DATA PROTECTION OFFICER IN THE LIGHT OF THE PROVISIONS OF THE GENERAL DATA PROTECTION REGULATION (GDPR)

RYSZARD SZAŁOWSKI*

DOI: 10.26399/iusnovum.v12.4.2018.38/r.szalowski

An information security administrator played an important role in the enforcement of the provisions of the Act of 29 August 1997 on the protection of personal data[1] as his main task was to ensure the compliance with the provisions of this statute, especially by:

– checking the compliance of data processing with the provisions;
– supervising development and updating of documents describing the way of data processing and technical and organisational means ensuring their protection, as well as the compliance with the rules determined in the documents; and
– ensuring that persons authorised to process personal data get acquainted with the provisions on their protection.[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) [3] entered into force on 25 May 2016 and has been applicable since 25 May 2018. The provisions of Chapter IV Section 4 GDPR (Articles 37 to 39) regulate the designation, status and tasks of the data protection officer (hereinafter: DPO). The function constitutes a counterpart of the

* PhD hab., Associate Professor, Faculty of Philology and History of Jan Długosz University in Częstochowa; e-mail: r.szalowski@ujd.edu.pl

1 Uniform text, Journal of Laws [Dz.U.] of 2016, item 922.

2 For information about the designation, tasks and status of the information security administrator, see: R. Szałowski, *Administrator bezpieczeństwa informacji*, Ius Novum No. 4, 2016, pp. 208–224 and the literature referred to therein.

3 OJ L 119 of 4.5.2016; hereinafter: GDPR.

information security administrator that operated earlier based on the provisions of Act on the protection of personal data.

The article aims to present, analyse and assess new regulations of the European Union law concerning the DPO's designation, tasks and status.

1. DESIGNATION OF THE DATA PROTECTION OFFICER

The DPO designation is regulated in Article 37 GDPR. The EU legislator calls the assignment of the DPO duties to a particular person a designation, which does not seem to be an accurate term in the light of legal jargon because it actually concerns employment, which seems to be confirmed by the specification laid down in Article 37 para. 6 stipulating that the DPO may be a staff member or fulfil tasks based on the basis of a service contract.

The DPO designation may take place as part of the fulfilment of the obligation determined in the GDPR provisions or result from the use of the adequate authorisation. The controller[4] or the processor[5] designate the DPO.

The issue concerning the scope of the obligation to designate the DPO is regulated in Article 37 para. 1 GDPR. The controller and the processor always designate the DPO when at least one of the three conditions laid down in the provision is fulfilled. The designation of the DPO is an obligation of the controller or the processor independently, which means that "the obligation can be fulfilled only by the controller or only by the processor, or by both entities at the same time".[6] Editing the content of the provision, the EU legislator ignores the fact that in the light of the GDPR provisions concerning the scope of rights of the obliged party, i.e. the controller or the processor, employment may not be possible in accordance with national laws. Thus, using the GDPR terminology, the controller or the processor may designate, i.e. employ, the DPO if, at the same time, he performs the function of the head of a unit or is authorised to employ staff in the organisation.

The first reason for the obligation is the performance of data processing by a public authority or body, except for courts acting in their judicial capacity. Thus, it concerns not only public authorities or bodies but also other entities, e.g. organisational or administrative units.[7] There is an opinion presented in literature

---

[4] In accordance with Article 4(7) GDPR, "controller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

[5] In accordance with Article 4(8) GDPR, "processor" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

[6] E. Bielak-Jomaa, [in:] E. Bielak-Jomaa, D. Lubasz (ed.), *RODO ogólne rozporządzenie o ochronie danych. Komentarz*, Warsaw 2018, p. 770. Similarly, P. Litwiński, P. Barta, M. Kawecki, [in:] P. Litwiński (ed.), P. Barta, M. Kawecki, *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz*, Warsaw 2018, p. 556.

[7] For more on the concepts of public authority or body, see: P. Litwiński, P. Barta, M. Kawecki, *Rozporządzenie UE w sprawie ochrony…*, pp. 557–559, and E. Bielak-Jomaa, [in:] *RODO ogólne rozporządzenie...*, pp. 772–773.

that also non-public entities performing public tasks are obliged to designate a DPO.[8] I do not share the opinion. It does not match the grammatical interpretation of the provision of Article 37 para. 1 GDPR because it constitutes grounds for deciding on the obligations. Thus, every obliged entity should be directly indicated in the content of the provision because the obligation it has cannot be subject to a presumption or the application of extended interpretation.

