THE CHAIRMAN OF PERSONAL DATA PROTECTION

Warsaw, 23

June

2022

DECISION

DKN.5131.14.2022

Based on Article. 104 § of the Act of June 14, 1960, Code of Administrative Procedure (Journal of Laws of 2021, item 735, as amended), art. 7 sec. 1 and art. 60 of the Act on the Protection of Personal Data (Journal of Laws of 2019, item 1781) and Art. 57 sec. 1 it. a) and h) and art. 58 sec. 2 it. b) in connection with Art. 34 sec. 2 of the 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 regulations) (Journal of Laws UE 119 of May 4, 2016, p. 1, Journal of Laws UE 127 of May 23, 2018, p. 2 and Journal of Laws UE 74 of March 4, 2021, p. 35), from the office of administrative proceedings regarding an incorrect notification by A. S.A. with its registered office in W., on a breach of the protection of personal data of persons affected by this breach, the President of the Office for Personal Data Protection

finding a breach by A. S.A. based in W., art. 34 sec. 2 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 UE 119 of May 4, 2016, p. 1, Journal of Laws UE 127 of May 23, 2018, p. 2 and Journal of further by Regulation 2016/679, granted by A. S.A. based in W., reminders.

Justification

On [...] May 2021 A. S.A. based in W., hereinafter referred to as the Company or the Administrator, notified the President of the Personal Data Protection Office, hereinafter referred to as the President of the Personal Data Protection Office, a breach of personal data protection, which was registered under the reference number [...]. The breach of personal data protection consisted in obtaining unauthorized access to the work e-mail account of the Company's employee. The analysis of the events showed that there was an unauthorized penetration of the user's box, using the protocols […] and […] - using his names and

passwords, as a result of which the confidentiality of the personal data processed was breached. The administrator determined in particular that the data of 12 persons affected by the reported breach included the name, surname, address of residence / correspondence address, PESEL number and number of the identity document (ID card / passport), data of 7 persons to whom the reported breach concerned, included the first name and surname, identity document number (ID card / passport / residence card) and PESEL number, data of 2 persons to whom the reported violation concerned, included first name, surname, PESEL number, residence address / correspondence address, data of 1 person included the name and address residence / correspondence number, identity document number (identity card / passport / residence card), data of 1 person included the name, surname, date of birth, identity document number (identity card / passport / residence card) and e-mail address. In the case of 6 persons affected by the violation, the data included the name, surname and number of the identity document (ID card / passport / residence card).

In the above-mentioned In the notification, the Administrator informed that he had notified the data subjects of a breach of their personal data protection, and also presented the anonymised content of the notification sent to these persons.

As a result of the content analysis of the above-mentioned of the notification, the President of the Personal Data Protection Office decided that the original notification of data subjects about the breach of their personal data did not contain the required pursuant to Art. 34 sec. 2 of Regulation 2016/679, i.e. a description of the nature of the personal data breach, name and surname and contact details of the Data Protection Officer or designation of another contact point from which more information can be obtained, a description of the possible consequences of the breach of personal data protection and a description of the measures applied or proposed by the controller to address the personal data breach, including, where appropriate, measures to minimize its possible negative effects.

Bearing in mind the above, the President of the Personal Data Protection Office, acting pursuant to Art. 52 sec. 1 of the Act on the Protection of Personal Data (Journal of Laws of 2019, item 1781) and Art. 34 sec. 4 of the Regulation 2016/679, asked the Administrator on [...] June 2021 to take appropriate actions aimed at immediate, correct and correct, i.e. covering all the above-mentioned and legally required elements, notification of data subjects about a breach of the protection of their personal data and elimination of similar irregularities in the future. In addition, the President of the Personal Data Protection Office informed the Administrator about the examples of threats to the rights or freedoms of data subjects related to the violation of the confidentiality of their personal data in the above-mentioned scope and provided the Company with information on the

recommendations that it should provide to data subjects, so that these persons can effectively protect themselves against the negative effects of violating the protection of their personal data.

In response to the received request, the Company, by letter of [...] ipca 2021, sent explanations in which it informed the data subjects about the breach of personal data protection and presented seven types of notifications to the abovementioned persons, depending on the scope of personal data covered by the breach. Analysis of the above-mentioned However, the notifications showed that the Administrator still did not include all the required elements in them, pursuant to Art. 34 sec. 2 of Regulation 2016/679, i.e. a description of the nature of the breach of personal data protection, taking into account the categories of personal data affected by the breach, a description of the possible consequences of the breach of personal data protection (the Company limited only to general phrases such as: identity, fraud, and financial loss, unsolicited marketing communications, phishing attempts ”) and the name of the data protection officer.

In view of the above, the President of the Personal Data Protection Office (UODO) initiated ex officio administrative proceedings regarding the possibility of the Company's breach of obligations under Art. 34 sec. 2 of Regulation 2016/679, in connection with incorrect notification of data subjects about a breach of the protection of their personal data (letter of [...] March 2022, ref. [...]).

In response to the notification sent by the President of the Personal Data Protection Office on this matter, the Company, in a letter of [...] March 2022, informed that on that date, i.e. [...] March 2022, it made, using electronic, traditional and directly, re-notify data subjects of a breach of the protection of their personal data and provided evidence confirming the actions taken by them, including the anonymised content of the notification addressed to the above-mentioned people. The analysis of the content of this notification showed that it contains all the elements indicated in Art. 34 sec. 2 of the Regulation 2016/679.

