THE CHAIRMAN OF PERSONAL DATA PROTECTION

Warsaw, on 21

June

2021

DECISION

DKN.5131.3.2021

Based on Article. 104 § 1 of the Act of 14 June 1960 Code of Administrative Procedure (Journal of Laws of 2021, item 735), art. 7 sec. 1 and art. 60, art. 101 and art. 103 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), art. 58 sec. 2 lit. e) and i), Art. 83 sec. 1 and sec. 2, art. 83 sec. 4 lit. a) in connection with Art. 33 paragraph 1 and art. 34 sec. 1, 2 and 4 of Regulation 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 data protection) (Journal of Laws UE L 119 of 04/05/2016, p. 1, Official Journal of the European Union L 127 of 23/05/2018, p. 2 and EU Official Journal L 74 of 04/03/2021, p. 35), hereinafter also referred to as "Regulation 2016/679", after administrative proceedings initiated ex officio regarding the failure to notify the personal data breach to the President of the Personal Data Protection Office and the lack of notification of the breach of personal data protection of the affected person by Sopot Towarzystwo Ubezpieczeń ERGO Hestia SA [...], President of the Personal Data Protection Office,

1) finding a breach by Sopockie Towarzystwo Ubezpieczeń ERGO Hestia S.A. [...] the provisions of Art. 33 paragraph 1 of Regulation 2016/679, consisting in not reporting to the President of the Office for Personal Data Protection the breach of personal data protection without undue delay, no later than 72 hours after the breach has been found and art. 34 sec. 1 of Regulation 2016/679, consisting in the failure to notify about a breach of personal data protection, without undue delay, the data subject is imposed on Sopockie Towarzystwo Ubezpieczeń ERGO Hestia S.A. [...] an administrative fine in the amount of PLN 159,176 (in words: one hundred and fifty-nine thousand one hundred and seventy-six zlotys),

2) orders Sopockiem Towarzystwo Ubezpieczeń ERGO Hestia S.A. [...] notification of the data subject about the breach of personal data protection in order to provide him with the information required pursuant to Art. 34 sec. 2 of the Regulation 2016/679, i.e .:

a) description of the nature of the personal data breach;

(b) the name and contact details of the data protection officer or designation of another contact point from which more information can be obtained;

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

d) 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 of its delivery.

Justification

The President of the Personal Data Protection Office, hereinafter also referred to as the "President of the Personal Data Protection Office", on [...] September 2020, received a notification of a personal data breach made by X Sp. z o.o., hereinafter also referred to as X. The breach consisted in sending on [...] September 2021 by e-mail to the wrong recipient by X, who is the processor (in connection with the concluded agency agreement) for Sopockie Towarzystwo Ubezpieczeń ERGO Hestia S.A. [...], hereinafter also referred to as the "Company", analysis of insurance needs containing personal data in the form of name and surname, the administrator of which was X, and an insurance offer containing personal data in the form of: name, surname, PESEL number, city, postal code, information about the subject of insurance (house), information about the insurance product [...], sum insured / guaranteed sum in the amount of PLN 300,000 and PLN 200,000 depending on the variant and the amount of the premium (PLN 162 and PLN 49 depending on the selected variants), the administrator of which of data is Sopockie Towarzystwo Ubezpieczeń ERGO Hestia SA

In the notification of the breach of personal data protection, X informed that although he was the administrator only in terms of the name and surname, due to the remaining data, which had also been disclosed, he decided to report the breach of personal data protection to the President of the Personal Data Protection Office. As a result of a mistake, employee X entered an incorrect e-mail address, so the correspondence was forwarded to a third party. In addition, "a third party confirmed the deletion of incorrectly received documents as soon as it became aware that they were intended for someone else. X has received a written declaration submitted by a third party confirming the above ". The breach concerned current customer X looking for housing insurance. The sent notification of a breach of personal data protection also showed that, in addition to documents containing personal data, the data administrator of which was X, the sent message was accompanied by other -

containing personal data - documents in the form of offers and calculations of insurance companies. Moreover, information was provided that, in accordance with the role X plays in relations with insurance companies, i.e. as an entity processing data on behalf of these companies, it had notified them of the breach. Based on the above information, the President of the Personal Data Protection Office (UODO) requested X, in a letter of [...] November 2020, to provide written explanations and indicate the entities involved in the processing of data that the breach relates to and evidence confirming that these entities were notified of the breach. In reply, X informed by letter of [...] November 2020 that the entities participating in the processing of the data concerned by the notification were: Y S.A., Z S.A. and Sopockie Towarzystwo Ubezpieczeń ERGO Hestia S.A. [...]. The verification carried out by the President of the Personal Data Protection Office on the basis of the above information showed that in connection with the breach of personal data protection, which took place on [...] September 2020, consisting in sending correspondence containing personal data to the wrong recipient by X, notification of a breach of protection personal data pursuant to art. 33 paragraph 1 and 3 of Regulation 2016/679, as data controllers, were performed by Y S.A and Z S.A. However, the notification of a breach of personal data protection was not made by Sopockie Towarzystwo Ubezpieczeń ERGO Hestia S.A.

In connection with the above letter of [...] December 2020, the President of the Personal Data Protection Office, pursuant to Art. 58 sec. 1 lit. a) and e) of Regulation 2016/679, asked the Company to clarify whether, in connection with the sending of electronic correspondence to an unauthorized recipient, an analysis was made in terms of the risk of violating the rights or freedoms of natural persons, necessary to assess whether there was a breach of data protection resulting in the need to notify the President of the Personal Data Protection Office (Article 33 (1) and (3) of Regulation 2016/679) and the persons concerned by the infringement (Article 34 (1) and (2) of Regulation 2016/679). In the letter, the President of the Personal Data Protection Office indicated to the Company how to report the violation and called for explanations within 7 days from the date of receipt of the letter. In the letter in question, the President of the Personal Data Protection Office also provided the information that pursuant to Art. 33 paragraph 1 and 3 of Regulation 2016/679, in the event of a breach of personal data protection, the data controller shall, without undue delay - if possible, no later than 72 hours after finding the breach - notify the competent supervisory authority pursuant to Art. 55, unless the breach is unlikely to result in a risk of violation of the rights or freedoms of natural persons and that the notification submitted to the supervisory authority after 72 hours is accompanied by an explanation of the reasons for the delay. The company was also informed that the President of the Personal Data Protection

Office on [...] September 2020 received a notification of a personal data breach made by X, consisting in sending correspondence containing personal data to the wrong recipient. The notifying entity informed that the administrator of personal data, in terms of some of the data covered by the violation, is the Company, which was also notified by the processor, i.e. X, on [...] September 2020, about the violation of personal data protection.