Regardless of the literal content of the provision, the legislator does not treat courts as an exception. If the exemption of courts from the obligation to designate a DPO is to exclude acting in their judicial capacity, this means that a court is obliged to designate a DPO but the scope of his competences (rights and obligations) must not cover the issues concerning the administration of justice.[9] Thus, a court shall designate an officer but "his or her duties will not include monitoring the compliance with the provisions in case of the data processing within a court's adjudication proceedings, e.g. data contained in court files or databases used to support adjudication".[10]

In accordance with Article 37 para. 3 GDPR, if the controller or the processor is a public authority or body, a single DPO can be designated for a few such authorities or bodies, depending on their organisational structure and size. As it is emphasized in literature, "the aim of this regulation is to avoid the designation of a single officer by a few big public authorities (or bodies processing a lot of data), and to designate a single officer by entities whose tasks are mutually connected. The provision does not indicate which of the entitled entities shall designate an officer and whether and under what condition they may withdraw from the earlier decision to designate a single DPO".[11] As M. Zadrożny emphasizes, "the designation of a single officer for a few entities should be carefully considered because it can result in fictitious supervision over the system of data protection in those entities".[12]

Other reasons for the creation of the obligation to designate a DPO concern only non-public entities, although the content of Article 37 para. 1 GDPR lacks such a reservation. It results *a contrario* from the general wording of the provision of para. 1(a) laying down the obligation for public authorities or bodies; thus, every public authority or body must designate a DPO, regardless of any subject-related circumstances. If the legislator indicates those reasons in the content of para. 1(b) and (c), it should be assumed that they apply only to non-public entities.

The designation of a DPO is the obligation of the non-public controller or the processor if their main activity[13] consists in data processing on a large scale:

---

[8] P. Litwiński, P. Barta, M. Kawecki, *Rozporządzenie UE w sprawie ochrony*…, p. 559.

[9] Similarly, E. Bielak-Jomaa, [in:] *RODO ogólne rozporządzenie*..., p. 775.

[10] K. Syska, *Administrator bezpieczeństwa informacji a inspektor ochrony danych – porównanie przesłanek powołania, statusu i zadań*, Monitor Prawniczy No. 20 (supplement), 2016, p. 76.

[11] *Ibid*.

[12] M. Zadrożny, *Inspektor ochrony danych (IOD) jako następca ABI*, [in:] A. Dmochowska, M. Zadrożny (ed.), *Unijna reforma ochrony danych osobowych. Analiza zmian*, Warsaw 2016, Legalis.

[13] In accordance with one of the theses of Recital 97 GDPR, in the private sector, the core activities of a controller relate to this body's primary activities and not to the processing of personal data as ancillary activities.

– and the nature, scope and aims of such operations require regular and systematic monitoring of persons whose data are processed, or
– data that are subject to processing belong to a special category referred to Article 9 para. 1,[14] and personal data concerning convictions and law violations referred to in Article 10.[15]

First of all, it should be stated that, while an obligation to designate a DPO by public authorities or bodies is absolute in nature and is not limited, the same obligation addressed to non-public entities was edited in a relatively liberal way. This raises serious doubts because a DPO should serve the ensuring of personal data protection, regardless of the fact whether a public or a non-public entity processes them.

The liberalism of the legislator's approach to the designation of a DPO by a non-public entity is expressed in the limitation of this obligation for the controllers and processors of data on a large scale within the scope of their main activity and only when the nature, scope and aims of the processing operations require regular and systematic monitoring of persons whose data are processed, or when data processed on a large scale within the main activity belong to special categories of personal data or personal data concerning convictions and law violations. Thus, monitoring people, even regularly and systematically, does not create the discussed obligation if it is not performed on a large scale, or when the scale of monitoring is large but it takes place beyond the sphere of the main activity. Similarly, the processing of special category personal data or personal data concerning convictions and violations of law does not result in the obligation to designate a DPO if it is not the main activity of the controller or the processor, which creates the need to process such data on a large scale or if a potentially obliged entity processes such data within the main activity but the scale cannot be recognised as large.

The reasons for the obligation to designate a DPO by a non-public authority, to a big extent, were edited with the use of insufficiently determined concepts[16] (e.g. a large scale of processing, regular and systematic monitoring) which raise serious doubts. A particular controller or processor, in order to establish whether they have the obligation resulting directly from the GDPR provisions, must interpret them, which may result in the interpretation different from that of the supervisory authority. Failure to designate a DPO against the obligation laid down in GDPR carries an administrative fine determined in Article 83 para. 4 GDPR. It should

[14] In accordance with the wording of the provision, the data include data revealing the racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership and genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

[15] In accordance with the provision, processing of personal data concerning convictions and offences or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorised by the Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority.

[16] The interpretation of the concepts is the subject matter of literature, see E. Bielak-Jomaa, [in:] *RODO ogólne rozporządzenie...*, pp. 778–783, and P. Litwiński, P. Barta, M. Kawecki, *Rozporządzenie UE w sprawie ochrony…*, pp. 560–566.

be added that in accordance with the rules of interpretation, the reasons for an obligation edited in a normative act should be subject to a narrowed interpretation.

As Article 37 para. 2 GDPR stipulates, a group of undertakings[17] may appoint a single data protection officer provided that a data protection officer is easily accessible from each establishment. The possibility of being easily accessible from each establishment as the condition for the designation of a single DPO laid down in para. 2 *in fine* seems to be practically irrelevant in the light of contemporary development of telecommunications and the Internet.

It is rightly raised in literature that if the GDPR provisions do not ban performing the DPO function, at the same time, for a few controllers or processors, "there will also be (…) a possibility of designating the same person to perform the function of a DPO by unrelated entities".[18] It should be added that there are no formal obstacles to employ the same person as a DPO by a public authority or body and an entrepreneur.

