THE CHAIRMAN OF PERSONAL DATA PROTECTION

Warsaw, 23

March

2022

DECISION

DKE.561.3.2022

Based on Article. 105 § 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 sec. 1 and 2 and article. 60 of the Act of May 10, 2018 on the Protection of Personal Data (Journal of Laws of 2019, item 1781), as well as pursuant to art. 58 sec. 1 lit. e) Regulation of the European Parliament and of 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 O. Sp. z o.o., President of the Personal Data Protection Office

discontinues the proceedings.

JUSTIFICATION

Facts

In connection with the [...] July 2021 by O. Sp. z o.o. (hereinafter referred to as the "Company"), with the notification of a breach of personal data protection consisting in unauthorized access to the Company's IT system, the President of the Personal Data Protection Office (hereinafter referred to as the "President of the Personal Data Protection Office") initiated administrative proceedings with reference number [...] aimed at explaining the circumstances of the breach reported by the Company.

As part of the above-mentioned procedure, the President of the Personal Data Protection Office (UODO) addressed the Company - in a letter of [...] August 2021 - with a request to answer the following questions and to present the following documents:

"Has the effectiveness of the technical measures used to ensure the security of processing been regularly tested, measured

and assessed? If so, please provide evidence of both pre-infringement and post-infringement testing (e.g. penetration testing).

Have any procedures been developed for authorizing users and granting them appropriate authorizations (e.g. regarding password parameters, their complexity, the policy of assigning identifiers)?

Delivering the procedure for making and testing backups.

Submitting the risk analysis carried out before and after the personal data breach.

Was an investigation conducted to determine whether the attacker did not gain access to data other than those specified in point 6 of the personal data breach notification.

Provide relevant evidence confirming the application of the security measures specified in item 9B of the form. "

The summons was delivered to the Company on [...] September 2021.

In a letter of [...] September 2021, the Company provided explanations regarding the questions addressed to it in the letter of the President of the Personal Data Protection Office of [...] August 2021; it also provided the following documents: […].

In a letter of [...] October 2021, the President of UODO requested the Company to submit additional explanations and provide additional evidence in the following scope:

"Please provide information as to whether, and if so, what categories of data and to whom an unauthorized person could have read, since he obtained access to the" list of our clients "and the" list of orders ", referred to in Annex 4 to the letter administrator of [...] September 2021

Please provide relevant evidence to support the statement that "the Company is currently verifying the effectiveness of technical measures."

The summons was delivered to the Company on [...] October 2021.

By letter of [...] October 2021, the Company provided additional explanations in the case, stating, inter alia, as follows:

"With regard to the" list of our clients ", information that did not contain personal data could have been obtained, because it was only the data of legal entities - customers of the Company [...]." "While referring to the" list of orders " - the data of clients, i.e. clients of administrators entrusting the Company with personal data belonging to natural persons who are their end clients, could be read. In relation to these data, the Company does not act as an administrator, but as a processor, which is beyond the scope of the submitted notification, and indicating the category of data would require confirmation of the possibility of their transfer by the Company with the Customers. "Attached to the letter, the Company also presented a statement of [...] October

2021 regarding the verification of the effectiveness of the technical measures implemented by the Company, together with appendices presenting relevant procedures in force in the Company.

In a letter of [...] November 2021, the President of UODO requested the Company to submit further explanations and provide additional evidence in the following scope:

"Indication of whether the data administrators for which the processing entity is the Company have been notified of the breach of personal data protection, and if so, please provide the date of their notification and provide relevant evidence in this regard.

Submission to the Personal Data Office of the list of data controllers for which the Company is the processor.

Indication of which categories of personal data were disclosed in the "order list" and how many people the data concerned.

Indication whether the effectiveness of the technical measures used to ensure the security of processing was regularly tested, measured and assessed before and after the breach of personal data protection (please provide relevant evidence). "

The summons was delivered to the Company on [...] November 2021.

By letter of [...] November 2021, the Company provided additional explanations and evidence regarding the notification of administrators of the breach of personal data protection (the first question contained in the letter of the President of the Personal Data Protection Office of [...] November 2021 - see point 6 of the justification hereof of the decision) and in the scope of regular verification of the effectiveness of the technical measures applied by the Company (the last of the four questions contained in the letter of the President of the Personal Data Protection Office of [...] November 2021 - see point 6 of the justification to this decision).

In a letter of [...] November 2021, the Company refused to answer the two remaining questions contained in the letter of the President of the Personal Data Protection Office of [...] November 2021.

