THE CHAIRMAN OF PERSONAL DATA PROTECTION

Warsaw, 27

March

2019

DECISION

ZWAD.405.1383.2018

Based on Article. 104 § 1 of the Act of 14 June 1960 Code of Administrative Procedure (Journal of Laws of 2019, item 60, as amended), in connection with Art. 34 sec. 4 and 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 UE. L. 2016.119.1, as amended), after the President of the Personal Data Protection Office conducted administrative proceedings regarding failure to notify X. Sp. z o.o., the data subject, on a breach of data protection,

I order notification of the data subject about the breach of personal data protection in order to provide him with the information required in accordance with 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 (Journal UE. L. 2016.119.1 as amended), i.e .:

description of the nature of the personal data breach;

the name 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 a breach of personal data protection;

description of measures taken or proposed by the administrator to remedy the breach - including measures to minimize its possible negative effects,

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

Justification

On [...] November 2018, the proxy of X. Sp. z o. o., hereinafter also referred to as the "administrator" or "the Company", submitted to the President of the Personal Data Protection Office, hereinafter also referred to as the "President of the Personal

Data Protection Office", a notification of a breach of personal data protection, which took place on [...] October 2018. In the notification, the Company indicated that she did not meet the 72-hour deadline for reporting by an employee error, who classified the event as a complaint and not a breach of personal data protection. The violation consisted in sending the wrong customer an order from another administrator's customer. The company stated in the notification that "the photobook containing family and pregnancy photos of the affected person was sent to another person" and that "(...) in the middle of the envelope, in addition to the photos, was the label of the relevant addressee of the order (...)". According to the notification, the violation concerned the following personal data: customer's name and surname, order number, data of one of the persons in the photo in the scope: name and surname, date of birth, gender and images of the customer and her family members, friends and child (in the period from births up to 3 years of age) from everyday life, family meetings and other events, including baptism, included in 126 photos. Moreover, X. Sp. z o.o. indicated in the notification of the violation that the event concerned specific categories of data, i.e. health data and data on religious and philosophical beliefs.

The administrator resigned from notifying the client about the event, in the manner specified in Art. 34 sec. 1 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 (Journal EU. L. 2016.119.1, as amended), hereinafter referred to as "Regulation 2016/679", indicating that after the breach, it applied measures to eliminate the likelihood of a high risk of violating the rights and freedoms of the data subject, in accordance with Art. 34 sec. 3 lit. b of the Regulation 2016/679, i.e. he immediately picked up photos from an unauthorized person and explained the situation with the client whose photos had been disclosed, justifying the situation with an error of the person preparing the order for shipment. The unauthorized person reported the incident to the Company and the customer who could be contacted thanks to the information contained on the address label included in the parcel with photos.

With the withdrawal of [...] December 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 of 2018, item 1000, as amended), hereinafter referred to as the "Personal Data Protection Act" and Art. 34 sec. 4 of Regulation 2016/679, called the controller 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. He indicated that the infringement consisted in issuing the client an order from another client, containing photos with the image of the client, family members of her friends and child (from birth to 3

years of age) and personal data, i.e. name and surname, order number, date of birth.

The President of the Personal Data Protection Office pointed out that in a situation where, as a result of a breach of personal data protection, there is a high risk of violation of the rights and freedoms of natural persons, the controller is obliged to notify the data subject about such a breach without undue delay. Pursuant to Art. 34 (4) of the Regulation, if the controller has not yet notified the data subject about the breach of personal data protection, the supervisory authority may request it or may state that one of the conditions referred to in para. 3 of this article. He indicated that the proper fulfillment of the obligation specified in Art. 34 of Regulation 2016/679 is to provide the data subject with quick and transparent information about the breach of personal data protection, along with a description of the nature of the breach, a description of its possible consequences and measures that can be taken to minimize its possible negative effects.

Later in his speech, the President of UODO mistakenly indicated that the violation concerned the PESEL number and the child's first and last name. Regardless of this error, however, he indicated - adequately to the violation in question - in which examples of unauthorized purposes the data of the person may be used, i.e .:

to extort funds from the immediate family, the so-called "Granddaughter method";

sharing the child's location data, which may endanger its safety;

discrimination of the child and his family by revealing a specific category of data, i.e. the child's health condition.

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, giving the following examples:

suggesting caution when disclosing personal information to others, especially over the Internet or by telephone;

caution by children and immediate family members against contacts with strangers.