In accordance with the provision of Article 37 para. 4, the controller or processor or associations and other bodies representing categories of controllers or processors may or, where required by the Union or Member State law, shall designate a DPO. The provision is applicable only to non-public entities because all public authorities and bodies have the obligation pursuant to the GDPR provisions.

The same GDPR provision grants private entities the right to designate a DPO even if it is not their obligation. The right is general in nature and not limited by any circumstances. Thus, a decision on designating a DPO or not is at the controller's or the processor's discretion.[19] K. Witkowska emphasizes that in case the controller or the processor performs an activity that is subject to professional secrecy, designation of a DPO "will be a good solution for them and a means of ensuring more efficient and effective protection of data (…)".[20]

The provision of Article 37 para. 5 GDPR stipulates that a DPO must be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks. As it is emphasized in Recital 97 GDPR, the necessary level of expert knowledge should be determined in particular according to the data processing operations carried out and the protection required for the personal data processed by the controller or the processor. The solution is recognised as "clear tendency to create a professional nature of the DPO function".[21] As far as the ability to fulfil the tasks is concerned, it may include, inter alia, passing knowledge, conducting training or efficient communication.[22]

---

[17] According to the definition adopted in Article 4(19) GDPR, "group of undertakings" means a controlling undertaking and its controlled undertakings.

[18] P. Litwiński, P. Barta, M. Kawecki, *Rozporządzenie UE w sprawie ochrony*…, p. 568.

[19] D. Lubasz, *Europejska reforma ochrony danych osobowych – nowe obowiązki administratora w ogólnym rozporządzeniu o ochronie danych*, [in:] E. Bielak-Jomaa, D. Lubasz (ed.), *Polska i europejska reforma ochrony danych osobowych*, Warsaw 2016, p. 84.

[20] K. Witkowska, *Data protection officer, czyli inspektor ochrony danych w ogólnym rozporządzeniu o ochronie danych*, [in:] *Polska i europejska reforma...*, p. 242.

[21] M. Chodorowski, *Nowe prawa i obowiązki administratora bezpieczeństwa informacji (inspektora ochrony danych) w świetle najnowszych opinii wydanych przez Grupę Roboczą Art. 29*, [in:] M. Kawecki, T. Osiej (ed.), *Ogólne rozporządzenie o ochronie danych osobowych*, Warsaw 2017, p. 157.

[22] K. Syska, *Administrator bezpieczeństwa informacji*…, p. 77.

The GDPR provisions do not indicate the reasons for a DPO dismissal; "thus, it should be assumed that the issue is left for regulation in national laws".[23]

2. DATA PROTECTION OFFICER'S TASKS

The DPO's tasks are laid down in Article 39 GDPR in the form of a closed catalogue. It is rightly raised in literature that in accordance with the English wording of the Regulation, the catalogue is open in nature.[24] Thus, it is necessary to agree with the stance that the DPO's tasks enumerated in GDPR "are determined as a minimum not closing the way to all activities and actions aimed at protecting personal data".[25]

The first task laid down in Article 39 para. 1(a) GDPR is to inform and advise the controller, the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions. The performance of the task may consist in conducting lectures, workshops and training or development of informative materials.[26] However, materials developed under the aegis of the supervisory authority should constitute the basic source of information. This would be the basis for uniform practice of applying the provisions on the protection of personal data developed within this body's fulfilment of a task (resulting from Article 57 para. 1(d) GDPR), consisting in promoting the awareness of controllers and processors of their obligations under the Regulation. As far as advising controllers, processors and employees is concerned, the DPO's task is limited, in my opinion, to suggestions concerning the way of performing tasks within the scope that does not require the interpretation of law, because such issues should be the competence of the entity providing legal advice in the organisation.

Secondly, according to Article 39 para. 1(b) GDPR, the DPO's task is to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data.[27] Monitoring means observing or checking; thus, the activity is not connected with any powers that might be derived from a supervisory-control function (e.g. possibility of requesting explanations). A purpose-related interpretation makes it possible to assume that what is established in the course of monitoring should be passed to the controller with suggestions of the ways of eliminating revealed irregularities. However, the presented suggestions are not binding on the addressee.

---

[23] M. Piech, *„Deregulacyjna" nowelizacja i unijna reforma zasad ochrony danych osobowych z perspektywy administratora danych osobowych*, [in:] *Polska i europejska reforma*…, p. 47.

[24] See P. Litwiński, P. Barta, M. Kawecki, *Rozporządzenie UE w sprawie ochrony*…, p. 592; and E. Bielak-Jomaa, [in:] *RODO ogólne rozporządzenie*..., p. 808.

[25] A. Lewiński, *Administrator bezpieczeństwa informacji – zagadnienia konstrukcyjne*, [in:] *Polska i europejska reforma*..., p. 155.

[26] E. Bielak-Jomaa, [in:] *RODO ogólne rozporządzenie*..., p. 810.

[27] Monitoring includes the assignment of responsibilities, awareness-raising and training of staff involved in processing operations and the related audits.

