THE CHAIRMAN OF PERSONAL DATA PROTECTION

Warsaw, 19

January

2022

DECISION

DKE.561.14.2021

Based on Article. 104 § 1 of the Act of 14 June 1960 Code of Administrative Procedure (Journal of Laws of 2021, item 735, as amended) in connection with Art. 7 and art. 60 of the Act of May 10, 2018 on the Protection of Personal Data (Journal of Laws of 2019, item 1781) and pursuant to Art. 58 sec. 1 lit. a) and lit. e) and art. 58 sec. 2 lit. b) Regulation of the European Parliament and the EU Council 2016/679 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 UE L 119 of 04/05/2016, p. 1, with changes announced in the Official Journal of the European Union L 127 of 23/05/2018, p. 2, and in the Official Journal of the European Union L 74 of 04.03. 2021, p. 35), following administrative proceedings to impose an administrative fine on T. Sp. z o.o., President of the Personal Data Protection Office,

gives a reminder T. Sp. z o.o., for violation of the provisions of Art. 58 sec. 1 lit. a) and lit. e) Regulation of the European Parliament and the EU Council 2016/679 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 UE L 119 of 04.05.2016, p. 1, with the changes announced in the Journal of Laws UE L 127 of 23/05/2018, page 2, and in the Journal of Laws of the European Union L 74 of 04/03/2021, page 35), consisting in failure to provide the President of the Office for Personal Data Protection with access to data personal data and information necessary for the performance of its tasks.

Justification

On [...] .06.2020, the Office for Personal Data Protection received a notification from T. Sp. z o.o. (hereinafter: "the Company") concerning a breach of personal data protection consisting in a phishing attack, as a result of which an unauthorized person obtained login data to the e-mail account of an accounting employee.

In view of the need to obtain additional information necessary to assess the circumstances related to the probable breach of

personal data protection, the President of the Personal Data Protection Office (hereinafter also: "President of the Personal Data Protection Office"), as part of the initiated administrative procedure with the reference number [...], addressed the Company in a letter from [...] November 2020 to submit the following explanations within 7 days from the date of delivery of the said correspondence:

whether the Company has an implemented procedure for the retention of data processed via e-mail;

whether the procedure specifying the rules of employee access to individual e-mail accounts of the Company has been implemented;

what are the technical and organizational safeguards in the event of loss of availability relating to e-mail boxes in the field of archiving and making backups;

whether employees received training in the safe use of e-mail, making them aware of potential social engineering and IT attacks and methods of protection against them;

whether the law enforcement authorities have been notified of the violation.

The aforementioned letter, sent via the Polish postal operator to the address of the registered office of the Company disclosed in the National Court Register (KRS), was received on [...]. Companies to submit explanations by setting a 7-day deadline for responding to such a request. At the same time, the Company was informed that failure to provide an exhaustive response to the summons may result in the imposition of an administrative fine referred to in Art. 83 sec. 5 lit. e) Regulation 2016/679. The letter was received on [...] April 2021. The Company did not reply to both of the above-mentioned letters.

Due to the lack of information necessary to resolve the case with the reference number [...], the President of the Personal Data Protection Office (UODO) instituted ex officio against the Company - pursuant to Art. 83 sec. 5 lit. e) Regulation 2016/679 - administrative proceedings to impose an administrative fine in connection with the violation of Art. 58 sec. 1 lit. a) and e) of Regulation 2016/679. The President of the Personal Data Protection Office advised the Company that he does not fulfill his obligation to provide information necessary for the performance of the office's tasks, which may result in the imposition of an administrative fine. He obliged the company to present the financial statements within 7 days from the date of the letter's delivery. Moreover, he informed that the provision of explanations within the above-mentioned deadline may have a mitigating effect on the size of the administrative fine or may result in its withdrawal. The Company was informed about the initiation of the procedure by letter of [...] July 2021, reference number [...], and the correspondence sent via Poczta Polska was received

by the Company on [...] July 2021.

