THE CHAIRMAN OF PERSONAL DATA PROTECTION

Warsaw, on 20

November

2018

DECISION

OUTPUT 405.29.2018

Based on Article. 104 § 1 of the Act of June 14, 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 pursuant to 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 (date of 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. Sending an e-mail with the customer's personal data was a one-off incident. 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

registration number and VIN number), policy number. 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 GDPR, i.e. sent to the person who received data not related to it, 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 [...] July 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 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 him to be notified within 30 days from the date of receipt of the request about 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. in a letter of [...] August 2018, she asked for reconsideration of the position of the President of the Personal Data Protection Office presented in her speech, because in the opinion of T. there was no high risk of violation of the rights and freedoms of the data subject in the case at hand, because:

data of only one person was disclosed to only one other person (wrong addressee). If the customer base were made public on the Internet, access to the data would be wide.

the duration of the violation was short (only a few days passed from the violation to the time of its finding, and in such cases, the wrong addressee was always asked to delete the message). A high risk could arise if the time between the breach and its finding were weeks, months, years, or still ongoing.

the scope of data did not include specific data categories or the series and number of the identity document.

T. also questioned the high probability of negative consequences for the data subject through the unauthorized use of his data for example purposes indicated by the President of the Personal Data Protection Office, pointing out that:

with regard to the probability of obtaining loans to the detriment of the data subject from non-bank institutions - it is not possible to obtain a loan from such institutions, because loan institutions are required to identify the customer also by determining the series and number of the identity document;

with regard to gaining access to health care services - the use of such services requires presentation of an identity document or only giving the name and surname. In the opinion of T., the use of such benefits does not constitute a high risk of violating the rights and freedoms of the data subject, and may at best generate costs on the part of the state for providing the benefit to an uninsured person;

with regard to the use of data to vote in voting on the funds of the civic budget - voting requires only giving the name and surname and place of residence of the person. In T.'s opinion, if someone wants to use someone else's identity for the above-mentioned purpose, they can do so by impersonating, for example, a neighbor, without obtaining his additional data apart from the name and surname;

with regard to extortion of insurance - it is not possible to use, for example, the rights of another person in the field of motor insurance, because in the event of a breakdown, a driving license is required to verify the rights, and the insured vehicle must

also participate in the event. In the case of other insurance contracts, the company is obliged, at the time of payment of the insurance, to identify the persons entitled under the insurance contract on the basis of a document confirming identity.

T. also indicated that it had applied corrective measures, i.e.

directing an incorrect address to the addressee to delete the message permanently, along with a request for feedback confirming its deletion.

instructing employees who enter 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 - clarification of these doubts with the client or a potential client before sending the message containing personal data;

rectification of personal data in the system if it has been incorrectly recorded.

At the same time, T. asked the President of the Personal Data Protection Office to change his position in the scope indicated in the case, which is very likely also indicated by the Personal Data Protection Office to other administrators and the media. It indicated that creating citizens' awareness is as important as preventing such situations. However, Y. S.A., as "an insurance company, is very anxious for citizens to associate insurance products with safety".

Due to the controller's failure to comply with the recommendations of the President of the Personal Data Protection Office on [...] August 2018 to Y. S.A. a letter of order to comply with the withdrawal of [...] July 2018 was sent.

In response to this request, in a letter of [...] September 2018, T. indicated that it was not possible to meet the request of the supervisory authority to notify the data subject about the breach of personal data protection, because the withdrawal from Art. 52 sec. 1 of the Act on the Protection of Personal Data, in which such an obligation was imposed on T., is not an administrative act, does not have an imperative character and does not constitute a measure to exercise the competences of the President of the Personal Data Protection Office. Moreover, Y. S.A. argued that the addressee of the petition has no possibility to question the theses contained in the petition through administrative or court-administrative proceedings.

[...] 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. SA. the data subject on the breach of personal data protection in accordance with art. 34 GDPR.

By letter of [...] October 2018, Y. S.A. informed the President of the Personal Data Protection Office that it decided to notify the data subject of the breach of personal data protection and that the notification would take place no later than [...] October 2018.

On [...] October 2018 (date of receipt by the Personal Data Protection Office) T. informed that the data subject was notified of the breach on [...] October 2018. At the same time, T. provided the anonymised content of the notification, in which he indicated to the person what the breach of personal data protection was and provided an e-mail address to the data protection officer personal. 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 e-mail address 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 such data - to clarify these doubts with the appropriate persons before sending the message containing personal data. As regards the description of the possible consequences of the breach, T. indicated that "as a result of the breach of personal data protection, 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 is not correct as it does not contain a sufficient description of the possible negative consequences of the personal data breach to which the data subject may be exposed and the measures proposed by the controller to minimize the negative effects of the breach. Thus, it does 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. decided to notify the person of the infringement only after the initiation of the administrative procedure in the present case (which took place on [...] October 2018). 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 to the statement "As a consequence of the above, the 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 [...] July 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. It should be noted that, contrary to the opposing position of T., it is possible for third parties, to the detriment of the data subject, to obtain loans from non-banking institutions, because many such institutions - in order to attract as many customers as possible, make it possible to obtain a loan or credit facility easily, quick way, e.g. via the Internet or by phone without the need to present an identity document.

Data such as name and surname together with the PESEL number can also be used to gain access to the use of health care services and view data on the health status of a person, because often access to patient registration systems can be obtained by phone confirming your identity with a PESEL number.

Providing the name, surname and PESEL number is in most cases sufficient to vote for a selected citizenship project under the participatory budget and so far there have been cases of impersonating other persons in order to obtain additional votes. Most local authorities allow you to vote using an electronic form, and the form of authentication of the voting person's identity is to indicate the name, surname and PESEL number in the voting form. In many communes, voters in the traditional form (paper voting cards) are also required to provide their name, surname, place of residence and PESEL number.

The personal data of another person may also be used to defraud insurance or insurance funds, which may have negative consequences for the data subject in the form of problems with an attempt to assign him responsibility for the fraud.

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