The third DPO's task (Article 39 para. 1(c) GDPR) is to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35. The indicated task results from the obligation imposed on the controller based on Article 35 para. 1 GDPR to carry out an assessment, prior to data processing, of the impact of the envisaged processing operations on the protection of personal data, taking into account the nature, scope, context and purposes of the processing, where a type of processing, in particular using new technologies, is likely to result in a high risk to the rights and freedoms of natural persons.

Carrying out an assessment of the impact on the protection of personal data, the controller must consult a DPO, provided he has been designated, and the DPO's task is to present an opinion on the described situation. The legislator determines the DPO's task in Article 39 para. 1(c) GDPR as providing advice where requested as regards the data protection impact assessment and monitoring its performance pursuant to Article 35. In Article 35 para. 2, the controller's activity is called seeking advice of a DPO and in Article 39 para. 1(c) it is referred to as requesting, and a potential DPO's response as providing advice that, however, cannot be treated as binding. According to the content of Recital 77, the DPO is authorised to provide guidelines on the implementation of appropriate measures and on the demonstration of compliance by the controller or the processor, especially as regards the identification of the risk related to the processing, its assessment in terms of origin, nature, likelihood and severity, and the identification of best practices to mitigate the risk. However, "it is the organisation and not the DPO that is obliged to ensure compliance with the law on the protection of personal data (…)".[28]

The provision of Article 39 para. 2 GDPR stipulating that the DPO in the performance of his tasks has due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing, seems to be important only in relation to the fulfilment of the discussed task.

Fourthly, the DPO's task is to cooperate with the supervisory authority and to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter (Article 39 para. 1(d) and (e) GDPR). In accordance with Article 37 para. 7 GDPR, the controller or the processor must communicate the contact details to the supervisory authority. It is indicated in literature that the data include "the first name and surname and a correspondence address as well as an e-mail address or telephone number".[29] In Articles 13 and 14 GDPR, editing the responsibilities of the controller and the processor towards the data subject, the legislator obliges them to provide information about their identity and contact details. In the provision of Article 37 para. 7 GDPR, however, it is not indicated that the DPO's identity is an obligatory element of the information provided by the controller or the processor to the supervisory authority. Is it possible

---

[28] M. Chodorowski, *Nowe prawa i obowiązki…*, p. 151. Similarly, E. Bielak-Jomaa, [in:] *RODO ogólne rozporządzenie...*, p. 810.

[29] K. Syska, *Administrator bezpieczeństwa informacji…*, p. 77.

that the European legislator's will was to guarantee the DPO's anonymity in his cooperation with the supervisory authority?

The GDPR provisions "do not precisely define the supervisory authority's competences towards a DPO".[30] As E. Bielak-Jomaa emphasizes, "the obligation to cooperate with the supervisory authority specified in a general way certainly goes beyond consultation-advisory activities".[31] The concept of cooperation with the supervisory authority should be interpreted as authorisation and obligation to joint work, supporting the supervisory authority by the DPO and the DPO by the supervisory authority, which pursuant to the provision of Article 57 para. 3 GDPR must be done free of charge. The fulfilment of a contact point role means the indication of the DPO as an entity being a potential source of information for the supervisory authority in issues concerning data processing.[32] It is emphasized in the doctrine that it may concern "allowing the supervisory authority access to documents and information in order to fulfil tasks referred to in Article 57, as well as to exercise the investigative powers, corrective powers, authorisation and advisory powers in accordance with Article 58".[33] However, this approach raises doubts because the provisions of Articles 57 and 58 GDPR do not indicate that the legislator envisaged whatever role of the DPO in this area. His participation, e.g. in conducted proceedings, would have to be legally determined first. On the other hand, it is not the DPO but the controller, the processor and, if appropriate, their representative who are the addressees of the obligation to provide the supervisory authority with all the information required for the performance of its tasks, which is laid down in Article 58 para. 1(a) GDPR.

The fifth task indirectly results from Article 38 para. 4 GDPR. In accordance with it, data subjects can contact the DPO with regard to all issues related to processing of their data and to exercise their rights under this Regulation. In accordance with Articles 13 and 14 GDPR, regardless of the method of obtaining data by the controller or the processor, they should provide data subjects with the DPO's contact data. Editing the scope of this obligation, the legislator skipped the DPO's identity, which means that the DPO remains anonymous to a data subject, which is hard to approve of. "In some situations, the knowledge of the DPO's identity may prove to be desirable from the point of view of creating an appropriate relation between the data subject and the DPO."[34]

In the situation indicated above, it should be assumed that the DPO's task, and precisely speaking obligation, is to provide entities with information concerning cases connected with the processing of their personal data and the exercise of rights

---

[30] *Ibid*.

[31] E. Bielak-Jomaa, *Wyzwania przed administratorami bezpieczeństwa informacji (inspektorami ochrony danych) w związku z wejściem w życie ogólnego rozporządzenia o ochronie danych*, Monitor Prawniczy No. 20 (supplement), 2016, p. 5.

[32] M. Chodorowski, *Nowe prawa i obowiązki…*, p. 154.

[33] E. Bielak-Jomaa, [in:] *RODO ogólne rozporządzenie*..., p. 813.