In response to the letter informing about the initiation of the administrative procedure, the Company, in a letter of [...] July 2021, provided explanations enabling the continuation of the procedure in the case No. [...]. She also stated that she is very serious about the protection of personal data, and the lack of receipt of the correspondence was due to organizational reasons related to the pandemic, which resulted in the loss of the parcel. The company also attached the financial statements for 2020.

After reviewing the entirety of the evidence collected in the case, the President of the Office for Personal Data Protection considered the following.

Pursuant to Art. 57 sec. 1 lit. a) Regulation 2016/679, the President of the Personal Data Protection Office, as a supervisory authority within the meaning of art. 51 of Regulation 2016/679, monitors and enforces the application of this regulation on its territory. As part of his powers, the President of the Personal Data Protection Office is entitled, inter alia, to conduct proceedings on the application of the provisions of the legal act in question (Article 57 (1) (h)), including proceedings related to the assessment of personal data breaches, reported to the President of the Personal Data Protection Office by administrators pursuant to Art. 33 of the Regulation 2016/679. In order to enable the performance of such defined tasks, the President of the Personal Data Protection Office is entitled to a number of tasks specified in art. 58 sec. 1 of Regulation 2016/679, the rights in the scope of conducted proceedings, including the right to order the administrator and the processor to provide all information needed to perform its tasks (Article 58 (1) (a)) and the right to obtain access from the administrator and the processor to all personal data and information necessary for the performance of its tasks (Article 58 (1) (e)). Violation of the provisions of Regulation 2016/679, consisting in the failure of the controller or the processor to provide access to the data and information referred to above, resulting in the violation of the authority's rights specified in art. 58 sec. 1, is subject to - in accordance with art. 83 sec. 5 lit. e) in fine of Regulation 2016/679 - an administrative fine of up to EUR 20,000,000, and in the case of an enterprise - up to 4% of its total annual worldwide turnover from the previous financial year, with the higher amount being applicable.

In addition, the President of the Personal Data Protection Office is entitled to a number of provisions specified in Art. 58 sec. 2 remedial powers, including reminders to the administrator or processor in the event of violation of the provisions of Regulation 2016/679 by processing operations. The President of the Personal Data Protection Office, acting pursuant to Art. 58 sec. 2 lit. b) of Regulation 2016/679, it may consider it justified to provide the administrator with a reminder in the scope of the

infringement of the provisions of art. 58 sec. 1 lit. a) and e) of Regulation 2016/679. Pursuant to recital 148 of Regulation 2016/679, in order for the enforcement of the provisions of the Regulation to be more effective, sanctions, including administrative fines, should be imposed for its breach - in addition to or instead of appropriate measures imposed by the supervisory authority pursuant to this Regulation. If the infringement is minor, the fine may be replaced by an admonition. However, due attention should be paid to the nature, gravity and duration of the breach, whether the breach was not intentional, the actions taken by the controller to minimize the damage, the degree of liability or any previous relevant breaches, how the supervisory authority learned on a breach, on compliance with the measures imposed on the controller or processor, on the application of codes of conduct, and on any other aggravating or mitigating factors.

Referring to the above-mentioned provisions of the Regulation 2016/679 to the facts established in this case, it should be stated that the Company, as a party to the proceedings No. and personal data necessary for the performance of its tasks, resulting from art. 58 sec. 1. lit. a) and lit. e) Regulation 2016/679. In this case, the information important for the further course of the proceedings was to determine whether the Company has an implemented procedure for the retention of data processed via e-mail, or whether a procedure has been implemented specifying the rules of employee access to individual e-mail accounts of the Company, what are the technical and organizational security measures in the event of loss of availability. relating to e-mail boxes in the field of archiving and making backups, whether employees have received training in the safe use of e-mail, making them aware of potential social engineering and IT attacks and methods of protection against them, or whether the law enforcement authorities have been notified of the breach.