In response to the above letter, the Company, in a letter of [...] December 2020, confirmed that a breach of personal data protection, consisting in disclosure of personal data to an unauthorized recipient, took place. It indicated that on [...] September 2020, the insurance intermediary X Sp. z o.o., which processes personal data on behalf of and for the benefit of the Company - on the basis of a written contract for entrusting the processing of personal data, which is an attachment to the agency contract, informed the Company about the breach. As evidence to the above-mentioned the letter was enclosed with the application of X Sp. z o.o., which was made to the Company. The submitted report shows that the breach of personal data protection consisting in sending correspondence containing personal data to the wrong recipient occurred on [...] September 2020, the breach was found on [...] September 2020, also on this day the Company was informed about the breach by processor. The breach occurred as a result of entering an incorrect e-mail address, and the document containing personal data named […] was sent to the wrong recipient. Further in the letter, the Company explained that in the above-mentioned The document contained personal data of the Company's client, such as: name, surname, PESEL number, city, postal code. As evidence, an insurance offer [...] was attached to the letter, which in addition to the above-mentioned personal data also included information about the insurance period, the subject of insurance (house), information about the insurance product [...], sum insured / guaranteed sum in the amount appropriate to the selected variant and the amount of premium for selected variants, respectively. An information clause was attached to the document [...], in which the Company informs, inter alia, that it is the administrator of personal data.

In addition, the Company indicated that on [...] September 2020 it asked the processor X Sp. z o.o. for proof / confirmation of deletion of mistakenly sent correspondence / personal data by an unauthorized person. In response of […] September 2020, processor (X) sent this declaration. Therefore, the Company attached a statement of the wrong recipient to the letter of [...] December 2020, which was a response to the supervisory authority's request. This statement shows that the wrong recipient deleted the messages sent to him by X and is not in their possession, and stated that he was not aware of the contents of the documents attached to the messages, as he had not read their contents before deleting the message. The declaration was

submitted on a ready form, in which the declaring person entered the following data: his name and surname, date and time in which he received the message, place and date of submission of the declaration. The declaration was signed by hand. In the lower right corner of the declaration form there is an annotation "X", while the date of submitting the declaration has visible traces of correction.

The company indicated that on [...] September 2020, an assessment was made in terms of the risk of violating the rights and freedoms of natural persons. Based on this assessment, the Company concluded that there was no breach resulting in the need to notify the President of the Personal Data Protection Office and the person whose personal data the breach concerns. The assessment was made using the personal data breach assessment form, which was a completed form along with the assessment methodology was sent as evidence with explanations. Moreover, the Company explained that it assessed the risk taking into account the categories of data concerned by the breach, in terms of the type and degree of their sensitivity, specific breach factors increasing or reducing the level of risk for the data subject, ease of identification of the person, breach circumstance in relation to the type of breach. As it results from the sent "Personal data breach assessment form", the Company assessing the seriousness of the potential effects of the breach in point 2.1. The "personal data criterion", when assessing the type and degree of sensitivity of personal data, indicated that the data subject to the violation belong to the category of "basic data" and "data on the behavior of a person or PESEL / ID document number", awarding a score of 2 points, but not belonging to the category of "personal data" financial "and" sensitive data or data relating to criminal convictions and prohibited acts ", for which, in accordance with the adopted methodology, a score of 3 and 4 points should be taken, respectively. At the same time, in the additional explanations regarding the data categories indicated in the table, for financial data, an example was indicated, inter alia, assets, transaction / payment history, invoices.

In point 2.2. The "specific factors criterion", in which, according to the adopted methodology, specific breach factors should be indicated that increase or decrease the level of risk for data subjects, such as: larger amounts of data on the same person (with a score of +1); specific characteristics of the data controller (with a score of +1 point); specific characteristics of the unit (with a score of +1 point); the nature of the data (with a score of +1 or -1); high importance of the negative effects of the violation for natural persons (with a score of +1); public availability of data (with a score - 1 point); incorrect data (with a result of -1 point) and other factors (with a result of +1 point or -1 point), the Company indicated the lack of factors reducing or increasing the risk, without awarding or subtracting points from this criterion.

In point 2.3. "The criterion of the possibility of identification", the Company defined the ease of identification as a limited possibility of identification, awarding 0.5 points in this criterion, on the scale: the incident does not constitute a breach of privacy (with a score of 0 points), a negligible possibility of identification (with a score of 0.25), limited possibility of identification (with a score of 0.5 points), high probability of identification (with a score of 0.75 points), maximum likelihood of identification (with a score of 1 point), with additional explanations regarding the levels of identification risk for "high "As an example," PESEL identification number in combination with other data, e.g. name and surname, e-mail address, or address of residence "was indicated, and for the" maximum probability of identification ", an example was indicated, inter alia, identification number or ID card number if data from the source database is also available (e.g. name, date of birth, photos, etc.).

In point 2.4. "Criterion of breach circumstances", the Company indicated breach of confidentiality with a limited number of known entities to whom the data was disclosed as the breach circumstances, awarding a score of 0.25 points on the scale: low probability with a score of 0 points, limited number of known entities, to whom the data were disclosed, with a score of 0.25 points, unknown number of entities to whom the data were disclosed, with a score of 0.5 points.

In point 2.5. "Other criteria" in the form were indicated the following criteria: intentional violation (with a score of +1 point), unreliable recipient (with a score of +1), a large number of people affected by the incident (with a score of +1 point), trusted recipient (with a score of +1) -1 point), data unavailable due to encryption (with a score of -1 point), a very small number of people affected by the incident (with a score of -1 point), other significant violation factors (with a score of +1 point or -1 point). As other criteria for the violation, the Company chose the factor: a very small number of people affected by the incident, subtracting 1 point. In the explanations for the above criterion, there is no explanation for the factor "Other material factors of the infringement".

Based on the above criteria, the Company assessed the severity of the effects of the infringement at 0.25 points, which in the adopted methodology is low risk on the scale of: no or low (if the result is less than or equal to 2), medium (if the result is less than or equal to 3) , high (if the score is less than or equal to 4), very high (if the score is greater than 4), where the data subject is not affected by the breach or may face some inconvenience that is easy to overcome - time spent re-entering information, irritation, irritation, etc., and additionally stressed, discomfort, time spent on clarifying the case and no other consequences of the breach due to the submission of a declaration on deletion of data and failure to read the data. For the

result of "high" assessment of potential impacts, the following description is included: "natural persons may face significant negative effects that they should be able to remedy, but with serious difficulties (misappropriation of assets / money, being blacklisted by financial institutions). , property damage, loss of job, summons, deterioration of health), and for the result "very high" assessment of potential effects, in the table of the assessment form, the following description is included: "natural persons may face very serious consequences or with consequences, which cannot be remedied (eg financial difficulties such as heavy debt or incapacity for work, long-term mental or physical discomfort, death, etc.) ".

The assessment of the degree of probability of the infringement effects was indicated as the neglected degree in the scale: neglected, limited, serious, maximum. On the other hand, the description for this degree shows that it does not seem possible for the threats (effects) to materialize. For the remaining levels of probability, the description was indicated as follows: limited - it seems difficult for the threats (effects) to materialize, serious - it seems possible for the threats to materialize, the maximum - it seems obvious that the threats (effects) will materialize.