In response to the request of the President of the Personal Data Protection Office, by letter of [...] January 2019, X. Sp. z o.o. informed that the Company did not notify the data subject because the level of risk related to the processing of his personal data was assessed by it as "the risk of violating the rights and freedoms of a natural person" and not "high risk of violating the rights and freedoms of a natural person". X. Sp. z o.o. that in the event of a reported violation, the PESEL number or the child's place of residence were not disclosed. In view of the above, the breach of the confidentiality of the data indicated in the notification may not lead to the consequences indicated in the request. Therefore, in the opinion of the Company, it is not

possible to use the disclosed data to obtain funds from the closest family, the so-called "Granddaughter method" or to determine the location of the child. X. Sp. z o.o. He also argued that the disclosed data did not contain information about the child's health (e.g. medical records), but only presented a pregnant client, which consequently did not lead to a high risk of violation of rights and freedoms. The company also emphasized that the parcel was immediately collected from an unauthorized person, the situation with the client was clarified and new rules regarding the photo packaging system were implemented. Taking into account the above circumstances, in the opinion of the Company, there is no need to notify the data subject about the breach.

Due to the failure to notify the data subject about a breach of data protection pursuant to art. 61 § 1 and 4 of the Act of 14 June 1960 Code of Administrative Procedure (Journal of Laws of 2019, item 60, as amended), hereinafter referred to as "the Code of Administrative Procedure", in connection with Art. 58 sec. 2 lit. e of the Regulation 2016/679, the President of the Personal Data Protection Office initiated administrative proceedings. On [...] February 2019, the Office for Personal Data Protection received a letter from the Company, in which it indicated that, in accordance with the adopted personal data protection policy, it had implemented and applies: "Procedure for the assessment and notification of personal data breaches", hereinafter also referred to as The "procedure" attached to the above-mentioned writings. The procedure followed by the Company was developed on the basis of the recommendations concerning the methodology for assessing the seriousness of the breach issued by the European Union Agency for Network and Information Security, hereinafter also referred to as "ENISA". On this basis, the Company assessed the infringement taking into account:

the context of data processing (PM) - the assumed value is 3; The company determined that the subject of the breach is basic data (value 1), which, however, may be a source of information about health or sexual life data, and therefore increased the value of the data processing context by 2;

ease of identification (I) - assumed value equal to 0.75; The company determined that the name and surname of the subject of the infringement are carried by many people in Poland, but due to the image (the photo is clear, which allows for identification, but it is not connected with data that would allow for direct identification of the person, e.g. address, telephone number), the assumed value was 0.75;

circumstances of violation (ON) - the assumed value was 0.25; The company determined that the confidentiality of the data has been lost, and the data has been disclosed to a specific number of identified recipients.

The administrator assessed the violation according to the formula P = KP × I + ON, giving the following result: 3 × 0.75 + 0.25 = 2.5. Thus, the Company assessed the level of the infringement as "medium", which, according to the criteria it adopted, means that "data subjects may encounter significant inconvenience that can be overcome despite the difficulties". The company also referred to Annex B of the Guidelines of the Article 29 Working Party on the reporting of personal data breaches in accordance with Regulation 2016/679 (WP250 rev. 01), hereinafter also referred to as the "Guidelines of the Article 29 Working Party", where examples of breaches of protection are indicated. personal data that can help distinguish between risk and high risk to the rights and freedoms of individuals. It stated that the risk related to the breach covered by the report in question differed from the examples of high-risk breaches set out in that annex, and in particular did not lead to similar consequences and afflictions for data subjects. Therefore, as she claims, she rightly assessed that there is no high risk of violating the rights and freedoms of an individual. The company reiterated that in the speech of the President of the Personal Data Protection Office of [...] December 2018, the assumption was made contrary to the facts that the disclosed data included the PESEL number and the child's place of residence, which could not lead to the consequences indicated above. in the above-mentioned speech. In her opinion - in the case of the infringement in question, the circumstances referred to in Art. 34 sec. 3 lit. b of the Regulation 2016/679, because the Company took steps to limit the effects of the breach, i.e. it immediately picked up the parcel from an unauthorized person.

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 for 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 of Regulation 2016/679, 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 Regulation 2016/679, 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.

The President of the Personal Data Protection Office, using his powers, sent to X. Sp. z o.o. a speech aimed at ensuring effective protection of personal data. In his speech, he indicated that in a situation where, as a result of a breach of personal data protection, there is a high risk of violation of the rights and freedoms of natural persons, the controller is obliged to inform the data subject about such a breach without undue delay. Pursuant to Art. 34 sec. 4 of Regulation 2016/679, if the controller has not yet notified the data subject about the breach of personal data protection, the supervisory authority may request it or may state that one of the conditions referred to in para. 3 of this article. He indicated that the proper fulfillment of the obligation specified in Art. 34 of Regulation 2016/679 is to provide the data subject with quick and transparent information about the breach of personal data protection, along with a description of the nature of the breach, a description of its possible consequences and measures that can be taken to minimize its possible negative effects.