Preventing access to information requested by the President of the Personal Data Protection Office from the Company stood in the way of a thorough examination of the case and resulted in the prolongation of the proceedings, which is contrary to the basic rules governing administrative proceedings - specified in Art. 12 sec. 1 of the Act of June 14, 1960, Code of Administrative Procedure (Journal of Laws of 2021, item 745, as amended), the principles of insight and speed of proceedings. The President of the Personal Data Protection Office, in order to establish the facts of the case with the reference number [...], twice requested the Company to send explanations. He received no reply to any of the letters dated […] November 2020 and […] April 2021. As a result of the above, it was necessary to initiate these proceedings to impose an administrative fine, as a result of which the Company started cooperation with the President of the Personal Data Protection Office by sending detailed explanations in the proceedings with reference number [...], which allowed the President of the Personal Data Protection Office

to continue the activities in the above-mentioned case.

Taking into account the above findings, there is no doubt that the Company violated the provisions of Regulation 2016/679 with its behavior. The justification provided by the Company for not responding to the requests of the President of the Personal Data Protection Office does not remove the responsibility for the identified omission. At the same time, however, the reasons indicated by the Company for the initial lack of cooperation with the supervisory body should be considered as credible and having a significant impact on the assessment of the Company's behavior in the context of the choice of the sanction applied to it in these proceedings. In the opinion of the President of the Personal Data Protection Office, the lack of reaction of the Company to the requests for explanations was due to the Company's negligence, which resulted in the loss of the parcel.

In the present state of affairs, apart from the lack of a response to the requests for explanations - which was supplemented by the Company as a result of the initiation of this proceeding - no other indications were found that the Company would not cooperate with the President of the Personal Data Protection Office. The circumstances of the case, and in particular the Company's attitude later, allow the conclusion that its initial tardiness did not result from bad will, nor was it intended to deliberately obstruct the proceedings. On the contrary - the subsequent, active attitude of the Company indicates its readiness for further cooperation with the President of the Personal Data Protection Office. In the opinion of the supervisory body, the very initiation of proceedings to impose an administrative fine and the real prospect of imposing a financial penalty have become a clear signal for the Company that further avoidance of the obligations imposed by the provisions of Regulation 2016/679 will inevitably lead to the application of the strictest sanctions provided for in these provisions.

Bearing in mind the above, acting pursuant to Art. 58 sec. 2 lit. b) of Regulation 2016/679, according to which each supervisory authority has the right to issue a reminder to the controller or processor in the event of violation of the provisions of this Regulation by processing operations, the President of the Personal Data Protection Office found it justified to provide the Company with a reminder regarding the breach of the provisions art. 58 sec. 1 lit. a) and lit. e) Regulation 2016/679, assuming that in the light of the criteria set out in Art. 83 sec. 2 of Regulation 2016/679, it will be effective and sufficient. It should be noted, however, that in the event of a similar event occurring in the future, each admonition issued by the President of the Personal Data Protection Office against the Company will be taken into account when assessing the premises for a possible administrative penalty, in accordance with the principles set out in Art. 83 sec. 2 of the Regulation 2016/679.

In this factual and legal state, the President of the Personal Data Protection Office resolved as in the sentence.

The decision is final. The party has the right to lodge a complaint against the decision with the Provincial Administrative Court in Warsaw, within 30 days from the date of its delivery, via the President of the Personal Data Protection Office (address: ul. Stawki 2, 00-193 Warsaw). The fee for the complaint is PLN 200. In the proceedings before the Provincial Administrative Court, the party has the right to apply for the right of assistance, which includes exemption from court costs and the appointment of an attorney, legal advisor, tax advisor or patent attorney. The right to assistance may be granted at the request of a party submitted prior to the initiation of the proceedings or in the course of the proceedings. The application is free of court fees.

2022-01-26