The assessment of the effects of the breach, in the opinion of the Company, was also influenced by the fact that an unauthorized person submitted a written declaration of not familiarizing himself with the content of the attachment to the e-mail containing the data and about its permanent removal. Therefore, it was concluded that the breach is unlikely to result in a risk of violation of the rights or freedoms of natural persons.

Additionally, in the sent "personal data breach assessment form", under point 2.6. "Assessment of the severity of the potential effects of the breach", a formula was provided to calculate the severity of the effects of the breach [...], the administrator's calculation for the breach in question: [...] and (in "Explanations") the following examples of breach effects: loss of control over own personal data; limiting the possibility of exercising the rights under Art. 15-22 GDPR; limiting the possibility of exercising rights; discrimination; identity theft or fraud; financial loss; violation of good name; loss of confidentiality of personal data protected by professional secrecy; stress, discomfort; receipt of unsolicited correspondence; health hazard; life-threatening; the need to collect data again; limiting the possibility of exercising civic rights and services addressed to the general public (e.g. voting under the civic budget, online registration of visits to offices, etc.); setting up an internet account on someone else's (e.g. on social networking sites); impersonating another person or institution in order to defraud the person affected by the breach of additional specific information (e.g. login details, credit card details); using the data of the affected person to register a prepaid calling card that may be used for criminal purposes; third parties may try to obtain loans from non-bank institutions

using the data of the affected person, e.g. via the Internet or by phone, without the need to present an identity document; third parties may attempt to gain access to systems that support the provision of medical services and gain access to data on the health status of the affected person, because sometimes access to patient registration systems can be obtained by confirming their identity with a PESEL number; personal data may be used by a third party to attempt to obtain insurance fraud; third parties may try to conclude to the detriment of a person affected by the violation of civil law contracts, e.g. real estate lease; personal data may be used by third parties to conceal their identity, e.g. when receiving a ticket.

Due to the lack of notification of the breach of personal data protection to the President of the Personal Data Protection Office and the lack of notification of the breach of personal data protection of the person concerned, on [...] January 2021 the President of the Personal Data Protection Office initiated administrative proceedings against the Company.

In response to the notification about the initiation of administrative proceedings in this case, by letter of [...] February 2021, the Company sent additional explanations, in which it indicated, inter alia, that:

She turned to X Sp. z o.o. to ask the wrong recipient to submit an additional statement. [...] on January 2021, the wrong recipient made a declaration in which he informed that he permanently deleted and is not in possession of the message that was sent to him by X Sp. z o.o. and the content of the documents attached to the message is not known to him, because he has not read their content before deleting the above-mentioned messages and it is not possible to identify the person whose data was in the attached documents. In addition, he stated that he had re-verified the media and did not have any copies of the documents incorrectly served on him and that he was aware of the consequences of processing personal data without a legal basis.

In her opinion, she was not obliged to report the breach of personal data protection to the President of the Personal Data Protection Office or the obligation to notify the affected person about the breach, and thus did not breach the provisions of Art. 33 paragraph 1 and art. 34 sec. 1 - 2 of Regulation 2016/679, indicating that it had correctly assessed the risk caused by the breach of personal data protection and that the unauthorized recipient of the data made another statement that he had not read the personal data of a third party that had been accidentally sent to him and that he had deleted it.

When assessing the risk caused by data protection breaches, the Company implemented a breach assessment methodology developed on the basis of the ENISA methodology (European Union Agency for Cybersecurity).

Pursuant to the processing entrustment agreement concluded between the Company and X Sp. z o.o., employees of the

processor are required to encrypt documents containing personal data before sending them by e-mail; the breach in question was individual and resulted from human error; the person who sent the message to the wrong recipient with unencrypted attachments containing personal data was re-instructed to encrypt documents sent as attachments to the e-mail; The company received from X a statement from the employee that he is aware of the obligation to encrypt all documents that contain personal data and are transferred to customers or potential customers; asked X to present internal policies regarding the protection of personal data in correspondence and informed that it was carrying out an inventory of the use of cryptographic protection measures in the case of transferring personal data by electronic means and analyzing service procedures. In addition, the Company indicated that it regularly reminds its employees and agents about the obligation to inform the Company's data protection officer about a breach of data protection and about the obligations to secure personal data sent in e-mail correspondence.

The company has no legal or actual possibility to notify the person whose personal data is breached, because the company does not have current contact details of this person. The company concluded an agreement with the person whose personal data the breach concerns, but the place of residence of that person indicated in the policy in 2000 is O. However, in the calculation for 2020, the town of K. was given. Bearing in mind the above, the Company adopted that the address from the 2000 policy is no longer valid and it is unacceptable to send correspondence to this address. In addition, the Company has no way of obtaining the contact details of the affected person. In addition, she pointed out that the possible acquisition of this data by the Company would raise doubts from the point of view of compliance with the principle of data minimization, set out in Art. 5 sec. 1 lit. c) of Regulation 2016/679. The contact details are not needed by the Company for any purpose. The company may not try to obtain the affected person's address details just to notify them of the breach. In the opinion of the Company, this would be inconsistent with the principle of data minimization. On the other hand, the decision of the President of the Personal Data Protection Office ordering the Company to notify the data subject would be unenforceable on the day of its issuance and its unenforceability would be permanent, which would constitute a premise for the decision to be invalid.

Along with the explanations, the Company attached as evidence a copy of the contract for entrusting the processing of personal data, on the basis of which the Company, as the data controller, entrusted the processing of personal data to the agent - ie X Sp. z o.o. As results from § 7 point 3 of the attached copy of the contract, the agent undertakes, inter alia, "Assist ERGO Hestia in fulfilling the obligations set out in Art. 32-36 GDPR; in particular, the Agent undertakes to provide ERGO

Hestia with information and carry out instructions regarding the security measures applied to the entrusted personal data, cases of personal data breach and notifying the supervisory authority or data subjects about it, conducting a data protection impact assessment and carrying out prior consultations with the authority supervisory and implementation of the authority's recommendations ”.

The company re-analyzed the risk caused by the breach, using the form available on the website [...] published by O Sp. z o.o. On the basis of the analysis performed, the Company determined that it is not necessary to report the violation to the authority or notify the person affected by the violation, enclosing as evidence screenshots showing the result of the violation risk assessment carried out using the form on the page [...].

In order to find a breach by the Company of the provisions on the obligations to notify data breaches to the supervisory body and to notify data subjects about the breach, it would be necessary to state that the Company incorrectly assessed the risk caused by the breach in question. As the Company applies the infringement risk assessment methodology, in order to justify the infringement of the above-mentioned obligations would have to be identified as an error in the methodology itself or in its application in relation to the data protection breach in question (e.g. failure to take into account certain criteria, insufficient scoring of certain factors). However, in the present case, the authority has in no letter challenged either the methodology itself or its application to the infringement in question. Therefore, the authority did not explain what, in its opinion, the Company's error in assessing the risk caused by the violation in question was.

