Stowarzyszenie
Administratorów
Bezpieczeństwa
Informacji

Warsaw, 26 January 2017

Comments of the Association of the Information Security Administrators (Association) to the document adopted on 13 December 2016 by the Working Party set up under Article 29 of Directive 95/46/EC (WP29). 'Guidelines on Data Protection Officers' (WP243)

The Association of Information Security Administrators (Association) recognizes the importance of the guidelines on Data Protection Officers presented by the Working Party set up under Article 29 of Directive 95/46/EC, for they constitute an important element of ensuring compliance with the data protection rules in organizational units and of implementing the General Data Protection Regulation itself (GDPR). The guidelines will certainly add to the more effective application of the GDPR in regard of the data protection officer (DPO) and they will promote appointing DPOs, determining their position in an organization and performing tasks in a correct manner.

At the same time, the Association notes that the guidelines require supplementing with issues concerning the DPO that have not been addressed, or that have been under-represented, and that some opinions included in the guidelines require explaining. Comments in this area can be found below.

I. Designation of a DPO by public authorities or bodies

Some substantive doubts are raised by distinguishing two different groups of entities in point 2.1.1 of the guidelines:

a) 'public authorities or bodies' carrying out public tasks and exercising public authority, that are obliged to appoint a DPO,
b) other authorities and bodies carrying out public tasks and exercising public authority, that are not obliged to appoint a DPO, and for which appointing a DPO is only recommended.

According to the Association, differentiating the second category is not based on the GDPR and its interpretation is unclear also under the national laws. It should be pointed out that the obligation to appoint a DPO has been imposed both on public authorities and public bodies. When the GDPR intends to limit a provision only to public authorities, it does so explicitly, as in Article 4(9) of the GDPR (recital 31 of the preamble to the GDPR provides for the explanation of what some examples of public authorities are). Public bodies constitute a category separate from public authorities, and these are conditions of 'exercising public authority', 'carrying out a public task' and being governed by 'public law' that determines what entities it covers. The answer whether the enumerated conditions are met depends on the national regulations and specific regulations of the European Union. If – on the grounds of these regulations – the conditions are deemed to have been met then there is a public body within the meaning of Article 37(1)(a) of the GDPR that is obliged to appoint a DPO. There is no basis, however, to distinguish a further category of entities which – in spite of carrying out these tasks and being governed by the public law – are not obliged to designate a DPO.

II. Designating a single DPO for a group of public bodies

1. The guidelines do not specify which entity (or entities) from a group of undertakings may designate a single DPO for the entire group. There are at least two options to be considered: a DPO is designated by the parent company or a DPO is designated by every undertaking in the group. According to the Association, even if the first position is taken, each undertaking in which the DPO is going to perform the function needs to confirm this fact. It is only after such confirmation is given that there is no doubt that the DPO may carry out the tasks in the undertaking providing the confirmation. This also increases the transparency of performing the function.

2. A similar problem may arise in a group of public authorities or bodies, that is whether each of them needs to designate the DPO, or only the authority (body) which – as a result of the management, supervision or control dependencies – holds a parent position towards the other authorities (bodies). According to the Association, this is determined by the national law which specifies the relations among public authorities (bodies). However, even when there is a strict hierarchy in relations among the authorities (e.g. an authority guides works of another authority by virtue of the law), the opinion expressed in point 1) remains valid, that is each authority in which the DPO is going to perform the function needs to confirm the fact. The reasons in support of the opinion and specified in point 1) also remain valid.

3. In case of public authorities or bodies, it has not been explained how to understand the phrase 'a several authorities or bodies' in the context of the function being performed by a single DPO, which may result in attempts to provide a maximum number of authorities or bodies that may designate a single DPO (e.g. no more than 9). According to the Association, the maximum number of public authorities or bodies should not be predetermined. It is, however, important that – taking account of their organizational structure and size – the number should be small enough to enable the DPO to effectively perform his or her tasks. In specific circumstances this condition may be fulfilled also when a single DPO is designated for more than 9 authorities (bodies).