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

Pursuant to Art. 34 of the Act on the Protection of Personal Data, the President of the Personal Data Protection Office is the competent authority for data protection and the supervisory authority within the meaning of Regulation 2016/679. Pursuant to Art. 57 sec. 1 it. (a) and (h) of Regulation 2016/679, without prejudice to the other tasks set out under that Regulation, each supervisory authority on its territory shall monitor and enforce the application of this Regulation and conduct proceedings for infringements of this Regulation, including on the basis of information received from other supervisory authority or other public

authority.

On the other hand, 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 independently 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.

Pursuant to Art. 34 sec. 1 of Regulation 2016/679, if the breach of personal data protection may result in a high risk of violation of the rights or freedoms of natural persons, the controller shall notify the data subject of such a breach without undue delay.

Pursuant to Art. 34 sec. 2 of Regulation 2016/679, the notification referred to in para. 1 of this article, in clear and simple language, describes the nature of the personal data breach and contains at least the information and measures referred to in Art. 33 sec. 3 it. b), c) and d), i.e. it contains the name and surname and contact details of the data protection officer or the designation of another contact point from which more information can be obtained, describes the possible consequences of the breach of personal data protection and describes the measures taken or proposed by the controller in to remedy 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 in question, which took into account the nature of the breach, its duration, data categories, the number of persons affected by the breach and the applied remedial measures - the President of the Personal Data Protection Office decided that the breach of confidentiality of data, in particular data concerning the number PESEL number together with the name and surname, ID card number and address of residence or stay, causes a high risk of violating the rights or freedoms of natural persons, therefore it is necessary to notify data subjects about the violation of the protection of their personal data and to provide all the 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, pursuant to Art. 34 sec. 1 of Regulation 2016/679, notify the data subjects 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 a breach of personal data protection and promptly inform the supervisory authority, and in cases of high risk of violating the rights or freedoms of data subjects. The administrator

should fulfill this obligation as soon as possible. Recital 86 to the preamble to Regulation 2016/679 explains that "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 necessary preventive actions. 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 controller 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 it. a) Regulation 2016/679 (cf. Chomiczewski Witold [in:] GDPR. General Data Protection Regulation. Comment. ed. E. Bielak - Jomaa, D. ubasz, 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.

In light of the above, it should be pointed out that by acting in accordance with the law and showing care for the interests of data subjects, the Administrator should without undue delay provide data subjects with the opportunity to best protect their rights or freedom. 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 notification of the infringement addressed to the data subjects, the Company did not indicate the required, pursuant to Art. 34 sec. 2 of Regulation 2016/679, elements, i.e. description of the nature of the personal data breach, name and surname and contact details of the data protection officer or designation of another contact point from which more information can be obtained, description of the possible consequences of the breach of personal data protection and a description of the measures applied or proposed by the

controller to address the personal data breach, including, where appropriate, measures to minimize its possible negative effects. In the next notification sent by the above-mentioned persons on [...] July 2021, 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 have been indicated, i.e. a description of the nature of the personal data breach taking into account the categories of personal data affected by the breach, a description of the possible consequences of the breach of personal data protection (the Company limited itself to general wording such as, for example, "As part of the analysis the main risks were identified as: identity theft, fraud, and financial losses, unsolicited marketing communications, phishing attempts ") and the name of the data protection officer. Indication of the above-mentioned information took place only after the President of the Personal Data Protection Office initiated the administrative procedure, when on [...] March 2022, the Company sent to persons whose data was covered by the violation in question, a notification of violation of the protection of its personal data containing all specified in Art. 34 sec. 2 of the Regulation 2016/679, information. Consequently, this means that up to this point the Administrator has not provided the affected persons with full information about the breach of their personal data protection, which deprived them of any indications as to what actions they can take to effectively counter the possible negative effects of the breach.

Based on the facts outlined in this case, it is clear that in the period from [...] May 2021 (the date when the Company received information about the breach) until [...] March 2022 (the date of the correct notification of the breach), the Company did not provide data subjects with full information about the breach of protection of their personal data, i.e. did not provide them in a transparent and understandable form with all required pursuant to Art. 34 sec. 2 of Regulation 2016/679 information. Considering the long duration of the breach of law (and this despite the fact that the authority, in its speech of [...] June 2021, indicated to the Company that it needed to take appropriate actions without undue delay in order to properly notify persons about the breach) and noting that the correct fulfillment by the Administrator of his obligation to properly notify data subjects about the violation of the protection of their personal data took place only after the President of the Personal Data Protection Office initiated administrative proceedings in this case, it should be stated with a high degree of certainty that the state of violation of the law would have continued had it not been for the above reaction from the supervisory authority.

Incorrect performance by the Company of the obligation specified in Art. 34 sec. 2 of Regulation 2016/679, by defective notification by the Company of data subjects about a breach of the protection of their personal data, therefore does not raise

any doubts, and the subsequent correct performance by the Administrator of this obligation towards the data subject may not cause the supervisory authority to withdraw from issuing a reminder since the existence of an infringement of the law in the said period is unquestionable.

Nevertheless, the President of the Personal Data Protection Office, exercising his right under Art. 58 sec. 2 it. 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 admonition of the Company 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. In the opinion of the President of the Personal Data Protection Office, the imposed reminder will also fulfill its preventive function, duly preventing future violations of the provisions on the protection of personal data by the Company and other data administrators.

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

2022-07-18