Provide additional clarifications on the criteria taken into account when assessing the risk of a breach to the rights and freedoms of data subjects, including that the scope of the data disclosed was very narrow; the disclosed data is not covered by insurance secrecy; there are no specific violation factors that increase or decrease the severity of the violation; the possible effects of the violation in question are possibly stress, discomfort, time spent on clarifying the matter - in the opinion of the Company, a breach of data protection would not result in effects such as identity theft, discrimination, financial losses, and the occurrence of negative serious consequences of the violation is theoretically possible, but in practice it is very unlikely. On the other hand, the ability to identify a natural person on the basis of the infringed data or in combination with other data that is, for example, publicly available or that can be easily obtained, is limited. The postal code and city do not constitute a complete address, which makes the person organically identifiable. It also pointed out that, even if the probability of identification were to be assumed as high as possible, the assessment of the seriousness of the infringement would still be 'low' due to the other

factors taken into account. The company assessed the importance of the potential breach to the negative impact of the breach on the data subject as low. On the other hand, she considered the probability of its occurrence ignored - bearing in mind that an accidental unauthorized recipient submitted a written declaration in this regard. The company took into account the criterion of the time in which the effects of the infringement could persist for a given person, indicating that from the date of the infringement (sending a message containing personal data to the unauthorized recipient) to the deletion of the data by the unauthorized recipient, a period of 5 days has elapsed.

The company took steps to search for information to identify the affected person. These data are not publicly available on the Internet, and there is no person with the indicated PESEL number in the Court and Economic Monitor or the National Court Register.

The company referred to the example of a breach presented in the guidelines of the European Data Protection Board 01/2021 (Guidelines of the European Data Protection Board 01/2021 on examples of data breach notifications, version 1.0), where in example 15 concerning the accidental sending of personal data to 15 unauthorized persons recipients, after sending the data, the sender (administrator) immediately contacted the unauthorized recipients and asked for the deletion of the data. In the opinion of the Company, the guidelines indicate that such a step can be considered a risk mitigating measure. In addition, as the Company explained, the Guidelines indicate that in the event of sending data to an unauthorized recipient, it is recommended to send a message to such recipient containing, inter alia, the need to delete the message containing personal data of third parties and that the recipient has no right to use the data.

The company referred to the publication of the Personal Data Protection Office entitled "Responsibilities of controllers related to breaches of personal data protection", arguing that the supervisory authority indicated that "a situation in which [...] correspondence (containing at least such data categories as name, surname and PESEL number) is provided to a person known or unknown to the administrator, as a rule it carries a high risk for data subjects ". The Company further indicated that, in its opinion, "this statement does not exclude the situation that, in certain circumstances, the risk assessment may be different (the authority uses the phrase" in principle) ". According to the Company, "such a different risk assessment should be applied to this data breach".

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

Pursuant to Art. 4 point 12 of Regulation 2016/679 "breach of personal data protection" means a breach of security leading to accidental or unlawful destruction, loss, modification, unauthorized disclosure or unauthorized access to personal data transmitted, stored or otherwise processed.

Art. 33 sec. 1 and 3 of Regulation 2016/679 provides that in the event of a breach of personal data protection, the data controller shall, without undue delay - if possible, no later than 72 hours after finding the breach - report it to the competent supervisory authority pursuant to Art. 55, unless it is unlikely that the breach would result in a risk of violation of the rights or freedoms of natural persons. The notification submitted to the supervisory authority after 72 hours shall be accompanied by an explanation of the reasons for the delay. The notification referred to in para. 1, must at least: a) describe the nature of the personal data breach, including, if possible, the categories and approximate number of data subjects, as well as the categories and approximate number of personal data entries affected by the breach; (b) include the name and contact details of the data protection officer or the designation of another contact point from which more information can be obtained; c) describe the possible consequences of the breach of personal data protection; (d) describe the measures taken or proposed by the controller to address the personal data breach, including, where appropriate, measures to minimize its possible negative effects.

In turn, art. 34 sec. 1 of Regulation 2016/679 indicates that in the event of a possible 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 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 paragraph 3 lit. b), c) and d) of Regulation 2016/679, i.e .:

a) the name and contact details of the data protection officer or designation of another contact point from which more information can be obtained;

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

(c) 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.

Reporting breaches of personal data protection by administrators is an effective tool contributing to a real improvement in the

security of personal data processing. When reporting a breach to the supervisory authority, the administrators inform the President of the Personal Data Protection Office whether, in their opinion, there is a high risk of violation of the rights or freedoms of data subjects, and - if such a risk occurred - whether they provided relevant information to natural persons affected by the breach. In justified cases, they may also provide information that, in their opinion, notification is not necessary due to the fulfillment of the conditions specified in Art. 34 sec. 3 lit. a) and b) of Regulation 2016/679. The President of the Personal Data Protection Office (UODO) verifies the assessment made by the controller and may - if the controller has not notified the data subjects - request such notification from him. Notifications of a personal data breach allow the supervisory authority to react appropriately, which may limit the effects of such breaches, because the controller is obliged to take effective measures to protect natural persons and their personal data, which, on the one hand, will allow for the control of the effectiveness of the existing solutions, and, on the other hand, for the assessment of modifications and improvements to prevent irregularities similar to those covered by the infringement. On the other hand, notifying natural persons about a breach enables them to be informed about the risk related to the breach and to indicate actions that these persons can take to protect themselves against the potential consequences of the breach. The obligation to notify a natural person about a breach does not depend on the materialization of negative consequences for such a person, but on the very possibility of such a risk. Thus, it enables a natural person to independently assess the infringement in the context of the possibility of materialization of negative consequences for such a person and to decide whether or not to apply remedial measures. On the other hand, the very assessment of the breach carried out by the controller in terms of the risk of violation of the rights or freedoms of natural persons, necessary to assess whether there has been a breach of data protection resulting in the need to notify the President of the Personal Data Protection Office (Article 33 (1) and (3) of Regulation 2016/679) and the persons concerned the infringement (Article 34 (1) and (2) of Regulation 2016/679) should be made through the prism of the person affected by the infringement.

When responding to the explanations of the Company, it should first be pointed out that in connection with the breach of personal data protection in question, consisting in unauthorized access to data and unauthorized disclosure of data as a result of sending correspondence containing personal data to the wrong recipient, not only the data indicated by the Company was disclosed in the letters of [...] December 2020 and [...] February 2021, i.e. the PESEL identification number along with the name and surname, city and postal code of the data subject, but also, as it follows from the attached letter from [...] December

2020, the insurance offer "Calculating ERGO [...]", containing the calculation of the insurance premium, data on the financial / property situation of the data subject in the form of: insurance period, subject of insurance (house), insurance product [...], sum insured / guarantee sum in the amount appropriate to the selected variant and the amount of the premium appropriate to the choice insurance variant, which were not included in the risk calculation carried out by the Company. Additionally, in view of the disclosure of the PESEL identification number, the date of birth should be included among the data covered by the infringement, because the eleven-digit PESEL identification number contains such information. It is also important to be able to easily determine the street of residence of the data subject, based on the disclosed zip code and city name.

