controller to be entitled to process data, the withdrawal of consent shall mean that the controller is no longer able to process the data for this purpose[19].

CONCLUSCION

The right to privacy as regards personal data protection particularly links to the right to restrict certain personal information for a private use and not to encroach on personal privacy by retaining control over what information, including marketing information, will take private time. Moreover, as human activities have moved into the digital world, the risk of inadequate control over what happens to personal data processed by personal data controllers or processors has soared. With a view to minimising this risk, the GDPR has introduced a number of tools that natural persons may exercise control over the data processed. Correlation of powers with high sanctions, the rules of which resemble those of competition and consumer protection law, constitutes a kind of guarantee for the exercise of rights of data subjects. Additionally, by strengthening the catalogue of information that the controller must provide under Articles 13 and 14 of the GDPR, data subjects are more and more aware of their rights, legal grounds for

[17] P. Makowski, D. Lubasz, *Artykuł 4 pkt 25 Usługa społeczeństwa informacyjnego*, [in:] ed. D. Lubasz, E. Bielak-Jomaa, *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*., p. 311.
[18] P. Fajgielski, *Komentarz do art. 14 ogólnego rozporządzenia o ochronie danych*, [in:] Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz, p. 147.
[19]P. Litwiński, *Komentarz do art. 21*, [in:] *ed.* P. Litwiński, M. Kawecki, P. Barta*, Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz.*, (11).

data processing or the purposes for which data are processed. Interestingly, whereas the information obligation clauses have contained more information on data processing following 25 May 2018, and thanks to the information campaign on the entry into force of the GDPR, the number of complaints received by the Office for Personal Data Protection since that date has stood at approx. 2 400. Compared to the prior year, 2017 which witnessed nearly 3 000 complaints, this apparently marks a considerable surge in the number of complaints, and thus a greater awareness of data subjects[20].

The right to object to the processed data seems to be a power that closes a kind of gap when the data of a data subject are processed on a ground that does not require an active participation of the natural person. Respectively, this right enables the data subject to take control of the processed data in an effective and expeditious manner. In particular, this will be a practical solution where the controller uses the data for direct marketing.

However, since the GDPR contains numerous general clauses, a risk arises that the provisions will be interpreted in favour of controllers and processors. In order to limit this, guidelines and guidance of any kind, whether issued by the supervisory authorities or the European Data Protection Board, under Article 57(1), could be employed.

BIBLIOGRAPHY

Barta, J., Fajgielski, P., Markiewicz, R. *Ochrona danych osobowych. Komentarz*, Warszawa 2015.

CyberDefence24, *Prezes UODO: Mamy ogromną liczbę skarg,* source: https://www.cyberdefence24.pl/nato/anuluj-zapisz-zmiany-prezes-uodo-mamy-ogromna-liczbe-skarg, access 15.07.2019.

Decision of the President of the Office for the Protection of Personal Data ZSPR.421.3.2018, source: https://uodo.gov.pl/pl/324/787, access on 15.07.2019.

[20]E. Bielak- Jomaa, *Prezes UODO: Mamy ogromną liczbę skarg,* źródło: https://www.cyberdefence24.pl/nato/anuluj-zapisz-zmiany-prezes-uodo-mamy-ogromna-liczbe-skarg, access 15.07.2019.

Fajgielski, P. *Komentarz do art. 12 ogólnego rozporządzenia o ochronie danych*, [in:] Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz, Warszawa 2018.

Fajgielski, P. *Komentarz do art. 14 ogólnego rozporządzenia o ochronie danych*, [in:] Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz, Warszawa 2018.

Fajgielski, P. *Komentarz do art. 21 ogólnego rozporządzenia o ochronie danych*, [in:] Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz, Warszawa 2018.

Grzelak, A., *Główne cele ogólnego rozporządzenia o ochronie danych*, [in:] red. M. Kawecki T. Osiej, *Ogólne rozporządzenie o ochronie danych - Wybrane zagadnienia*, Warszawa 2017.

European Commission - Press release, *Commission proposes high level of privacy rules for all electronic communications and updates data protection rules for EU institutions*, Brussels 2017.

Litwiński P., *Komentarz do art. 12*, [in:] *ed.* P. Litwiński, M. Kawecki, P. Barta,, *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz,* Warszawa 2017.

Litwiński P., *Komentarz do art. 21*, [in:] *ed.* P. Litwiński, M. Kawecki, P. Barta, *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz.,* Warszawa 2017.

Łuczak, J. *Artykuł 83 Ogólne warunki nakładania administracyjnych kar pieniężnych* [in:] ed. Lubasz D., Bielak-Jomaa, E., *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, Warszawa 2017.

Makowski, P., Lubasz D., *Artykuł 4 pkt 25 Usługa społeczeństwa informacyjnego*, [in:] ed. Lubasz D., Bielak-Jomaa E, *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, Warszawa 2017.

UODO, *The President of the Office of Personal Data Protection (UODO) has awarded the first fine of over PLN 943 thousand.*, source: https://uodo.gov.pl/pl/138/786, access on 15.07.2019.