III. Setting up a DPO team

Although it is point 3.2 ('Necessary resources') of section 3 'Position of the DPO', and not section 2 ('Designation of a DPO') that mentions the aspect of a DPO team, developing this aspect is fundamental for the designation of the DPO, as well as his/her position. What raises doubts is whether all persons in the team are going to perform the function of a DPO, which – on the one hand – requires that they need to fulfill the condition of professional qualities, and on the other hand that they should benefit from the guarantees provided for the function (acting in an independent manner, no dismissal or penalties, absence of conflict of interests). The doubts are strengthened by the fact that the guidelines offer a different approach towards an 'internal DPO' and an 'external DPO' (from outside the company). In case of an 'internal DPO' the guidelines refer to a DPO team, that is the DPO and his/her staff (which means that there is a single DPO, and the other persons are only his/her staff), and in case of an 'external DPO', a team of individuals may carry out the tasks of a DPO and one of them becomes merely a lead contact for the client.

According to the Association, whenever it is necessary for the effective protection of personal data, in case of big entities with an expanded organizational structure, there should be a possibility to appoint a team of more than one person to perform the function of a DPO. Each member of the team should be protected by the guarantees provided for the DPO under the GDPR (acting in an independent manner, no dismissal or penalties, absence of conflict of interests). However, no interpretation of the GDPR provisions should differentiate between the legal position of an internal DPO and the external one. In addition, whenever the function is performed by a single DPO, it should be recommended that the data controller indicates a deputy for the DPO in his/her absence resulting from a holiday or sickness. The deputy needs to meet the condition of professional qualities and enjoy guarantees provided for a DPO.

IV. Professional qualities of a DPO

Under Article 37(5) of the GDPR, professional qualities cover the expert knowledge and the ability to fulfill the tasks. Meanwhile, the guidelines do not explain the conditions regarding the abilities. According to the Association, what especially needs to be taken into account in this regard is the ability to form relations with third parties, that is with data subjects who refer to the DPO when exercising their rights and individuals within the organization for whom the DPO runs information campaigns. When it comes to the expert knowledge, it is worth emphasizing that it should enable identifying threats and carrying out risk assessments related to the personal data processing activities.

V. The autonomy of a DPO

Point 3.3 of the guidelines explains the guarantees for the autonomy of a DPO under the GDPR. Under Article 38(3) of the GDPR a controller and a processor ensure that the DPO does not receive any instructions regarding the exercise of his or her tasks. According to the Association, as this is the main provision ensuring the independence of the DPO, the guidelines need supplementing with regard to its interpretation.

In accordance with the standards on other professions and functions, acting in an independent manner includes independence of mind and independence in appearance. Consequently, the ban on giving instructions should be understood as a ban on each and every interference with the independence of mind and independence in appearance.

VI. Tasks of the DPO

Section 4 (Tasks) requires the most extensive comments, as the explanations omit three out of five tasks specified in Article 39(1) of the GDPR, namely:

- informing and advising of obligations pursuant to the regulation and other data protection provisions,
- cooperating with the supervisory authority,

- acting as the contact point for the supervisory authority on issues relating to processing, including the prior consultation and to consult, where appropriate, with regard to any other matter.

The Association suggests supplementing the guidelines in this area, for the performance of tasks by a DPO has a direct influence on the standard of personal data protection, and the general provisions of the GDPR do not specify the manner and mode of carrying out the tasks by the DPO, including his/her forms of action. In case of Poland it constitutes a far-reaching change as compared to the currently applicable personal data protection regulations which – not only in the act on the protection of personal data but also in the executive provisions to the act by the Minister of Digital Affairs – specify the manner and mode of carrying out the tasks by an administrator of information security.

VII. The task to monitor compliance with the GDPR

Point 4.1 provides explanation on the task of monitoring compliance with the GDPR. However, the guidelines do not provide sufficient explanation on what actions a DPO may take in case a breach of the GDPR is found or when there is a need to raise the level of personal data protection. The guidelines indicate that a DPO may 'inform, advise and issue recommendations'. However, in case of informing and advising, it is a repetition of competences specified in Article 39(1)(a) of the GDPR, whereas the recommendation regarding issuing recommendations does not specify the details of this action.