It should be emphasized that the breach of confidentiality of data that occurred in the case in question, in connection with the breach of personal data protection consisting in sending a document with the calculation of the insurance premium to an unauthorized recipient, in particular data on the PESEL number along with the name and surname, city and postal code of the person data subject and information on the proposed insurance period, the subject of insurance (house), insurance product [...], sum insured / guarantee sum in the amount appropriate to the selected variant and the amount of the premium appropriate to the selected insurance variant, causes a high risk of violation of rights or freedoms natural persons. As indicated by the Article 29 Working Party (i.e. the Working Party on the Protection of Individuals with regard to the Processing of Personal Data, established pursuant to Article 29 of Directive 95/46 / EC of the European Parliament and of the Council of 24 October 1995, replaced in accordance with Article 68 of Regulation 2016/679 to the European Personal Data Protection Board, which, during the first plenary session of the EDPB, approved, inter alia, the below-mentioned guidelines) in the guidelines on reporting personal data breaches in accordance with Regulation 2016/679, hereinafter also referred to as "guidelines" : “This risk exists where the breach could lead to physical or material or non-material damage to the data subjects of the breach. Examples of such damage include discrimination, identity theft or fraud, financial loss and damage to reputation. " There is no doubt that the examples of damage cited in the guidelines, due to the scope of data covered by this personal data breach, including the PESEL number together with the name and surname and information about the financial / property status, may occur in the discussed case.

As a consequence, this means that there is a high risk of violating the rights or freedoms of the person affected by the violation, which in turn results in the emergence of the Company's obligation to report the violation of personal data protection to the supervisory body, in accordance with Art. 33 paragraph 1 of the Regulation 2016/679, which must contain the

information specified in art. 33 paragraph 3 of Regulation 2016/679 and notifying that person about the infringement, in accordance with art. 34 sec. 1 of the Regulation 2016/679, which must contain the information specified in art. 34 sec. 2 of Regulation 2016/679.

It should be noted that the disclosure of the personal data in question, in connection with the breach that occurred on [...] September 2020, and in particular such data as the PESEL registration number together with the name and surname and information on the financial / property status may be used or cause, for example, limiting the possibility of exercising civic rights and services addressed to the general public (e.g. voting under the civic budget, online registration of visits to offices, etc.); third parties may try to obtain loans from non-bank institutions using the data of the affected person, e.g. via the Internet or by phone, without the need to present an identity document; third parties may attempt to gain access to systems that support the provision of medical services and gain access to data on the health status of the affected person, because sometimes access to patient registration systems can be obtained by confirming their identity with a PESEL number; third parties may try to conclude to the detriment of a person affected by the violation of civil law contracts. It should be emphasized that the catalog of the consequences of the breach of personal data protection, which took place as a result of the breach in question for the data subject, is much wider, while the above-mentioned examples for a better illustration of the existing consequences were taken from the "impact assessment form", developed and sent by the Company together with explanations in a letter of [...] December 2020. Also, the Company itself, in its explanations of [...] February 2021, did not exclude the possibility of materializing significant negative consequences of the breach for the data subject.

It is irrelevant that the infringement did not apply to the address of the data subject, because such an address is not needed for the above consequences to materialize. It should be emphasized that the address of residence is determined by the data subject as the place where his or her life center is located, therefore it is a variable determined by the natural person to whom the data relate. Thus, it should not and does not constitute an element on the basis of which the correct verification of the data subject can be made, e.g. when concluding a contract or using the benefits to which they are entitled. Such an address may be freely indicated by a person who intends to use the disclosed data with malicious intentions. The lack of an exact postal or residential address may only frustrate the sending of unwanted correspondence. It may also make it difficult to intercept the correspondence for the purpose of authentication, but it does not eliminate this risk and other risks, the importance of which is significant for the data subject. On the other hand, it was important to disclose the PESEL registration number along with the

name and surname and information on the financial / property status, which, contrary to the position of the Company presented in the letter of [...] February 2021, not only makes it possible to easily identify the data subject, but most of all about the unequivocal identification of such a person. The above is determined by the essence of the identification number of the Universal Electronic System for Population Register. According to Art. 15 sec. 2 of the Act of 24 September 2010 on population records (Journal of Laws of 2021, item 510), this number uniquely identifies a natural person.

In the explanations contained in the letters of [...] December 2020 and [...] February 2021, the Company indicated that an assessment was made in terms of the risk of violating the rights or freedoms of natural persons. On its basis, the Company concluded that there was no breach of personal data protection resulting in the need to notify the President of the Personal Data Protection Office and the person whose personal data was breached. The assessment was made using the personal data breach assessment form, which was a completed form along with the assessment methodology was sent as evidence with explanations. In addition, the Company, in a letter of [...] February 2021, indicated that "in order to find a breach by the Company of the provisions on the obligations to notify data breaches to the supervisory authority (i.e. Article 33 (1) of the GDPR) and to notify the data subjects of breach of (Article 34 (1-2) of the GDPR), it would be necessary to state that the Company incorrectly assessed the risk caused by the violation in question. As the Company applies a breach risk assessment methodology, in order to justify failure to fulfill obligations under Art. 33 paragraph. 1 and art. 34 sec. 1-2 of the GDPR (due to an incorrect risk assessment), an error in the methodology itself or an error in its application in relation to the data breach in question should be indicated (e.g. failure to take into account certain criteria, insufficient scoring of some factors).

Considering the above, the President of the Personal Data Protection Office indicates that the Company should analyze the risk of violating the rights or freedoms of natural persons necessary to assess whether there has been a breach of data protection resulting in the need to notify the President of the Personal Data Protection Office and the persons affected by the infringement in a manner that is not focused on achieving the previously adopted result. The use of a form with an adopted assessment methodology is a tool to assist in carrying out such an assessment and, as an implemented technical and organizational measure, should enable a quick response to a breach. At the same time, it should be emphasized that the analysis of the risk of violation of the rights or freedoms of natural persons necessary to assess whether there has been a breach of data protection resulting in the need to notify the President of the Personal Data Protection Office (Article 33 (1) and (3) of Regulation 2016/679) and the persons affected by the violation (Article 34 (1) and (2) of Regulation 2016/679), carried