[34] G. Sibiga, K. Syska, *Działania organizacyjne i informacyjne związane z wyznaczeniem i wykonywaniem funkcji inspektora ochrony danych*, Monitor Prawniczy No. 20 (supplement), 2017, p. 26.

they have under GDPR. "Data subjects may ask questions directly to the DPO and expect the DPO's answers."[35] E. Bielak-Jomaa states that, since the controller is the addressee of the obligation (e.g. resulting from Article 15 GDPR), "the role of the DPO formally consists in preparing draft answers to data subjects".[36] Taking into account the controller's liability for failure to comply with the GDPR provisions, it is necessary to ask a question whether the controller's stance on the issue should not be subject to assessment by a person providing legal services for the organisation.

As far as contacting the DPO with regard to exercising a data subject's rights is concerned, the procedure raises doubts because, e.g. the provisions of Article 15 (right of access), Article 16 (right of rectification), Article 17 (right to erasure), and Article 18 (right to restriction of processing) indicate that their enforcement takes place in the form of a complaint filed to the controller. One can have doubts whether filing a request to the DPO bears legal effects if a data subject knows the controller's identity and his contact data.

3. DATA PROTECTION OFFICER' STATUS

The designation of a DPO based on professional qualities, in particular expert knowledge of data protection law and practices and the ability to fulfil the tasks, as well as the status of this body laid down in Article 38 GDPR are to guarantee efficient fulfilment of tasks by the DPO.

First of all, it should be indicated that the legislator obliges the controller and the processor to ensure that the DPO is involved, properly and in a timely manner, in all issues that relate to protection of personal data and guaranteeing access to personal data and data processing operations. The fulfilment of tasks by the DPO requires maintaining up-to-date and complete knowledge about data processing and protection in the organisation. However, the very general provision ensuring the DPO's right of access to personal data raises serious doubts because it can suggest that it should be permanent and unlimited. The issue needs more precise determination because access to personal data may be necessary in order to fulfil only some tasks and if the data constitute information that is protected by the law based on other provisions, the general regulation of GDPR cannot ignore limitations to access to such information, which results from national law.

"If a DPO is to verify the compliance with rules and procedures in the field of data processing and safeguard the rights and freedoms of individuals, the DPO must be guaranteed independence."[37] The collector and the processor should ensure that the DPO does not receive any instructions regarding the exercise of those tasks. The DPO directly reports to the highest management level of the controller or the processor. This means that the legislator strives to ensure the DPO's independent position, which is directly expressed in Recital 97 GDPR. In accordance with it, data

---

35 M. Chodorowski, *Nowe prawa i obowiązki…*, p. 155.
36 E. Bielak-Jomaa, [in:] *RODO ogólne rozporządzenie...*, p. 805.
37 E. Bielak-Jomaa, *Wyzwania przed administratorami...*, p. 6.

protection officers, whether or not they are employees of the controller, should be in a position to perform their duties and tasks in an independent manner.

The instructions referred to are to concern the performance of tasks, i.e. the way of their fulfilment. "In the field of the performance of tasks, DPOs have absolute discretion."[38] This is the DPO who has expert knowledge and skills to perform tasks on his own, within the limits of the law, and decide on the implementation procedures.

However, the limitation introduced by the legislator is not applicable to the possibility of delegating tasks. Of course, the highest management level, to which the DPO reports, is entitled to delegate tasks. The controller or the processor can do this when they are authorised by the highest management. The limitation is not applicable when the controller plays the role of the highest management at the same time. In my opinion, the provision excluding the possibility of giving instructions to the DPO should not be overestimated because the DPO does not have decision-taking powers.

The instructions laid down in the discussed provision addressed to the controller and the processor and with regard to providing the DPO with resources necessary to carry out those tasks and to maintain his expert knowledge are unquestionable.

A conclusion made in Article 38 para. 3 GDPR that the DPO shall not be dismissed or penalised by the controller or the processor for performing his tasks cannot be interpreted as a kind of immunity granted to the DPO. Firstly, the limitation to the possibility of dismissing or penalising is to be applicable only to the performance of his tasks. Thus, penalisation or dismissal is possible if the DPO does not fulfil the tasks. Secondly, the issue of limitation concerns the controller or the processor and does not cover potential rights of an entity that the EU legislator refers to as the highest management level. If the head of a unit is also the controller, they may undertake steps against the DPO within the performance of a managerial function. Thirdly, the provision cannot be treated as a mechanism ensuring a lack of criminal, disciplinary or civil liability. It is emphasized in literature that the protection of the DPO against penalisation is only applicable to "the manner and content of his activities connected with his performance of duties provided that they are in compliance with GDPR".[39]

Article 38 para. 5 GDPR stipulates that the DPO shall be bound by secrecy or confidentiality concerning the performance of his tasks, in accordance with Union or Member State law. E. Bielak-Jomaa emphasizes that "it is not clear whether the discussed provision constitutes the DPO's secrecy on its own",[40] and eventually draws a conclusion that the provision "directly determines subject- and object-related scope of the DPO's secrecy".[41] In my opinion, such a conclusion is groundless because there is no content in the DPO's activity that would require legal protection due to the performed function. However, such protection is necessary with regard to

