THE CHAIRMAN OF PERSONAL DATA PROTECTION

Warsaw, 22

September

2020

DECISION

DEP. 405.31.331.2019

Based on Article. 104 § 1 of the Act of June 14, 1960 Code of Administrative Procedure (Journal of Laws of 2020, item 256, as amended), art. 7 sec. 1 and art. 60 sec. 1 lit. a) the Act on the Protection of Personal Data (Journal of Laws of 2019, item 1781 as amended) and art. 29 and art. 32 sec. 1 and 4 in connection with Art. 38 sec. 2,3 and 6, art. 39 sec. 1 and art. 57 sec. 1 lit. a) and art. 58 sec. 2 lit. b) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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 (general regulation on data protection) (Journal of Laws UE.L.2016.119.1 and Journal of Laws EU.L.2018.127.2), after conducting administrative proceedings regarding the breach by the Hospital in C. of the provisions of Art. 29, art. 32 sec. 1 and 4 in connection with Art. 38 sec. 2, 3 and 6 and article. 39 sec. 1 of Regulation 2016/679 to the extent to which the Hospital in C. obliged data protection inspectors to grant authorizations to personnel in the field of personal data processing, President of the Office for Personal Data Protection

I. By finding a violation by the Hospital in C. of the provision of Art. 38 sec. 6 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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 (general regulation on the protection of data) (Journal of Laws EU.L.2016.119.1 and Journal of Laws EU.L.2018.127.2) to the extent to which the Hospital in C. obliged the data protection officer in the period from [...] January 2019 by [...] July 2020 to authorize staff in the field of personal data processing, issue a reminder to the Hospital in C.

II. In the remaining scope, the proceedings are discontinued.

Justification

The President of the Personal Data Protection Office, acting pursuant to art. 58 sec. 1 lit. a) and e) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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 (General Data Protection Regulation) (Journal of Laws EU.L.2016.119.1 and Journal of Laws EU.L.2018.127.2), hereinafter: Regulation 2016/679, in a letter of [...] November 2019. asked the Hospital in C., hereinafter: the Hospital, to provide detailed information on the solutions adopted by the Hospital in terms of ensuring the data protection inspector, hereinafter referred to as: the DPO, with the effective performance of tasks. In response to the above-mentioned a letter that was received by the local office on [...] December 2019 (reference number: [...]), the Hospital informed, inter alia, that for the tasks of the DPO specified in point 6 of the procedure [...] in force from [...] May 2019, it is necessary, inter alia, "Empowering staff with regard to the processing of personal data".

The information in question was, in the opinion of the President of the Office for Personal Data Protection, a sufficient premise to initiate ex officio administrative proceedings regarding violation of the provisions on the protection of personal data by the Hospital within the meaning of Regulation 2016/679 on [...] June 2020.

In the course of the proceedings conducted in this case, the President of the Personal Data Protection Office, hereinafter referred to as: the President of the Personal Data Protection Office, determined as follows:

1. The hospital is the data controller within the meaning of Art. 4 sec. 7 of Regulation 2016/679.2. By letter of [...] December 2019 (presentation of the Personal Data Protection Office: [...] December 2020), the Hospital informed the President of the Personal Data Protection Office that the procedure [...] provides in point 6 the obligation of the DPO to "issue authorizations to the processing of personal data to employees". Similar provisions can be found in the procedures that have been in operation since [...] May 2019: [...] and [...], which in point 6 define "the right and responsibility of the DPO for granting authorizations to the hospital staff in the scope of personal data processing". Moreover, the Hospital emphasized that "the overriding aim of the procedures is to ensure an adequate level of protection of patients and employees in connection with the processing of their personal data", and for its implementation, "all DPOs have been authorized by the Administrator to authorize other persons to process personal data." 3. On [...] July 2020, the Hospital sent a letter to the President of the Personal Data Protection Office (presentation of the Personal Data Protection Office: [...] July 2020), containing information on: making changes "in three procedures ([...], [...], [...]), which included the original version of the provisions making the DPO responsible for granting the personnel authorizations in the field of personal data processing and indicating him as a person authorized by the Data Administrator, i.e. the Director of the Hospital to issue authorizations to process personal data "," revocation by Of the Director

of the Hospital, the authorization to grant authorizations to process personal data, which was granted to the DPO, and to issue authorizations to grant authorizations to process personal data to the Deputy Director for Administrative and Organizational Affairs and the Coordinator of the Personal Affairs Section ". To the above-mentioned the document is accompanied by evidence that the administrator has performed the actions described by him, in the form of the above-mentioned internal regulations.