out by the Company on [...] September 2020, the completed form of which was attached to the Company's letter of [...] December 2020, was not performed correctly. As is clear from the personal data breach assessment form sent with the letter of [...] December 2020, the Company, when assessing the severity of the potential consequences of the breach in point 2.1. The "personal data criterion", when assessing the type and sensitivity of personal data, indicated that the data subject to the violation belong to the category of "basic data" and "data on the behavior of a person or PESEL / ID document number", giving a score of 2 points, but not "Financial data" and "sensitive data or data relating to criminal convictions and prohibited acts", for which, in accordance with the adopted methodology, the results of 3 and 4 points should be adopted, respectively. At the same time, in the additional explanations as to the data categories indicated in the table, for the data on "person's behavior or PESEL / ID number", examples were indicated: location data (GPS), preferences and habits, searched internet resources, network identifiers (cookies etc.), recorded calls / picture, PESEL number, ID number, and for "financial data", examples were indicated, inter alia, assets, transaction / payment history, invoices. Doubts are raised in particular by classifying the type and sensitivity of personal data of the PESEL number into the category entitled "data on the behavior of a person or PESEL / ID document number" with a result of Sensitivity to data such as location data (GPS), network identifiers (cookies, etc.), searchable internet resources. It should be pointed out that the disclosure of the PESEL number together with the name and surname, due to possible significant negative consequences for a natural person, may cause great stress or discomfort related to the possibility of materialization of negative threats (in the form of e.g. financial loss or identity theft), disrupting the person's sense of security, as is the disclosure of behavioral data. However, the level of stress or discomfort of an individual in connection with the disclosure of a PESEL number is much higher than in disclosing data such as location data (GPS), network identifiers (cookies, etc.), and searched Internet resources. The severity of disclosure of data in the form of a PESEL number together with the name and surname is comparable to the disclosure of "financial data" (which were also disclosed as a result of the breach in question) or "sensitive" data and depending on the changing context, e.g. emergence of new or reduction of existing threats should be assessed by the Company on a case-by-case basis. The classification of the PESEL number together with the name and surname to the category of behavioral data, which is not the PESEL number, indicates that such an individual assessment has not been carried out. On the other hand, as already indicated above, the disclosure of the PESEL number together with the name and surname due to the level of criticality of this data should be classified by the Company in the analysis carried out as higher categories. In addition, the Company did not include in the category "Financial

data - data on the financial situation of a natural person" with a score of 3, the subject of the proposed insurance, i.e. a house with the scope of insurance, i.e. the amount of PLN [...], third party liability insurance in private life with a guaranteed sum in in the amount of PLN [...] and the amount of the premium for selected variants in the amount of PLN [...] and PLN [...], while for this category the form in the explanation of which data should be assigned to this category indicates "assets" or, " transaction / payment history, invoices ". The European Union Agency for Cybersecurity (ENISA) indicates in its Recommendations on the methods of assessing the seriousness of personal data breaches, the recommendations of which the Company refers to in its explanations, that it is any type of financial data. Additionally, it should be pointed out that the recommendations of the European Union Agency for Cybersecurity (ENISA) can help in the assessment, however, taking into account the national context. This context has been incorrectly taken into account by the Company by ignoring the major threats posed by the disclosure of this data, in particular the PESEL number, and then classifying the PESEL number together with the name and surname to a group whose data sensitivity is not adequate with the data sensitivity in the form of a PESEL number along with the name and surname.

In point 2.2. The "specific factors criterion", in which, according to the adopted methodology, specific breach factors should be indicated that increase or decrease the level of risk for data subjects, such as: larger amounts of data on the same person (with a score of +1); specific characteristics of the data controller (with a score of +1 point); specific characteristics of the unit (with a score of +1 point); the nature of the data (with a score of +1 or -1); high importance of the negative effects of the violation for natural persons (with a score of +1); public availability of data (with a score - 1 point); incorrect data (with a result of -1 point) and other factors (with a result of +1 point or -1 point), the Company indicated the lack of factors reducing or increasing the risk, without awarding or subtracting points from this criterion. On the other hand, the disclosed personal data was collected in the process of offering insurance immediately preceding the conclusion of the insurance contract and should be covered by insurance secrecy referred to in Art. 35 sec. 1 of the Act of 11 September 2015 on insurance and reinsurance activities (Journal of Laws of 2020, item 895, as amended). The company could reasonably anticipate that, in connection with the prepared offer, an insurance contract could be concluded, and therefore there would be a disclosure of data that the Company is obliged to protect in particular, which, consequently, should be taken into account in the adopted risk assessment methodology and classified under "other factors" , and thus increase the infringement rating by 1 point. In addition, the information that the disclosure of the data in question may pose a risk of "loss of confidentiality of personal data protected by

professional secrecy" was communicated to the Company in the breach notification of [...] September 2020 sent to the Company by the processor. In addition, the Company omitted that the disclosure of data, in particular about the PESEL number together with other data, including name and surname and information about the financial / property status, causes a high weight of negative effects for natural persons, which should additionally increase the assessment of the infringement by 1 point. and that due to the violation, more data concerning the same person was disclosed, which should also increase the rating of the violation by 1 point - in accordance with the methodology adopted by the Company.

In point 2.3. "The criterion of the possibility of identification", the Company defined the ease of identification as a limited possibility of identification, awarding this criterion 0.5 points, on the scale: the incident does not constitute a breach of privacy (with a score of 0 points), a negligible possibility of identification (with a score of 0.25 points), limited possibility of identification (with a score of 0.5 points), high probability of identification (with a score of 0.75 points), maximum likelihood of identification (with a score of 1 point), with additional explanations regarding the levels of identification risk for "high probability identification "as an example was indicated" PESEL identification number in conjunction with other data, e.g. name and surname, address, e-mail or address of residence ", and for the" maximum likelihood of identification "as an example was indicated, inter alia, also an identification number or ID card number if data from the source database is also available (e.g. name, date of birth, photos, etc.). The above clearly determines the intention to classify the PESEL number in the adopted methodology to the "maximum likelihood of identification" or at least to the "high probability of identification". Bearing in mind the above, it should be pointed out that the determination by the Company of the ease of identification based on the PESEL identification number together with the name and surname, as a "limited possibility of identification", contrary to the description from the adopted methodology, is an obvious error. On the other hand, the inclusion of the PESEL number along with the name and surname in the adopted methodology at the same time in two levels of identification risks confirms that the methodology was developed in a completely arbitrary manner. Regardless of the above, the supervisory authority indicates that the breach of confidentiality of personal data in the form of a PESEL number together with the first and last name in the analysis should be considered as the "maximum probability of identification" because the PESEL identification number uniquely identifies a natural person.