In response to the request to present a list of data administrators for which the Company is a processor, the Company indicated, inter alia, that "This obligation [confidentiality obligation] usually applies to all data received from Administrators, including data on the conclusion of contracts on the basis of which there is cooperation and data that the contractor uses the services of the Company. The company, wishing to comply with the obligation of confidentiality, in order to avoid negative sanctions, not only legal and financial, but also image-related, it is not possible to disclose this data without obtaining the prior consent of the Administrators. " And further: “Additionally, we make a reservation that, irrespective of the above, the list of Administrators is also a legally protected business secret of the Company (Article 11 of the Act on Combating Unfair

Competition). This information has a significant economic value for the Company as it constitutes the Company's customer base. "

In response to the question about the categories of personal data disclosed in the "list of orders" and the number of persons to whom these data pertained, the Company argued in particular that with regard to these data, "the Company does not act as an administrator, but as a processor, therefore it does not is entitled to disclose this type of data without a documented instruction from the Administrators. The Company is bound by contracts for entrusting the processing of personal data concluded with the Administrators, which strictly define the Company's rights and possibilities as well as processing guidelines, which also include the transfer of data to the Office for Personal Data Protection. Also, in accordance with the General Data Protection Regulation (GDPR), the notification of a personal data breach is the sole obligation and right of the personal data controller. " The company also indicated that "Regardless of the contractual obligations, the Company is expressly obliged to keep the data received from the Administrators ([...] also the data that was included in the" order list ") in strict confidence and confidentiality. This is information of economic value for the Administrators, constituting their business secret, which is subject to special legal protection, including based on the Act of April 16, 1993 on Combating Unfair Competition (Art. 11). Disclosure of information constituting a trade secret could constitute an act of unfair competition [...]. "

On [...] January 2022, the Department of Control and Violations of the Office for Personal Data Protection carried out at the Company an inspection of the compliance of its personal data processing with the provisions on the protection of personal data in connection with the breach of personal data protection, which initiated the procedure with reference number […].

During the inspection, conducted under reference number [...], and completed with the preparation of [...] January 2022, the inspection report, the Company provided the inspectors with all the information and documents requested by them; it also provided full visibility into its IT systems. In particular, the Company presented a list of its clients - entities for which it provides services related to the processing of personal data entrusted to it. The company also provided information on the categories of personal data processed by it. As stated in the inspection report: "The Company processes the full scope of data of employees, employees of the Company's clients (contact persons in the scope of: name, surname, e-mail address and possibly telephone number), as well as data of clients of cooperating entities, i.e. . recipients of parcels in the scope of: name, surname, e-mail address, telephone number, shipping address. " Moreover, it was established that "a person who got into the Company's system had access to the data of employees of all customers, while access to data resulting from orders

concerned about 20 customers [customers of entities cooperating with the Company - addressees of shipments]."

The above facts of the case were determined by the President of the Personal Data Protection Office on the basis of all official correspondence between the Company and the President of the Personal Data Protection Office, contained in the files of the proceedings with reference number [...], as well as documents from the control files with reference number […]. This documentation reflects all the attempts by the President of the Personal Data Protection Office to obtain access to information necessary for the performance of his tasks, i.e. in this case - to consider the case no. [...], and on the other hand - the reaction of the Company to the demands of the President of the Personal Data Protection Office.

Procedure

Due to the failure by the Company to provide the information necessary to settle the case no. [...], irrespective of the control proceedings with reference number [...] (see points 11-12 of this justification), the President of the Personal Data Protection Office initiated ex officio against the Company - pursuant to Art. 83 sec. 5 lit. e) Regulation 2016/679 - these administrative proceedings (ref. DKE.561.3.2022) regarding the imposition of an administrative fine, in connection with the violation of Art. 58 sec. 1 lit. e) Regulation 2016/679. The Company was informed about the initiation of the procedure by letter of [...] January 2022 (ref .: DKE.561.3.2022 [...]), delivered to the Company on [...] January 2022. The Company was also requested by this letter - in order to establish the basis of the penalty, based on art. 101a paragraph. 1 of the Act of May 10, 2018 on the Protection of Personal Data (Journal of Laws of 2019, item 1781), hereinafter referred to as "u.o.d.o." - to present a financial statement or other document showing the amount of turnover and financial result achieved by the Company in 2021.

In response to the information on the initiation by the President of the Personal Data Protection Office (UODO) of the procedure to impose an administrative fine, the Company - in a letter of [...] January 2022 - explained that during the inspection carried out at it on [...] January 2022, "all the requested information and documents, including information on (i) the category of personal data contained in the Order List, (ii) the number of data subjects and (iii) the list of data controllers for which the Company is a processor that have not been sent earlier". In connection with the above, the Company applied for the waiver of the administrative pecuniary penalty for violation of Art. 58 sec. 1 letter e) of Regulation 2016/679. At the same time - attached to the letter - the Company submitted its financial statements for 2021, requested by the President of the Personal Data Protection Office in a letter of [...] January 2022.

After considering all the evidence collected in the case, the President of the Personal Data Protection Office considered the

following.