In the opinion of the President of the Personal Data Protection Office, disclosing to an unauthorized person the name and surname of the client, contact details with the place of residence of the client and her minor child, as well as other information disclosed in photographs presenting situations in the life of the family in the period from the child's birth to the child's 3 years of age, including those indicated by The company - of special categories of data, i.e. health data and data on religious and philosophical beliefs, causes a high risk of violating the rights and freedoms of natural persons, and the controller was obliged to notify the data subject about such a violation without undue delay.

In his speech of [...] December 2018, the President of the Personal Data Protection Office indicated the possible consequences of the breach of personal data protection that could be disclosed to the data subject, taking into account that the breach covered information about the child. Pursuant to recital 75 of Regulation 2016/679, the severity and likelihood of risk are affected by the fact that the data of vulnerable persons, in particular children, are processed. The President of UODO indicated, inter alia, the possibility of using the data covered by the infringement to obtain funds from the immediate family, the so-called "Granddaughter method". In the opinion of the President of the Personal Data Protection Office, the data could be used to extort funds through telephone contact with the reference to knowledge of the circumstances of the client's life. In addition, a set of information disclosed as a result of a breach, including the name and surname of the client, date of birth of the child, information on events and people related to the client and her child make it easier to take actions resulting in exposure or violation of the child's physical safety. Such scope of data may be made available to other unauthorized persons, regardless of the remedial actions taken by the administrator (e.g. receipt of a confidentiality declaration).

Due to the fact that the Company indicated that there had been disclosure of specific categories of data, i.e. health data and data on religious and philosophical beliefs, the President of the Personal Data Protection Office also indicated the risk of discrimination against the child and his family. Photographs as a specific information medium can reveal many physical, physiological, economic, cultural or social characteristics. Both photos of a pregnant woman and events recorded in photographs (pregnancy, childbirth, her baptism) could relate to the special sphere of the client's privacy, intimate aspects of her life and access to such information should not be granted to unauthorized persons who could use this information in a way leading to physical harm, property or non-pecuniary damage or discrimination.

In a letter received by the Personal Data Protection Office on [...] February 2018, the Company indicates that it has implemented and applies the "Procedure for the assessment and notification of personal data breaches", developed on the basis of recommendations on the methodology for assessing the seriousness of a breach issued by the Union Agency European Network and Information Security (ENISA). On this basis, the Company assessed the seriousness of the infringement at an average level which does not oblige the Company - in its opinion - to notify the data subject.

In the opinion of the President of the Personal Data Protection Office, the above procedure in the case at hand led the Company to incorrect conclusions, because the Company did not take into account all the factors provided for in this procedure. First of all, it should be noted that - in accordance with the above-mentioned European Union Agency for Network and Information Security recommendations - the scoring of the criteria proposed in the recommendations should be tailored to the specific circumstances in order to obtain the most appropriate and appropriate results. The criteria for assessing the seriousness of the breach proposed by the Agency include the context of data processing (PM) and ease of identification (I). In the opinion of the President of the Personal Data Protection Office (UODO), the company wrongly underestimated these criteria, contrary to the threats indicated in the occurrence.

Both the ENISA methodology and the Company's procedure (Annex E to the procedure, point 3.3) indicate that the final score for the processing context (PM) may be increased or decreased depending on the occurrence of various factors, including the nature of the data and the scale of the data breached (for the same person).

The company rightly assumed that the nature of the disclosed data may be a source of information about health or sexual life data, therefore it increased the value of the data processing context by 2 points. However, another circumstance indicated in the Company's procedure was omitted, which, in the opinion of the President of the Personal Data Protection Office, influences

the increase of this score in accordance with the adopted procedure, i.e. "due to its characteristic features, the information may be of particular importance to the safety of that person or his or her physical condition or mental health (eg vulnerable groups, children) ”(Appendix E of the Procedure, point 3.4). The scale of the data breached (for the same person) is also a factor that has not been taken into account by the Company, and should support accepting the above-mentioned circumstances. As indicated by ENISA and the Company's procedure, this is a factor that may increase the final point value of the processing context (PM) due to the increase in the amount of breached information, and this amount should be considered both in terms of time (126 photographs covering the period from birth to the age of 3) and content (the information disclosed includes people participating in everyday life situations and family meetings such as baptism).