In point 2.5. "Other criteria" in the form were indicated the following criteria: intentional violation (with a score of +1 point), unreliable recipient of data (with a score of +1), a large number of people affected by the incident (with a score of +1 point), trusted recipient of the data (with a score of -1), data unavailable due to encryption (with a score of -1), a very small number of

people affected by the incident (with a score of -1), other significant violation factors (with a score of +1 or -1)), as other criteria for the violation, the Company chose the factor: a very small number of people affected by the incident, subtracting 1 point. Dropping the analysis result by 1 point due to the very small number of people affected by the incident raises doubts. It should be pointed out that for the seriousness of the infringement and the probability of negative consequences of the infringement for the individual data subject, the above circumstance regarding the number of persons affected by the infringement is irrelevant. The company assumed that the circumstance of a small number of people affected by a breach that lowers the risk assessment, in line with the adopted methodology, will apply when the breach concerns less than 20 people. Assuming the above circumstance to assess the seriousness of the infringement, a situation may arise where for two similar infringements with a different number of people affected by the infringement, with an infringement with a smaller number of people, e.g. 19, the final risk score, due to taking into account such circumstances, may show that there is no need to reporting the breach and notifying the data subjects, and the failure to take this circumstance into account for 20 persons may result in the need to report and notify these persons, which in fact will unjustifiably deprive the persons from the group of a reduced possibility of adequately responding to the breach, and the supervisory authority to evaluate the submitted application. Taking into account the categories of data affected by the breach which result in a high weighting of the negative effects on the individual when assessing the risk of violating the rights or freedoms of an individual, the small number of people affected by the breach should not be taken into account as a risk mitigating factor. Additionally, it should be emphasized that the fact that the result was reduced due to a very small number of people affected by the infringement is not reflected in the above-mentioned recommendations of the European Union Agency for Cybersecurity (ENISA). The situation is different when the breached categories of data do not constitute the possibility of high risk occurrence, but due to the large number of persons affected by the breach, the severity of the breach increases by extending the possibility of negative consequences, which may require reporting to the supervisory authority and, in the event of the administrator's doubts as to the need to submit a notification, it should actually be taken into account. Incidentally, it should be noted that such a circumstance in the methodology adopted by the Company was taken into account by the criterion of "a large number of people affected by the incident (with a score of +1 point)". However, in this assessment, this criterion was not applicable and was not taken into account.

Based on the conducted analysis, the Company assessed the seriousness of the infringement effects with a score of 0.25 points as "none or low", which in the adopted methodology classifies the seriousness of the infringement effects to the lowest

possible scale from: none or low (if the result is lower or equal to 2), medium (if the score is less than or equal to 3), high (if the score is less than or equal to 4), very high (if the score is greater than 4), where the data subject will not be affected by the breach or may face some inconveniences that are easy to overcome. Also, the probability of negative effects for the data subject was assessed by the Company at the lowest possible level, as omitted on the scale: omitted, limited, serious, maximum. However, in the opinion of the Company, the degree of probability was also influenced by the fact that the wrong recipient of the message made a declaration that he did not read the content of the documents and that they were removed, which, as explained in this decision, did not reduce the probability to a degree that would release the Company from the obligation to report and notify the data subject about the breach. Then, the Company, taking into account in the conducted analysis a defective assessment of the seriousness of the effects of the infringement and a defective assessment of the probability, assessed the risk level as the lowest possible for selection in the risk matrix, indicating that it is unlikely that the infringement would result in violation of the rights or freedoms of natural persons, and thus no is obliged to report the breach to the supervisory authority or to notify the data subject about the breach.

In addition, in a letter dated […] February 2021, the Company announced that it had re-performed the analysis using the form available on the website […], which, in the Company's opinion, confirms that it did not have to report the breach to the supervisory authority or notify the person affected by the breach. In view of the above, it should be pointed out that the completed infringement risk assessment form, which was attached as evidence to the above letter, is in fact a printout from the calculator of the seriousness of personal data breaches available on the website of one of the entities providing support services in the field of personal data protection. The President of the Personal Data Protection Office cannot assess the correctness of the indicated calculator, the additionally completed form does not have a detailed description of the adopted or non-adopted criteria and explanations on how and why the "calculator" calculates the partial results and the final result for the assessment of individual criteria. Moreover, the analyzes differ in terms of the criteria assessed. The above fact makes it impossible to perform a detailed assessment of the conducted analysis, as well as a reliable comparison of the conducted analyzes. Nevertheless, even a superficial assessment of the screenshot attached by the Company to the letter of [...] February 2021 showing the result of the infringement risk assessment carried out using the form on the page [...] shows that the analysis carried out duplicated the errors of the analysis made on [...] September 2020 . and attached to the letter of [...] December 2020, and thus does not confirm that this analysis was carried out correctly. Doubts concern in particular: failure to

take into account that the infringement also related to data on financial / property status, indication that the scope of the data breached was not wide, or determination of the probability of identifying the data subject as limited. In addition, what was not presented by the Company along with a screenshot of the completed form, the entity providing the form on the website indicated by the Company with the option of "saving to a pdf file", made a reasonable reservation that "any breach or suspected breach of personal data protection should be analyzed individually, in particular with regard to the obligations set out in Art. 33 and 34 of the GDPR, therefore this calculator can only be used as an additional resource and cannot be used as an independent basis for decision-making by any entity or person that uses the calculator on their own responsibility ”.

As indicated above, the assessment made by the Company was carried out incorrectly. Obvious errors, as well as irregularities consisting in particular in underestimating the results in individual criteria, failure to take into account important factors for individual criteria, or taking into account factors that should not be applicable, indicate that the analysis was carried out arbitrarily and was not used as a tool for assisting the Company in assessing whether a breach should be reported to the supervisory authority and the data subject should be notified of the breach, but rather for the purpose of demonstrating that he or she is not subject to such obligations. The final assessment of the infringement was grossly underestimated, assuming the lowest of the possible values, which confirms the deliberate lowering of the adopted values in order to avoid the necessity to fulfill the obligations under Art. 33 and 34 of Regulation 2016/679. On the other hand, conducting the analysis in a correct manner, devoid of at least some of the above-mentioned doubts, should result in demonstrating the obligation to notify a breach of personal data protection in accordance with Art. 33 paragraph. 1 of the Regulation 2016/679 and notification of the breach of the data subject, in accordance with art. 34 sec. 1 of Regulation 2016/679.

It should be emphasized again that in the present case, due to the scope of the disclosed personal data and the significant consequences for the data subject, there was a high risk of violating the rights or freedoms of a natural person related to the necessity to fulfill the obligations of reporting a personal data breach and notification of breach of the data subject. Both the processing entity being the data controller with regard to the name and surname, as well as other insurance companies, in connection with the breach in question, unlike the Company, had no doubts as to the necessity to report the breach of personal data protection to the President of the Personal Data Protection Office and made such a notification.

The above assessment is also not affected by the fact of obtaining a declaration from the wrong recipient about the deletion of the correspondence received. There is no certainty that before these activities the person did not forward the received

message, did not e.g. make a copy or did not record the personal data contained in the document in another way, e.g. by writing them down. Therefore, the mere deletion of correspondence does not provide any guarantee that the intentions of such a person will not change now or in the future, and the possible consequences of using such categories of data may be significant for the person whose data was affected by the breach. Also, the Company is not able to actually verify the declaration of the lack of familiarity with its content or the deletion of the correspondence received. The WP29 guidelines state: “Whether a controller knows that personal data is in the hands of persons whose intentions are unknown or who may be malicious may be relevant to the level of potential risk. There may be a breach of data confidentiality consisting in an accidental disclosure of personal data to a third party, as defined in Art. 4 point 10, or to another recipient. This may be the case, for example, if personal data is inadvertently sent to the wrong department of the organization or to a vendor organization whose services are widely used. The administrator may request the recipient to return or securely destroy the data received. In both cases - due to the fact that the controller is in a permanent relationship with these entities and may know their procedures, their history and other relevant details concerning them - the recipient can be considered "trusted". In other words, the controller can trust the recipient enough to be able to reasonably expect that the party will not read or access the data sent by mistake, and that it will follow the instruction to send it back ”. In the present case, however, there are no grounds for recognizing an unauthorized recipient and treating it as a "trusted recipient". The above was also confirmed by the Company in a letter of [...] February 2021, indicating that "the Company did not recognize the accidental, unauthorized recipient of the data as a trusted recipient". In stating the above, however, the Company did not show consistency, assuming at the same time that the statements made by an accidental recipient (who is not a trusted recipient) reduce the probability of the negative consequences of the breach materializing for the person whose personal data was disclosed.