---

38 E. Bielak-Jomaa, [in:] *RODO ogólne rozporządzenie...*, p. 802.
39 M. Chodorowski, *Nowe prawa i obowiązki...*, p. 148.
40 E. Bielak-Jomaa, [in:] *RODO ogólne rozporządzenie...*, p. 805.
41 *Ibid*., p. 806.

the information provided to the DPO. The Union legislator refers to other EU or Member State regulations if such norms lay down the obligation to keep information available to the DPO secret. Thus, the obligation does not constitute a separate, new value. The ban on providing information about the performance of tasks to unauthorised entities is in force if it is laid down in other legal acts that may determine the status of information at the DPO's disposal. In the described situation, the opinion that the DPO shall "be made exempt from secrecy if the controller or the processor decides so"[42] is groundless. The procedure of making the DPO exempt from secrecy in case of information protected by the law should be each time analysed individually, depending on its type in the context of the provisions constituting it.

The DPO can also carry out other tasks and duties. It is emphasized in literature that "due to the workload imposed on the DPO as a result of the new regulations, it seems really difficult to perform the function by an employee who has other duties connected with another post".[43] The controller or the processor must ensure that such tasks and duties do not cause a conflict of interests. The entities may satisfy the employer's demands only in a situation when they are identified with the highest management level the DPO directly reports to. Avoiding a conflict of interests should, in my opinion, mean that the DPO is not delegated tasks requiring the processing of personal data in circumstances not related to the performance of the DPO's function and such activities that would be directly connected with ensuring the security of data. Therefore, I do not share the opinion presented in literature suggesting that the controller may delegate a task of "maintaining a record of personal data processing activities" (Article 30 GDPR) to a DPO.[44]

4. CONCLUSIONS

The regulation of the DPO's position and competences laid down in Articles 37 to 39 GDPR is very general and indefinite in nature.

The DPO's status is insufficiently specified. There is not a requirement of legal education for the post and the performance of the tasks requires the skill of applying the provisions of law. The DPO must train entities indicated in GDPR but these are also the supervisory authority's tasks. The DPO monitors personal data processing in an organisation but his powers in this area are not precisely determined. If the controller or the processor are the addressees of comments on the irregularities revealed in the course of monitoring, although they are responsible for data processing in compliance with the provisions of law, they are not obliged to take into consideration the comments made by the DPO, who, on the other hand, is not authorised to inform the supervisory authority about the revealed irregularities. The GDPR provisions only stipulate, as

---

[42] P. Litwiński, P. Barta, M. Kawecki, *Rozporządzenie UE w sprawie ochrony*…, pp. 586–587.

[43] M. Zadrożny, *Inspektor ochrony danych (IOD)*…

[44] P. Litwiński, P. Barta, M. Kawecki, *Rozporządzenie UE w sprawie ochrony*…, p. 593. Also see: E. Bielak-Jomaa, [in:] *RODO ogólne rozporządzenie...*, p. 809; K. Syska, *Administrator bezpieczeństwa informacji*…, p. 78; P. Fajgielski, *Rejestry czynności przetwarzania danych osobowych*, Monitor Prawniczy No. 20 (supplement), 2017, p. 37.

a rule, the cooperation between the DPO and the supervisory authority but do not lay down its forms. The competences of the DPO as a contact point for a data subject are not precisely determined. Doubts concern, in particular, a situation when a data subject, exercising his rights, files requests to a DPO, while the GDPR provisions stipulate that the controller or, if applicable, the processor shall be the addressee.

The Article 29 Working Party for the Protection of Individuals with regard to the Processing of Personal Data developed Guidelines concerning data protection officers adopted on 13 December 2016, recently amended and adopted on 5 April 2017.[45] The interpretation provided in the Guidelines is not discussed in the present article. The Article 29 Working Party ceased to exist on the date of GDPR entry into force, i.e. 25 May 2018. In accordance with Recital 139 GDPR, the European Data Protection Board (EDPB) substitutes for the Article 29 Working Party for the Protection of Individuals with regard to the Processing of Personal Data established based on Directive 95/46/EC. In accordance with Article 70 para. 1(e) GDPR, the EDPB must ensure the consistent application of this Regulation, and on its own initiative or at the request of one of its members or the Commission examines any question covering the application of this Regulation, issues guidelines and recommendations, and determines best practices in order to encourage consistent application of this Regulation. There is an opinion expressed in the doctrine that "a strong position of the EDPB shall ensure uniform application and interpretation of the provisions by the EU bodies for the protection of personal data, which will have a positive impact on strengthening the role of this body at the stage of coordinating stands of data protection bodies and will ensure more consistent application at the national level".[46] However, the potential guidelines, recommendations and best practices developed by the EDPB will not be binding in the light of Article 288 Treaty on the Functioning of the European Union.[47] Thus, acts issued by the EDPB in the future, regardless of the level of readiness to apply them by the bodies operating on the basis of GDPR, should not blur the scientific reflection on the content of the GDPR provisions concerning the DPO.

