THE CHAIRMAN OF PERSONAL DATA PROTECTION

Warsaw, 23

January

2019

DECISION

ZWAD.405.158.2018

Based on Article. 104 § 1 of the Act of 14 June 1960 Code of Administrative Procedure (Journal of Laws of 2017, item 1257, as amended), hereinafter referred to as "the Code of Administrative Procedure", in connection with Art. 58 sec. 2 lit. e 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 (Journal of Laws No. UE.L.2016.119.1), hereinafter referred to as the "General Data Protection Regulation" or "GDPR", following an administrative proceeding regarding failure by YSA to notify a person affected by a personal data breach, contrary to Art. 34 sec. 2 GDPR, President of the Personal Data Protection Office.

orders to notify the data subject again of the breach of personal data protection in order to provide him with all the information required in accordance with art. 34 sec. 2 GDPR, i.e .:

a description of the possible consequences of a breach of personal data protection;

description of measures proposed by the administrator to remedy the breach of personal data protection, including measures to minimize its possible negative effects,

within 3 days from the date on which this decision becomes final.

Justification

On [...] July 2018, the attorney of Y. S.A., hereinafter also referred to as "T." or "Y. S.A. ", submitted a notification of a personal data breach to the President of the Personal Data Protection Office (finding: [...] July 2018, [...]). The breach consisted in sending an e-mail regarding one of the clients of Y. S.A. to the wrong e-mail address, as a result of which the customer's personal data was made available to an unauthorized person. In the notification, the administrator stated that the breach concerned such data as: name, surname, registration address identical to the correspondence address, PESEL number, telephone number, vehicle data (including VIN number, registration number and vehicle brand), proposal / policy number, date

birth, insured status. The administrator assessed the risk of violating the rights and freedoms of the data subject as medium and resigned from notifying this person about the event, indicating that after the breach, the administrator applied measures to eliminate the likelihood of a high risk of violation of the rights and freedoms of the data subject, in accordance with art. . 34 sec. 3 lit. b of the GDPR, i.e. he directed to the person who received data not related to him, information about the need to delete the e-mail and about the confidentiality of the data contained in this message and the prohibition of their use.

On [...] August 2018, the President of the Personal Data Protection Office pursuant to Art. 52 sec. 1 of the Act of May 10, 2018 on the Protection of Personal Data (Journal of Laws 2018.1000 of 2018.05.24 as amended), hereinafter referred to as the "Personal Data Protection Act", and Art. 34 sec. 4 GDPR, sent to Y. S.A. a request to notify the data subject about the breach of personal data protection and to provide that person with recommendations on how to minimize the potential negative effects of the breach. In his speech, the President of the Personal Data Protection Office indicated that the breach of confidentiality of such personal data as: PESEL number along with the name and surname, address, location data, as well as documentation regarding the insured vehicle causes a high risk for the rights and freedoms of a person in connection with the following exemplary threats:

obtaining by third parties, to the detriment of the data subject, loans from non-bank institutions;

gaining access to use the healthcare services due to the data subject;

exercising the civil rights of the data subject, e.g. using the data to vote on the funds of the citizens' budget;

extortion of insurance.

The President of the Personal Data Protection Office also indicated that the data subject should be provided with recommendations as to the measures he may take to protect himself against the negative effects of the breach and indicated the following examples:

the ability to set up an account in the credit and economic information system to monitor your credit activity;

suggesting that a person be careful about disclosing personal information to others, especially over the Internet or by telephone.

At the same time, the President of the Personal Data Protection Office called for notification to him within 30 days from the date of receipt of the request on the actions taken in connection with this request, i.e. notifying the person about the infringement in accordance with Art. 34 sec. 1 GDPR and providing it with appropriate recommendations, as well as about

actions taken to eliminate similar irregularities in the future.

In response to the above, Y. S.A. by a letter of [...] September 2018, it indicated that the data subject has knowledge of the event that has occurred, therefore, in the opinion of Y. S.A. pointless. According to T., the data subject repeatedly discussed the breach with Y. S.A. employees, was apologized for the incident and informed in detail about its course and cause. In addition, the data subject has been informed about the measures taken to minimize the negative effects of the breach, i.e .: sending a request to the recipient of the wrong address to permanently delete the message and informing the person that the message contained confidential data and that their use was prohibited.

Instructing the employee entering personal data provided by clients or potential clients about the need to carefully save the data of the recipient of the electronic message, and in case of doubts as to the content of such data - to clarify these doubts with the appropriate persons, including the client or potential client - the interlocutor, before sending a message containing personal data.

Correction of personal data in the system.

T. also indicated the actions taken to eliminate potential similar events in the future:

monitoring the situation related to the functioning of new processes launched under the GDPR, including the process of handling incidents of personal data breaches;

organizing workshops to exchange experiences and implement ad hoc solutions to reduce the risk of leaks (e.g. verification of the e-mail address with the customer during contact, mandatory spelling of e-mail addresses by YSA employees so that the customer can confirm its correctness or instructing employees to e-mails were filled in legibly, in block letters);

launching a project aimed at introducing systemic solutions to eliminate the occurrence of breach incidents, including employee education and problem mitigation;

steps have been taken to cooperate with the processor which largely generates breaches of personal data protection Y. S.A.

In conclusion, T. assured that he made every effort to maintain the confidentiality of the data obtained in the course of his activities.

[...] October 2018 pursuant to Art. 61 § 1 and 4 of the Code of Administrative Procedure in connection with Art. 58 sec. 2 lit. e) GDPR, administrative proceedings were initiated regarding the failure to notify by Y. S.A. the data subject on the breach of personal data protection in accordance with art. 34 GDPR.

