THE CHAIRMAN OF PERSONAL DATA PROTECTION

Warsaw, 02

June

2022

DECISION

DKN.5131.23.2022

Based on Article. 104 § 1 of the Act of June 14, 1960, Code of Administrative Procedure (Journal of Laws of 2021, item 735, as amended) in connection with Art. 7 sec. 1 and art. 60 of the Act of May 10, 2018 on the Protection of Personal Data (Journal of Laws of 2019, item 1781), as well as Art. 57 sec. 1 lit. a) and h) and art. 58 sec. 2 lit. b) in connection with Art. 34 sec. 2 in connection with Art. 33 sec. 3 lit. c) and d) Regulation of the European Parliament and of the EU Council 2016/679 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 on data protection) (Journal of Laws UE L 119 of May 4, 2016, p. 1, Journal of Laws UE L 127 of May 23, 2018, p. 2 and EU Official Journal L 74 of March 4, 2021, p. 35), after conducting the ex officio administrative procedure concerning the infringement by N. Sp. z o.o. with headquarters in G. provisions on the protection of personal data, the President of the Office for Personal Data Protection

finding an infringement by N. Sp. z o.o. based in G. provisions of Art. 34 sec. 2 in connection with Art. 33 sec. 3 lit. c) and d) of Regulation 2016/679 of the European Parliament and of the Council 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 regulation on data protection) (Journal of Laws UE L 119 of May 4, 2016, p. 1, Journal of Laws UE L 127 of May 23, 2018, p. 2 and EU Official of 4.03.2021, p. 35), hereinafter referred to as Regulation 2016/679, consisting in not providing the data subject without undue delay with a notification of a breach of personal data protection containing a description of the possible consequences of the breach and a description of the measures applied or proposed by the controller in in order to remedy a breach of personal data protection, including measures to minimize its possible negative effects, it issues a reminder to N. Sp. z o.o. based in G.

Justification

On [...] August 2021, the President of the Personal Data Protection Office, hereinafter referred to as the President of the

Personal Data Protection Office, received a notification of a personal data breach made by N. Sp. z o.o. with headquarters in G. (hereinafter referred to as N. or the Administrator), registered under the reference number [...], informing about a breach of personal data protection of two people, i.e. a patient and a doctor N. The incident which was the subject of the report was the use of the patient's and doctor's data to issue a prescription for a refunded drug. The data administrator found out about this fact as a result of the initiation of control activities by the Department of Control, Local Control Department XI in the National Health Fund. The categories of data that have been violated are: in the case of a patient - name and surname, address of residence or stay and PESEL number, and in the case of a doctor - name and surname and PWZ number. Due to the scope of the disclosed personal data, the indicated breach resulted in a high risk of violating the rights or freedoms of patient N. Therefore, the Administrator informed in the notification of [...] August 2021 that on [...] July 2021 about the breach of data protection personal data, he notified the data subject and provided the content of this notification.

The President of the Personal Data Protection Office, acting pursuant to Art. 52 sec. 1 of the Act on the Protection of Personal Data and Art. 34 sec. 4 of Regulation 2016/679, with a request of November 2021, requested the Administrator to notify the data subject (patient [...]) again about the breach of the protection of his personal data, due to the fact that the breach notification, which was anonymised the content was provided by the Administrator along with the notification of the breach of personal data protection, did not meet the conditions set out in art. 34 sec. 2 in connection with Art. 33 sec. 3 lit. c) and d) of Regulation 2016/679, i.e. it did not contain a description of the possible consequences of a breach of personal data protection and a description of the measures taken or proposed by the controller to remedy the breach - including, where applicable, measures to minimize its possible negative effects.

The administrator did not respond to the request of the supervisory authority and did not provide the content of the repeated notification addressed to the person whose data was subject to the infringement.

In view of the above, in a letter of April 2022, the President of the Personal Data Protection Office (UODO) initiated ex officio administrative proceedings against the Administrator regarding incorrect notification of a breach of personal data protection of the person concerned by the breach, due to failure to provide this person with a description of the possible consequences of the breach of personal data protection and a description of measures. applied or proposed by the administrator to remedy the breach of personal data protection, including, where appropriate, measures to minimize its possible negative effects, in accordance with art. 34 sec. 2 in connection with Art. 33 sec. 3 lit. c) and d) of Regulation 2016/679 (letter reference [...]).