Ease of identification (I), another criterion that the Company took into account when assessing the seriousness of the infringement, was assessed at the level of 0.75 points. X. Sp. z o.o. It also indicates that "the photo is clear, allows for identification, but is not combined with data that allows the direct identification of the person, eg address, telephone number". The adopted arguments contradict the facts reflected in the infringement notification, in which the Company indicated that the photos showed the image of the client and "(...) in the middle of the envelope, apart from the photos, there was a label of the appropriate addressee of the order (...)", and therefore data allowing direct establishing the identity of a person. Due to the above, the Company should adopt the maximum level of identification, which, according to the adopted procedure, means that "identification is possible directly with the use of the data being breached without the need to conduct other tests to determine the identity of a given person" (Annex E to the procedure, point 4.6).

In the proceedings in question, the Company referred to Annex B of the Guidelines of the Article 29 Working Party on reporting personal data breaches in accordance with Regulation 2016/679 (WP250 rev. 01) and indicates that the risk related to the breach covered by its notification differs from the examples of breaches, with a high degree of risk, indicated in this appendix, and in particular does not lead to consequences similar in nature and to afflictions for data subjects. Therefore, he claims, he rightly assessed the risk as "a risk of violating the rights and freedoms of a natural person" and not "a high risk of violating the rights and freedoms of a natural person".

It is impossible to share this position of the Company. As the Article 29 Working Party points out in its guidelines, Annex B provides a non-exhaustive list of examples of situations where there is a high probability that a breach would pose a high risk to individuals, and therefore where a controller is required to notify individuals, whom the data concern. In addition, the

Guidelines emphasize that certain types of personal data may appear "at first glance" harmless and carefully consider what information such data may reveal about the individual affected by the breach and recommends that, in case of any doubts, the controller he has made a notification (by the supervisory authority and / or data subjects), even if such caution could turn out to be excessive. The guidelines also indicate that if the controller decides not to notify a natural person about a breach, the supervisory authority may require it if, in its opinion, the breach may result in high risk for natural persons, as indicated in Art. 34 sec. 4 of the Regulation 2016/679.

Art. 34 sec. 3 letter b of the Regulation 2016/679 indicates that the notification referred to in para. 1 is not required if the controller has then applied measures to eliminate the likelihood of a high risk of violation of the rights or freedoms of the data subject referred to in para. 1. This situation concerns the controller taking remedial actions after the occurrence of a personal data breach, which results in eliminating the likelihood of a high risk of violating the rights or freedoms of the data subject.

X. Sp. z o.o. in the notification of the violation, in the letter in response to the request of the President of the Personal Data Protection Office and in the letter received by the Personal Data Protection Office on [...] February 2019, he emphasizes that the circumstances referred to in Art. 34 sec. 3 lit. b of the Regulation 2016/679, because the parcel was immediately collected from the authorized person and the situation with the customer whose photos were disclosed was explained (by explaining the reason for the delay - error of the person preparing the order for shipment).

However, as indicated by the Article 29 Working Party in its Guidelines, whether the controller knows that personal data is in the hands of persons whose intentions are unknown may be relevant to the level of the potential risk of violating the rights or freedoms of natural persons. in this respect, the perspective of the data subjects should be taken and it is from this perspective that the degree of severity in the event of a risk materializing should be assessed.

In the event of delivering erroneous correspondence to a person known to the administrator, e.g. to another customer of the administrator who informed about the mistake of the Company, there is no guarantee that the intentions of such a person - now or in the future - will not change, bearing in mind that the possible consequences of using the disclosed categories of data may be significant. Such an assessment, in particular, does not release the controller from the obligation to take any actions to minimize the potential risk of violating rights or freedoms. Recital 85 of the preamble to Regulation 2016/679 indicates that "in the absence of an appropriate and quick response, a breach of personal data protection may result in physical, property or non-material damage to natural persons, such as loss of control over own personal data or limitation of rights, discrimination,

identity theft or falsification, financial loss, unauthorized reversal of pseudonymisation, breach of reputation, breach of confidentiality of personal data protected by professional secrecy or any other significant economic or social damage. '

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 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 and freedoms, also the data subject. The controller should fulfill this obligation as soon as possible. Recital 86 of the preamble to 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 measures. 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.

Art. 34 sec. 1 and 2 of Regulation 2016/679 is intended not only to ensure the most effective protection of the fundamental rights and freedoms of data subjects, but also to implement the principle of transparency, which results from the provision of 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 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 care for the interests of the data subject, X. Sp. z o.o. it should, without undue delay, provide the data subject with the best possible protection of personal data. To achieve this goal, it is necessary to at least indicate the information listed in Art. 34 sec. 2 of Regulation 2016/679, from which the administrator did not fulfill.

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

I would like to inform you that pursuant to Art. 41 of the Code of Administrative Procedure, in the course of the proceedings,

the parties and their representatives and proxies are required to notify the public administration body of any change of their address. In the event of neglect of this obligation, the delivery of the letter to the current address has legal effect.

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.

2019-04-26