In this factual state, the President of the Personal Data Protection Office considered the following.

Pursuant to Art. 4 sec. 7 of Regulation 2016/679, the administrator is a natural or legal person, public authority, unit or other entity that alone or jointly with others sets the purposes and methods of personal data processing; If the purposes and means of such processing are specified in Union law or the law of a Member State, the controller may also be designated under Union law or the law of a Member State, or specific criteria for his appointment may be laid down. The obligations of the administrator defined under Art. 32 sec. 1 above sources of law, it is necessary to ensure an appropriate level of security of personal data processing, i.e. such technical and organizational measures that, taking into account the state of technical knowledge, the cost of implementation and the nature, scope, context and purposes of processing as well as the risk of violating the rights or freedoms of natural persons with different probability and severity , provide a degree of security corresponding to this risk. For this purpose, the administrator is to undertake, pursuant to Art. 29 and art. 32 sec. 4 of Regulation 2016/679, measures to ensure that any natural person, acting under his authority, who has access to personal data, processes it only at his request, unless required by Union law or the law of a Member State. A literal interpretation of these provisions allows for the conclusion that it is possible for the administrator to authorize a subordinate employee to process personal data, including the delegation of the right to perform the administrator's obligations in the field of granting authorizations to process personal data on his behalf. The basic scope of the DPO's tasks, among which it is in vain to look for those related to granting the administrator's employees authorizations to process personal data, was specified by the EU legislator in Art. 39 sec. 1 of the Regulation 2016/679, however, pursuant to Art. 38 sec. 6 above of the Regulation, the DPO may also perform other tasks and obligations, as long as the controller or processor ensures that these tasks and obligations do not cause a conflict of interest.

However, it should be assumed that due to the specificity of the DPO's tasks focusing on advising and controlling the administrator's activities in terms of compliance of personal data processing operations with the provisions on the protection of personal data, the administrator should not grant the DPO the right to grant authorizations to process personal data on his

behalf, leaving the DPO in the procedure of issuing authorizations to process personal data to perform advisory and supervisory functions. The adoption of a different assumption, in which the DPO would be responsible for carrying out this procedure, and at the same time would monitor its compliance with the provisions on the protection of personal data, to which he is obliged by the regulation contained in Art. 39 sec. 1 lit. b) of Regulation 2016/679, would lead to a situation where the DPO would exercise supervision over his own activities, and thus to a conflict of interest, which is explicitly prohibited by Art. 38 sec. 6 of Regulation 2016/679. It should be emphasized that the DPO, who has a special status in the field of ensuring proper compliance with the provisions on the protection of personal data, must be guaranteed appropriate operating conditions for this purpose, i.e. those that will allow him to effectively, independently and correctly fulfill his obligations under legal provisions, as provided for in Art. 38 sec. 2 and 3 of Regulation 2016/679. In this context, the view that imposing on the DPO of obligations leading to the emergence of a conflict of interest should be considered correct, not only the possibility of effective fulfillment of tasks by him, the implementation of which is required by the provisions of Art. 39 of the Regulation 2016/679, but it violates the very foundations of the DPO, which is based primarily on the independence of its functioning.

Based on the collected evidence and bearing in mind the above comments, it should be stated that the Hospital incorrectly fulfilled the obligation specified in Art. 38 sec. 6 of Regulation 2016/679 by obliging the DPO to grant authorizations to personnel in the scope of personal data processing. It should be pointed out that the role of the DPO should focus on monitoring compliance with the provisions on the protection of personal data and internal policies and the proper performance of their obligations, as well as advising and raising awareness of these obligations. Therefore, the DPO should not be a person who performs the obligations set out in Art. 29 and art. 32 sec. 1 and 4 of Regulation 2016/679, the more that the addressee of the standards contained in the above-mentioned provisions is the data controller or the processor. As already indicated above, adopting a different view would result in a conflict of interest, the occurrence of which is prohibited in relation to IOD Art. 38 sec. 6 of Regulation 2016/679. Therefore, it is legitimate to believe that, for the purposes of ensuring the proper effectiveness of the personal data protection system adopted by the Hospital, the best solution is the one in which authorizations to process personal data are issued by a person performing a managerial function in the above-mentioned an entity, including e.g. the head of the HR department or managers of other organizational units, i.e. people who are able to most precisely define to whom and to what extent the authorization should be granted and update it on an ongoing basis.