The administrator responded in writing to the infringement of the provisions on the protection of personal data, which is the subject of the administrative procedure, mentioned in the notice of initiation of the procedure and on [...] April 2022 sent explanations regarding the above-mentioned breach of personal data protection, in which it states that: "N. Sp. z o.o. at G. performed without delay and with all due diligence all actions indicated by the Office for Personal Data Protection in a letter dated […] .11.2021 The person whose data was disclosed was notified in a letter of […] .11.2021 about the breach of personal data protection, taking into account the possible consequences of this breach and the measures taken by N. Sp. z o.o. in order to minimize its possible negative effects. Moreover, we explain that due to the age of the data subject, the administrator, in addition to sending a written notification, spoke again by phone to the person whose data was disclosed, so as to explain the whole situation in the most accessible way and not causing unnecessary stress and convey the required legal information. At the same time, we explain that the letter informing you about the activities performed has been prepared, unfortunately, as it has now turned out, due to human error, it was not sent to you, so we have not fulfilled the obligation to inform the Office for Personal Data Protection about the above-mentioned activities performed within the time limit. We deeply regret this. At the same time, please treat this letter as meeting the obligation to inform the Office for Personal Data Protection about the actions taken, indicated by the Office for Personal Data Protection in the letter of [...] .11.2021 and pursuant to Art. 105 of the Code of Administrative Procedure, discontinuation of the initiated procedure ". To the submitted explanations, the Administrator attached another notification addressed to the person affected by the infringement. The notification sent to the supervisory authority of [...] November 2021, addressed to the data subject, described the possible consequences of the personal data breach and the actions taken by N. to minimize the risk of a recurrence of the breach, but did not describe the measures remedial actions that can be taken by the person whose data has been violated, which meant the Administrator's failure to comply with the obligation specified in art. 34 sec. 2 in connection with Art. 33 sec. 3 lit. d) Regulation 2016/679.

Then, on [...] May 2022, the Administrator sent further explanations regarding the above-mentioned violations in which he informed that: “In addition to our reply to the Notice of Initiation of Proceedings in […] of […] .04.2022, we would like to provide you with additional information. Due to the health condition, age of the data subject and possible health consequences resulting therefrom, before sending the notification provided to you on [...]. On November 11, 2021, the employee of N. met this person in person to provide him with the information required by law in a form that takes into account the health condition of this person and the medical indications of the doctor. All information provided by you in the Introduction of [...] .11.2021 were

provided in a clear and accessible form, the data subject is in close contact with N. and knows that he can count on any support in this matter from the data controller. However, given that the written notification sent to the data subject on […] .11.2021 did not contain all the elements indicated by you in the Statement of [...]. On 11/2021, we decided to send another letter to the data subject in order to provide this person with complete information indicated by you in writing. We would like to emphasize that we treated the matter of informing the data subject about the infringement very seriously from the moment the infringement was discovered. The data subject was immediately informed about the incident and its consequences in a form adapted to his or her health condition in consultation with a doctor. After receiving from you the indications contained in the Statement of […]. On November 11, 2021 we immediately completed it. In addition to the above-mentioned actions, the data breach that occurred was analyzed by us in detail, corrective and corrective actions were taken, as reported in the Incident Analysis Report attached to this letter ". To the above N. attached the letter of the notice of [...] May 2022, addressed to the person affected by the infringement, containing all the information specified in Art. 34 sec. 2 of Regulation 2016/679.

In these facts, the President of the Personal Data Protection Office considered the following.

Art. 34 sec. 1 of Regulation 2016/679 indicates that in a situation of high risk to the rights or freedoms of natural persons resulting from the breach of personal data protection, the controller is obliged to notify the data subject about the breach without undue delay. Pursuant to Art. 34 sec. 2 of Regulation 2016/679, the correct notification should:

1) describe the nature of the personal data breach in clear and simple language;

2) contain at least the information and measures referred to in Art. 33 sec. 3 lit. b), c) and d) of Regulation 2016/679, that is: - name and contact details of the data protection officer or designation of another contact point from which more information can be obtained; or proposed by the controller to address the personal data breach, including, where appropriate, measures to minimize its possible negative effects.

As a result of the analysis of the breach of personal data protection reported by the Administrator, which took into account the nature of the breach, its duration, data categories, the number of persons affected by the breach and the remedial measures applied - the President of the Personal Data Protection Office decided that the breach of confidentiality of data, in particular data concerning the name, surname, address of residence or stay and PESEL number, causes a high risk of violating the rights or freedoms of natural persons, therefore it is necessary to notify the data subject (patient [...]) about the breach of personal data protection and transfer all information specified in Art. 34 sec. 2 of Regulation 2016/679.