According to the Association, there is a need to specify what actions a DPO may take if in the process of monitoring he or she identifies the need to raise the level of data protection, or finds a breach of personal data protection rules. The actions taken by the DPO may consist in identifying the area in need of improvement and defining actions that he/she believes will enable ensuring the proper state, together with drawing a potential schedule for the actions. In case of a data protection breach, actions to be taken by a DPO could be compared with the data controller's obligations to notify the breach to the supervisory authority (Article 33 of the GDPR) or communicating it to the data subject (Article 34 of the GDPR). A DPO could especially decide whether there was a breach, whether the obligation arises, or what corrective measures should be applied.

VIII. Tasks of a DPO with relation to binding corporate rules

The guidelines also make no reference to the task regarding binding corporate rules that is set out in Article 47(2)(h) of the GDPR (monitoring compliance of the binding corporate rules within the group of undertakings, or group of enterprises engaged in a joint economic activity, as well as monitoring training and complaint-handling). It needs to be emphasized that, unlike in Article 39(1)(b) of the GDPR, monitoring refers not only to monitoring compliance with certain rules, but also to monitoring trainings and handling complaints. Therefore, it is well justified to provide explanation what should be the tasks of monitoring and how they should be carried out with regard to binding corporate rules, as well as to provide advice on how they link with the task of monitoring as specified in Article 39(1)(b) of the GDPR.

IX. Tasks of a DPO connected with the supervisory authority

The guidelines make no reference to the relation between a DPO and the supervisory authority. Article 39(1) of the GDPR specifies two tasks connected to these relations (letters (d) and (e)) and what needs to be determined first is the difference between them. According to the Association, using the word „cooperate" means communication in both directions, meaning also that each of the parties may benefit from the cooperation. It is worth referring the task to cooperate not only to general activities of the supervisory authority, but also to specific cases handled by the supervisory authority. Activities of the supervisory authority should not be limited to presenting its opinions, they should also be of interactive nature (forum for the exchange of views, forms enabling asking a question by a DPO, direct consultations). As for the role of a contact point, it should not result in the DPO being in a conflict of interests with regard to the duty of loyalty towards the data controller (data processor), or in being obliged to disclose secrets of the data controller (processor). In this respect we fully agree with the arguments raised in the note („Results of the discussion") from the Fablab workshop 'GDPR/from concepts to operational toolbox, DIY' that took place in Brussels on 26 July 2016.

X. Tasks of a contact point for data subjects

In many legal systems including the Polish law, it is a novelty to provide data subjects with the possibility to contact a DPO with regard to all issues related to processing of their personal data and to the exercise of their rights under the GDPR. It is therefore all the more important to explain what

specific duties are imposed on a DPO with regard to this new solution and in what way the duties should be carried out by the DPO. According to the Association, the approach based on internal procedures specifying the scope of a DPO's activities and his/her cooperation with other parties and business units may be of importance. The essential elements that need to be taken into consideration in the procedure are as follows: the need for a prior verification of cases addressed to the DPO (whether they are cases concerning personal data protection), defining the role of a DPO after receiving the case (whether he/she is only a contact point or participates actively in handling the case) and to whom in the organization and in what way he/she passes the case whenever he/she is not competent to deal with it on his/her own. It is also important that the DPO has proper support in performing his/her tasks, especially at times of high interest on the part of data subjects (request response time).

XI. The obligation of the officer to maintain secrecy or confidentiality concerning the performance of his or her tasks

The guidelines make no reference to the obligation of maintaining secrecy or confidentiality by the DPO. Such secrecy is provided for in Article 38(5) of the GDPR, however, according to the Association, this provision requires further explanation. The basic question is whether the GDPR provision creates an independent obligation of secrecy (confidentiality), or whether it is merely a reference to national regulations and EU law with respect to secrecy obligations defined in those legal systems. If the first approach is the proper one, further issues need explaining: the difference between the obligation to maintain secrecy and confidentiality, what information the obligation refers to (any information obtained by the DPO or only specific information), in what scope and towards whom the obligation of the DPO is waived. If, however, Article 38(5) of the GDPR is only a reference to other regulations (national and those of the European Union), then it creates no new obligation of secrecy (confidentiality) over those that are imposed on the DPO anyway in national regulations and the regulations of the European Union.

Management Board of the Association
of Information Security Administrators