In the light of the general wording of the GDPR provisions concerning the DPO, there is an opinion in the doctrine according to which "in order to determine the rules of the officer's functioning and competences more precisely, it is necessary to develop and implement an internal organisational act, e.g. rules and regulations or a set of principles concerning the performance of the DPO's function".[48] I do not share the opinion because a different interpretation might be adopted in such rules

---

[45] 16/EN, WP 243, Polish version (unofficial translation): www.giodo.gov.pl/pl/1520259/10066, [accessed on 27/02/2018]. The Working Party for the Protection of Individuals with regard to the Processing of Personal Data is an advisory body established based on Article 29 Directive 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 those data, OJ L 281/31 of 23.11.1995.

[46] G. Sibiga, *Wdrażanie ogólnego rozporządzenia o ochronie danych. Aktualne problemy prawnej ochrony danych osobowych*, Monitor Polski No. 20, 2017, p. 13.

[47] OJ of 2016, C 202/01.

[48] G. Sibiga, K. Syska, *Działania organizacyjne i informacyjne…*, p. 23.

and regulations, which seems natural, and thus, the DPO's status and the rules of performing the function would be different in particular organisations.

According to another stand, only within the limits determined in GDPR, "the national provisions may regulate the matters covered in the Regulation".[49] The content of this act, however, lacks provisions that might constitute the obligation or authorisation of national legislators to refer to GDPR.

It is directly emphasized in literature that the regulation of the DPO's status and tasks in a general manner may hamper their real implementation in practice.[50]

BIBLIOGRAPHY

Bielak-Jomaa E., *Wyzwania przed administratorami bezpieczeństwa informacji (inspektorami ochrony danych) w związku z wejściem w życie ogólnego rozporządzenia o ochronie danych*, Monitor Prawniczy No. 20 (supplement), 2016.

Bielak-Jomaa E., Lubasz D. (ed.), *RODO ogólne rozporządzenie o ochronie danych. Komentarz*, Warsaw 2018.

Chodorowski M., *Nowe prawa i obowiązki administratora bezpieczeństwa informacji (inspektora ochrony danych) w świetle najnowszych opinii wydanych przez Grupę Roboczą Art. 29*, [in:] M. Kawecki, T. Osiej (ed.), *Ogólne rozporządzenie o ochronie danych osobowych*, Warsaw 2017.

Fajgielski P., *Rejestry czynności przetwarzania danych osobowych*, Monitor Prawniczy No. 20 (supplement), 2017.

Kalinowska N., Litwiński P., *Ocena skutków dla ochrony danych i uprzednie konsultacje – nowe obowiązki podmiotów przetwarzających dane osobowe*, Monitor Prawniczy No. 13, 2017.

Lewiński A., *Administrator bezpieczeństwa informacji – zagadnienia konstrukcyjne*, [in:] E. Bielak-Jomaa, D. Lubasz (ed.), *Polska i europejska reforma ochrony danych osobowych*, Warsaw 2016.

Litwiński P. (ed.), Barta P., Kawecki M., *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz,* Warsaw 2018.

Lubasz D., *Europejska reforma ochrony danych osobowych – nowe obowiązki administratora w ogólnym rozporządzeniu o ochronie danych*, [in:] E. Bielak-Jomaa, D. Lubasz (ed.), *Polska i europejska reforma ochrony danych osobowych*, Warsaw 2016.

Piech M., *„Deregulacyjna" nowelizacja i unijna reforma zasad ochrony danych osobowych z perspektywy administratora danych osobowych*, [in:] E. Bielak-Jomaa, D. Lubasz (ed.), *Polska i europejska reforma ochrony danych osobowych*, Warsaw 2016.

Sibiga G., *Dopuszczalny zakres polskich przepisów o ochronie danych osobowych po rozpoczęciu obowiązywania ogólnego rozporządzenia o ochronie danych – wybrane zagadnienia,* Monitor Prawniczy No. 20 (supplement), 2016.

Sibiga G., *Wdrażanie ogólnego rozporządzenia o ochronie danych. Aktualne problemy prawnej ochrony danych osobowych*, Monitor Polski No. 20 (supplement) 2017.

Sibiga G., Syska K., *Działania organizacyjne i informacyjne związane z wyznaczeniem i wykonywaniem funkcji inspektora ochrony danych*, Monitor Prawniczy No. 20 (supplement), 2017.

---

[49] G. Sibiga, *Dopuszczalny zakres polskich przepisów o ochronie danych osobowych po rozpoczęciu obowiązywania ogólnego rozporządzenia o ochronie danych – wybrane zagadnienia*, Monitor Prawniczy No. 20 (supplement), 2016, p. 18.

[50] M. Chodorowski, *Nowe prawa i obowiązki…*, p. 157.

Syska K., *Administrator bezpieczeństwa informacji a inspektor ochrony danych – porównanie przesłanek powołania, statusu i zadań*, Monitor Prawniczy No. 20 (supplement), 2016.
Szałowski R., *Administrator bezpieczeństwa informacji*, Ius Novum No. 4, 2016.
Witkowska K., *Data protection officer, czyli inspektor ochrony danych w ogólnym rozporządzeniu o ochronie danych*, [in:] E. Bielak-Jomaa, D. Lubasz (ed.), *Polska i europejska reforma ochrony danych osobowych*, Warsaw 2016.
Zadrożny M., *Inspektor ochrony danych (IOD) jako następca ABI*, [in:] A. Dmochowska, M. Zadrożny (ed.), *Unijna reforma ochrony danych osobowych. Analiza zmian,* Warsaw 2016, Legalis.