By letter of [...] October 2018 (reference number [...]), T. informed that the data subject had been notified of the breach by telephone on [...] July 2018. At the same time, T., supplemented by [...] October 2018 (reference number [...]) provided the anonymised content of the notification, in which it indicated to the person what the breach of personal data protection was based on and provided an e-mail address to the personal data protection officer. It also informed that in order to minimize the negative effects of the breach of personal data protection, it asked the recipient of the incorrect address to delete the message permanently and corrected the incorrect personal data in the Y. S.A. system. It also advised employees entering personal data of customers or potential customers about the need to carefully record the data of the recipient of an electronic message, and in case of doubts as to the content of these data - to clarify these doubts with the appropriate persons before sending a message containing personal data and train employees in the field of compliance with principles of personal data protection. As regards the description of the possible consequences of the breach, T. indicated that "a third party may use your data".

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

Art. 34 sec. 1 of the General Data Protection Regulation indicates that in a situation of high risk to the rights and 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 GDPR, the correct notification should:

describe the nature of the personal data breach in clear and plain language;

contain at least the information and measures referred to in Art. 33 paragraph 3 lit. b, c and d of the GDPR, that is:

the name 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 a breach of personal data protection;

a description of the measures taken or proposed by the controller to address the personal data breach, including, where appropriate, measures to minimize its possible negative effects.

Notification sent on [...] October 2018 by Y. S.A. to the data subject was not correct as it did not contain a sufficient description of the possible negative consequences of the personal data breach to which the data subject could be exposed and the measures proposed by the controller to minimize the negative effects of the breach. Thus, it did not meet the conditions set out in Art. 34 sec. 2 in connection with Art. 33 lit. c and d GDPR.

The President of the Personal Data Protection Office, using his powers under Art. 52 sec. 1 of the Act on the Protection of

Personal Data, sent to Y. S.A. a speech aimed at ensuring effective protection of personal data. It indicated that the breach of confidentiality of data such as the PESEL number along with the name and surname, address, location data, as well as documentation regarding the insured vehicle causes a high risk for the rights and freedoms of the person, requires the person to be notified of the breach in order to inform, inter alia, . about the possible negative effects of the violation and the actions (measures) it may take to protect against the negative effects of the violation. In his speech, the President of the Personal Data Protection Office (UODO) advised the controller for what possible, unauthorized purposes the data may be used and about which, exemplary security measures, the person should be notified in order to protect against the negative effects of the breach.

In a situation where, as a result of a breach of personal data protection, there is a high risk of violating the rights and freedoms of natural persons, the controller is obliged under Art. 34 sec. GDPR, 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 and freedoms, also the data subject. The controller should fulfill this obligation as soon as possible. Recital 86 of the GDPR explains: "The controller should inform the data subject without undue delay of a breach of personal data protection where this may result in a high risk of violation of 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 immediate risk of harm will require the immediate notification of data subjects, while the implementation of appropriate measures against the same or similar breaches of data protection may justify subsequent notification. '

Y. S.A. it has informed the data subject many times (by phone and by letter) about the circumstances of the breach. However, in the notification sent to the data subject on [...] October 2018, she did not indicate to the person possible ways of unauthorized use of the data, limiting herself only to the statement "As a consequence of the above, a third party may use your data". The person's notification did not include the indication of measures to minimize the possible negative effects of the violation.

In his speech of [...] August 2018, the President of the Personal Data Protection Office indicated the possible consequences of a breach of personal data protection that could be disclosed to the data subject. Despite the resulting from Art. 34 sec. 3 in connection with Art. 33 section 3 lit. c GDPR, the obligation to provide the data subject with a description of the possible consequences of the breach, T. did not provide this person with a description of the consequences suggested by the supervisory authority, or a description of any other consequences of the breach of personal data protection.

Apart from the obligation to provide the data subject with a description of the possible consequences of the breach, T. was also obliged under Art. 34 sec. 3 in connection with Art. 33 section 3 lit. d GDPR to provide the data subject with a description of the measures proposed by the controller to remedy the data protection breach, including measures that the person may take to minimize the possible negative effects of the breach. T. did not fulfill this obligation and did not provide the person with any recommendations in this regard.

Art. 34 sec. 1 and 2 GDPR is aimed not only at ensuring the most effective protection of the fundamental rights and freedoms of data subjects, but also the implementation of the principle of transparency, which results from the provision of art. 5 sec. 1 lit. a GDPR. (see.Chomiczewski Witold [in:] GDPR. General Data Protection Regulation. Comment, edited by E. Bielak-Jomaa, D. Lubasz, Warsaw 2018). Proper fulfillment of the obligation set out in this provision is to provide the data subject - quickly and transparently - with information about the breach of personal data protection, together with a description of the possible consequences of the breach of personal data protection and the measures that may be taken to minimize it. possible negative effects. Acting in accordance with the law and showing concern for both the safety of insurance products and the interests of the data subject, T. should therefore, without undue delay, provide the data subject with the best possible protection of his rights and freedoms at risk resulting from a breach of personal data protection. To achieve this goal, it is necessary to at least indicate, inter alia, the information listed in Art. 34 sec. 2 in connection with Art. 33 paragraph. 3 lit. c and d of the GDPR, from which this obligation was not fulfilled by T.

In view of the above, 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 Office for Personal Data Protection (address: Office for Personal Data Protection, ul. Stawki 2, 00-193 Warsaw). A proportional fee should be filed against the complaint, in accordance with Art. 231 in connection with Art. 233 of the Act of August 30, 2002, Law on proceedings before administrative

courts (Journal of Laws of 2018 1302, i.e. of 2018.07.05). 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.

2019-04-10