Regulations

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 this legal act (Article 57 (1) (h) of Regulation 2016/679), including proceedings related to the assessment of personal data breaches, reported to the President of the Personal Data Protection Office by data 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 has a number of specified in Art. 58 sec. 1 of Regulation 2016/679, 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) of Regulation 2016/679) and the right to obtain from the administrator and the entity processing access to all personal data and all information necessary to perform its tasks (Article 58 (1) (e) of Regulation 2016/679).

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.

Pursuant to Art. 105 § 1 of the Act of June 14, 1960 Code of Administrative Procedure (Journal of Laws of 2021, item 735, as amended), hereinafter referred to as the "k.p.a.", when the proceedings for any reason have become redundant in whole or in part , a public administration body issues a decision to discontinue the proceedings, respectively, in whole or in part.

Pursuant to Art. 60 u.o.d.o. proceedings regarding infringement of provisions on the protection of personal data are conducted by the President of the Personal Data Protection Office. Art. 7 sec. 1 u.o.d.o. and stipulates that in matters not regulated in this act, the CCP shall apply to administrative proceedings before the President of the Personal Data Protection Office (including proceedings on the imposition of an administrative fine, referred to in Chapter 11 of the Act on Public Procurement Law).

Pursuant to Art. 7 sec. 2 u.o.d.o. these proceedings are single-instance proceedings.

Legal assessment

In this case, due to the failure by the Company to provide the information necessary to resolve the case no. [...], the President of the Personal Data Protection Office (UODO) initiated ex officio proceedings to impose an administrative fine on the Company. The Company was informed of this fact by letter dated [...] January 2022, and delivered to it on [...] January 2022. Therefore, the date of initiation of these proceedings should be [...] January 2022. According to the doctrine and jurisprudence of administrative courts, "[z] and the date of initiation of ex officio proceedings should be the first official action against the party or action taken in the case by the authority ex officio public administration (judgment of the Supreme Administrative Court of October 13, 1999, IV SA 1364/97, unpublished; judgment of the Supreme Administrative Court of January 20, 2010, II GSK 321/09, Legalis). The jurisprudence also often emphasizes that the fact of taking such an action must be related to the notification of the party (post. NSA of 4.3.1981, SA 654/81, ONSA 1981, No. 1, item 15; judgment of the Supreme Administrative Court of 26.10. 1999, III SA 7955/98, Legalis). " (R. Hauser, M. Wierzbowski (eds), Code of Administrative Procedure. Comment. 7th edition, Warsaw 2021, commentary to Art. 61, Legalis).

At the same time, based on the explanations provided by the Company in a letter of [...] January 2022 (see point 14 of the justification to this decision) and the documents from the inspection files with reference number [...] (see point 12 of the justification to this decision), it was found that the information requested from the Company in the letter of [...] November 2021 (see point 6 of the justification to this decision) was provided to the President of UODO - to the extent not previously available - By […] January 2022 at the latest. On that date, the final inspection protocol was drawn up, in which the protocol (and its appendix) contained the above-mentioned information.

In connection with the above, it should be stated that the present proceedings, initiated after the date of obtaining by the President of the Personal Data Protection Office, all necessary for him in the proceedings with reference number [...] information was redundant from the moment of its initiation. As it was established in the course of the proceedings, there was no actual state of affairs justifying the imposition of an administrative fine on the Company for the infringement covered by the subject matter of the proceedings specified in the letter informing about its initiation, i.e. for the infringement of Art. 58 sec. 1 lit. e) Regulation 2016/679 consisting in failure to provide the President of the Personal Data Protection Office with access to information necessary for the performance of his tasks.

Pursuant to Art. 105 § 1 of the Code of Administrative Procedure, used in administrative proceedings before the President of

the Personal Data Protection Office pursuant to Art. 7 sec. 1 u.o.d.o., in such a situation ("when the proceedings for any reason became groundless in whole or in part"), the administrative proceedings are subject to obligatory discontinuation. The prerequisite for discontinuation of the proceedings may exist even before its commencement, which will be revealed only in the pending proceedings (as was the case in the present case), and it may also arise during the proceedings, i.e. in a case already pending before the administrative authority.

The doctrine indicates that "The discontinuation of the proceedings is not dependent on the will of the administrative body, and even less left to the discretion of the body - this body is obliged to discontinue the proceedings if it is found to be irrelevant. […] Circumstances which constitute the grounds for discontinuation of the proceedings may arise both before and during the initiation of the proceedings. […] The redundancy of the proceedings may also result from a change in the facts of the case. The proceedings must be deemed to be groundless due to the cessation of the facts subject to regulation by the administrative authority by way of a decision (see the justification of the judgment of the Supreme Administrative Court of 29 September 1987, IV SA 220/87, ONSA 1987, No. 2, item 67). " (P. M. Przybysz [in:] Code of Administrative Procedure. Updated commentary, LEX / el. 2022, commentary to Art. 105).

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

Instruction

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.

2022-05-10