Legal regulations

Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych [Act of 29 August 1997 on the protection of personal data], Uniform text, Journal of Laws [Dz.U.] of 2016, item 922.
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 281/31 of 23.11.1995.
Regulation (UE) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119 of 4.5.2016.
Guidelines of the Article 29 Working Party for the Protection of Individuals with regard to the Processing of Personal Data concerning DPOs adopted on 13 December 2016, recently amended and adopted on 5 April 2017, 16/EN, WP 243 – Polish unofficial translation: www.giodo.gov.pl/pl/1520259/10066.

DATA PROTECTION OFFICER IN THE LIGHT OF THE PROVISIONS OF THE GENERAL DATA PROTECTION REGULATION (GDPR)

Summary

The article aims to present, analyse and assess the legal grounds for the designation, tasks and status of the data protection officer in the light of the provisions of Articles 37 to 39 Regulation 2016/679 (EU) 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).
The obligation to designate a DPO is imposed on public authorities and bodies with no limitations. On the other hand, in case of non-public entities, it has been considerably narrowed. The DPO's status is not sufficiently determined. There is no requirement for the DPO to have professional legal qualifications and he has been assigned tasks requiring the knowledge on the application of law. The DPO must monitor personal data processing in an organisation but his powers with regard to this area have not been sufficiently determined. If the controller or the processor is the addressee of comments on irregularities revealed in the course of monitoring, although they are responsible for data processing in compliance with the law, they are not obliged to take into consideration the DPO's comments, and the DPO is not authorised to inform the supervisory authority about the revealed irregularities. The GDPR provisions only stipulate, as a rule, the cooperation between the DPO and the

supervisory authority but do not lay down its form. The DPO's competences as a contact point for a data subject have not been precisely determined, either. Doubts are raised especially in connection with a situation when data subjects, exercising their rights, file their claims to the DPO. The GDPR provisions indicate that they should be addressed to the controller or, if applicable, the processor. The general regulation of the DPO's status and tasks may hamper their implementation in practice.

Keywords: personal data, personal data protection, data protection officer, GDPR

INSPEKTOR OCHRONY DANYCH W ŚWIETLE ROZPORZĄDZENIA O OCHRONIE DANYCH (RODO)

Streszczenie

Przedmiotem artykułu jest prezentacja, analiza i ocena podstaw prawnych wyznaczania, zadań oraz statusu inspektora ochrony danych w świetle przepisów art. 37–39 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).
Obowiązek powołania IOD ciąży bez ograniczeń na organach i podmiotach publicznych, natomiast w odniesieniu do podmiotów niepublicznych został znacznie zawężony. Status IOD jest niedookreślony. Nie wprowadzono warunku spełnienia przez IOD wymogu posiadania wykształcenia prawniczego, a powierzono mu zadania wymagające umiejętności stosowania przepisów prawa. IOD monitoruje przetwarzanie danych osobowych w organizacji, ale jego uprawnienia w tej materii nie zostały dookreślone. Jeżeli adresatem uwag o nieprawidłowościach ujawnionych w toku monitorowania będzie administrator danych lub podmiot przetwarzający, to chociaż są oni odpowiedzialni za przetwarzanie danych zgodnie z przepisami prawa, nie są zobowiązani do uwzględniania uwag IOD, który z kolei nie jest upoważniony do informowania organu nadzorczego o stwierdzonych nieprawidłowościach. Przepisy RODO przesądzają jedynie, co do zasady, o współpracy IOD z organem nadzorczym, lecz nie konkretyzują jej form. Nie zostały precyzyjnie określone kompetencje IOD jako punktu kontaktowego dla podmiotu danych. W szczególności wątpliwości dotyczą sytuacji, gdy podmiot ten, korzystając z przyznanych mu uprawnień, przedstawia żądania pod adresem IOD, w sytuacji gdy przepisy RODO wskazują, że ich adresatem ma być administrator danych bądź, gdy ma to zastosowanie, podmiot przetwarzający. Ogólnikowa regulacja statusu oraz zadań IOD może w praktyce utrudniać ich realizację.

Słowa kluczowe: dane osobowe, ochrona danych osobowych, inspektor ochrony danych, RODO

Cytuj jako:

Szałowski R., *Data protection officer in the light of the provisions of the General Data Protection Regulation (GDPR) [Inspektor ochrony danych w świetle rozporządzenia o ochronie danych (RODO)]*, „Ius Novum" 2018 (12) nr 4, s. 115–130. DOI:10.26399/iusnovum.v12.4.2018.38/r.szalowski

Cite as:

Szałowski, R. (2018) 'Data protection officer in the light of the provisions of the General Data Protection Regulation (GDPR)'. *Ius Novum* (Vol. 12) 4, 115–130. DOI:10.26399/iusnovum.v12.4.2018.38/r.szalowski