It should be emphasized that in a situation where as a result of a breach of personal data protection there is a high risk of violating the rights or freedoms of natural persons, the controller is obliged under Art. 34 sec. 1 of the Regulation 2016/679, notify the data subject of such a breach without undue delay. This means that the controller is obliged to implement all appropriate technical and organizational measures to immediately identify the breach of personal data protection and promptly inform the supervisory authority, and in cases of high risk of violation of rights or freedoms, also the data subject. The administrator should fulfill this obligation as soon as possible. Recital 86 of Regulation 2016/679 explains: "The controller should inform the data subject without undue delay of the breach of personal data protection if it may result in a high risk of violating the rights or freedoms of that person, so as to enable that person to take the necessary preventive measures. . Such information should include a description of the nature of the personal data breach and recommendations for the individual concerned to minimize the potential adverse effects. Information should be provided to data subjects as soon as reasonably possible, in close cooperation with the supervisory authority, respecting instructions provided by that authority or other relevant authorities such as law enforcement authorities. For example, the need to minimize the imminent risk of harm will require the immediate notification of data subjects, while the implementation of appropriate measures against the same or similar data breaches may justify subsequent notification. '

By notifying the data subject without undue delay, the Administrator enables the person to take the necessary preventive measures to protect the rights or freedoms against the negative effects of the breach. Art. 34 sec. 1 and 2 of Regulation 2016/679 is intended not only to ensure the most effective protection of the fundamental rights or freedoms of data subjects, but also to implement the principle of transparency, which results from Art. 5 sec. 1 lit. a) Regulation 2016/679 (cf. Chomiczewski Witold [in:] GDPR. General Data Protection Regulation. Comment. ed. E. Bielak - Jomaa, D. Lubasz, Warsaw 2018). Proper fulfillment of the obligation specified in art. 34 of Regulation 2016/679 is to provide data subjects with quick and transparent information about a breach of the protection of their personal data, together with a description of the possible consequences of the breach of personal data protection and the measures that they can take to minimize its possible negative effects. Acting in accordance with the law and showing concern for the interests of the data subject, the controller should, without undue delay, provide the data subject with the best possible protection of personal data. To achieve this goal, it is necessary to indicate at least the information listed in Art. 34 sec. 2 of Regulation 2016/679, the obligation of which the administrator did not properly fulfill. In the original breach notification addressed to the data subject on [...] July 2021, the

administrator did not indicate all the required elements, pursuant to Art. 34 sec. 2 in connection with Art. 33 sec. 3 lit. c) and d) of Regulation 2016/679, i.e. the notification did not contain a description of the possible consequences of the breach of personal data protection and a description of the measures taken or proposed by the Administrator to remedy the breach - including, where applicable - measures to minimize its possible negative effects. In the next notification, dated [...] November 2021, sent by the Administrator to the data subject, as a result of an application submitted by the President of the Personal Data Protection Office pursuant to Art. 52 sec. 1 of the Act on the Protection of Personal Data and Art. 34 sec. 4 of Regulation 2016/679, again not all the required elements were indicated, i.e. the notification did not contain a description of the measures taken or proposed by the administrator to remedy the breach - including, where applicable - measures to minimize its possible negative effects, which may be taken by the person himself the data subject to limit the effects of the breach, pursuant to Art. 34 sec. 2 in connection with Art. 33 sec. 3 lit. d) Regulation 2016/679. Only in the notification of [...] May 2022, N. provided the data subject with a notification containing all the aforementioned the provisions of Regulation 2016/679 information. Consequently, this means that up to this point, the Controller has not provided the affected person with full information about the breach of personal data protection, which deprived him of any indications as to what actions he can take to effectively counter the possible negative effects of the breach.

Improper performance by the Administrator of the obligation specified in art. 34 sec. 2 in connection with Art. 33 sec. 3 lit. c) and d) of Regulation 2016/679, as a result of incorrect notification of the data subject about a breach of the protection of his personal data, therefore, it does not raise any doubts. The Administrator's failure to fulfill this obligation towards the data subject upon the first notification of a personal data breach and provision of all required information only with the third notification (which was sent on [...] May 2022, i.e. 289 days after the breach was found ) causes the supervisory authority to apply a corrective measure, since the existence of a violation of the law in the above-mentioned scope is indisputable. 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 Administrator for the incorrect performance of obligations incumbent on him 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. In the opinion of the President of the Personal Data Protection Office, the admonition imposed will also fulfill its preventive function, duly preventing future violations

of the provisions on the protection of personal data by [...] and other data administrators.

In view of the above, the President of the Personal Data Protection Office resolved as in the sentence.

2022-07-18