In the opinion of the President of the Personal Data Protection Office (UODO), the above demand was met by the Hospital, as

indicated by the content of the letter sent to the local Office on [...] July 2020, in which the administrator informed both about making changes "in three procedures ([...], [...] , [...]), which included in the original version the provisions making the DPO responsible for granting the personnel authorizations in the field of personal data processing and indicating him as a person authorized by the Data Administrator, i.e. the Director of the Hospital to issue authorizations to process personal data ", as and about "the revocation by the Director of the Hospital of the authorization to grant authorizations to process personal data, which was granted to the DPO, and the issuing of authorizations to grant authorizations to process personal data to the Deputy Director for Administrative and Organizational Affairs and the Coordinator of the Personal Affairs Section". Therefore, it should be considered inappropriate for the Hospital to be restored by the President of the Personal Data Protection Office (UODO).

Nevertheless, the circumstances indicating that the Hospital inadequate fulfillment of the obligations set out in Art. 38 sec. 6 of Regulation 2016/679, by obliging the DPO in the period from [...] January 2019 to [...] July 2020 to grant authorizations to personnel in the field of personal data processing, should be considered proven (as evidenced by the content of on [...] January 2019, the procedures [...] and the following procedures: [...] and [...] operating from [...] May 2019, which provided for "the right and responsibility of the DPO for granting authorizations to hospital staff in the field of personal data processing "). It also leaves no doubt that in the aforementioned wide period of time, the DPO was forced to perform duties that resulted in a conflict of interest, and therefore could not properly perform his function, which in the context of the DPO's tasks provided for in Art. 39 of Regulation 2016/679 means that the gravity of this infringement should be considered significant. In view of the above, the President of the Personal Data Protection Office decided that, in the established circumstances of this case, the appropriate remedial measure would be to grant the Hospital, pursuant to Art. 58 sec. 2 lit. b) of Regulation 2016/679, a reminder for inappropriate in the period from [...] January 2019 to [...] July 2020, the implementation of the obligation specified in Art. 38 sec. 6 of Regulation 2016/679, by obliging the DPO to grant authorizations to personnel in the scope of personal data processing.

Improper performance by the Hospital of the obligation specified in Art. 38 sec. 6 of Regulation 2016/679, by obliging the DPO to grant authorizations to personnel in the scope of personal data processing, does not raise any doubts, and a subsequent change by the Hospital of personal data processing procedures may not cause the supervisory authority to withdraw from issuing a reminder, since the existence of a violation in the above-mentioned, more than annual period is indisputable. The evidence collected in the case in question also allows us to notice that the restoration of the compliance of the personal data

protection policies adopted by the Hospital with the applicable legal status was only the result of proceedings conducted by the President of the Personal Data Protection Office. Therefore, there is a reasonable suspicion that, had it not been for the above actions by the supervisory authority, the breach of law would have continued.

Nevertheless, the President of the Personal Data Protection Office, exercising his right under Art. 58 sec. 2 lit. b) of Regulation 2016/679, found that the purpose of the present proceedings, which is to restore lawfulness, can nevertheless be achieved by applying a less severe measure. In the opinion of the supervisory body, the reminder of the Hospital for incorrect performance of its obligations as a data controller within the meaning of Art. 4 sec. 7 of Regulation 2016/679, is the appropriate manifestation of the implementation of the principle of proportionality.

At the same time, the President of the Personal Data Protection Office, finding no grounds to believe that the provisions on the protection of personal data had been breached, discontinued the administrative proceedings in the remaining scope covered by this proceeding.

Bearing in mind the above, the President of the Personal Data Protection Office resolved as in the operative part of this decision.

2021-02-01