Additionally, it should be indicated that the declaration of the wrong recipient was submitted on a ready-made form, which may indicate that the content of the declaration was prepared by the processor. Also, the date on which the declaration was marked has visible traces of correction, which should raise doubts of the administrator. Moreover, it is difficult to expect that a person with bad intentions will refuse to make an appropriate statement, as such action could destroy his evil intentions. In addition, according to the notification of a personal data breach by X, "a third party confirmed the deletion of incorrectly received documents as soon as it became aware that they were intended for someone else." The foregoing casts doubt on the wrong recipient's statement that he did not know the content of the attached documents, since he realized, however, that the

correspondence was not intended for him. Also, it does not appear from the collected evidence that the wrong recipient himself turned to the processor or controller with the information that he had received a message not intended for him. In addition, it should be noted that the Company cannot be sure (and in this respect it is not possible to verify) whether the e-mail box is not accessed by other people, or that the box has not been infected with malware, which could potentially result in access to this data. other people than the addressee of incorrectly directed correspondence. In the case in question, the Company obtained twice the declaration of an unauthorized addressee, which may indicate that it had significant doubts in this respect. By contrast, the Article 29 Working Party clearly states in the guidelines that "In case of any doubts, the controller should report the breach, even if such caution could turn out to be excessive".

The company, by letter of [...] February 2021, applied for admission and taking evidence from the testimony of witness Ł P that he had permanently deleted the e-mail that was sent to him on [...] September 2020, approximately 12 o'clock and is not in the possession of this message, he is not familiar with the content of the documents attached to the message, because he has not read their content before deleting the message, it is not possible to identify the person whose data was in the attached documents and re-verified the media and not has no copies of any documents wrongly served on him.

Taking evidence from the testimony of the above-mentioned persons as a witness to the circumstances indicated in the letter of [...] February 2021, and thus in fact also to the confirmation of the statements made by that person of [...] September 2020 and [...] January 2021, is redundant and will not have an effect, in the light of the above-mentioned arguments relating to the already submitted by the above-mentioned person, for the assessment of the supervisory authority of the level of risk of violation of the rights or freedoms of the data subject in relation to the violation of personal data protection in question.

Consequently, it would not reduce the probability of the breach to a degree that would release the Company from the obligation to notify the breach of personal data protection to the supervisory body within 72 hours of finding the breach and notifying the data subject about the breach. As indicated above, both the Company, based on the submitted declarations, and the President of the Personal Data Protection Office, based on the submitted declarations and possible testimonies confirming the content of the submitted declarations, there is no actual possibility of their verification. Taking evidence from the testimony of the above-mentioned person acting as a witness does not exclude the possibility that the submitted explanations may turn out to be false, and thus does not exclude the possibility of a high risk of violation of the rights or freedoms of a natural person.

It should be emphasized again that the declaration made by an unauthorized addressee does not prejudge that it is unlikely

that this breach would result in a risk of violating the rights or freedoms of natural persons and does not exclude the assumption that there was a high risk of violating the rights or freedoms of the data subject. It should be pointed out once again that the personal data has been made available to an unauthorized recipient, which means that there has been a security breach leading to unauthorized disclosure of personal data, the unauthorized recipient cannot be considered a "trusted recipient", and the scope of this data determines that there was a high the risk of violating the rights or freedoms of natural persons.

In addition, as it follows from the explanations of the Company contained in the letter of [...] February 2021, the Company determined that the personal data covered by the violation in question is not publicly available on the Internet, and there is no person in the Court and Economic Monitor or the National Court Register. the indicated PESEL number. The Article 29 Working Party in its guidelines for situations where reporting of breaches is not necessary indicates, for example, the situation "where personal data are already publicly available and the disclosure of such data does not represent a likely risk for the individual concerned." Bearing in mind the above, it should be pointed out that in the present case such circumstance did not occur, which consequently did not lower the probability of the risk for the data subject.

It should also be pointed out that the fact of the short - in its opinion - of the time, in which the effects of the breach towards the data subject may have persisted, that is raised by the Company, i.e. from the date of the breach to the date of the declaration by the wrong recipient about the deletion of the message not intended for him. , does not apply in the proceedings in question, because, as has already been explained, the declaration of the unauthorized addressee does not exclude the possibility of materialization of significant negative consequences of the breach for the data subject.

It should also be pointed out that in the present case it is not important whether the unauthorized recipient has become acquainted with the personal data of other persons, but the fact that such a risk has occurred and, consequently, there has also been a potential risk of violating the rights or freedoms of the data subject.

At this point, it should be noted that for the obligation to notify the data subject about a breach of personal data protection, it is not necessary to materialize the negative consequences of the breach, the mere possibility (risk) of such consequences is sufficient in this respect, as in the present case, in the opinion of the supervisory authority, it is high. As 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 inform the data subject about such a breach without undue delay. However, as it results

from Art. 33 paragraph 1 of Regulation 2016/679, in the event of a breach of personal data protection, the controller shall, without undue delay, report it to the supervisory authority, unless the breach is unlikely to result in a risk of violation of the rights or freedoms of natural persons. When assessing the risk of violation of the rights and freedoms of natural persons, on which the notification of a personal data breach and notification of the breach of the data subject depend, the probability factor and the significance of the potential negative effects should be taken together. A high level of any of these factors has an impact on the overall score on which the fulfillment of the obligations set out in Art. 33 paragraph 1 and art. 34 sec. 1 of Regulation 2016/679. Bearing in mind that due to the scope of the disclosed personal data, there was a possibility of significant negative consequences for the data subject, the importance of the potential impact on the rights or freedoms of natural persons should be considered high. At the same time, the likelihood of high risk arising from the present infringement is not small and has not been eliminated. Thus, it should be pointed out again that in connection with the breach in question there was a high risk of violation of the rights or freedoms of the data subject, which in turn determines the obligation to report the breach of personal data protection to the supervisory authority and to notify this person about the breach. The Article 29 Working Party states in its guidelines that “when assessing the risks that may arise from a breach, the controller should collectively consider the importance of the potential impact on the rights and freedoms of individuals and the likelihood of their occurrence. Of course, the risk increases when the consequences of a breach are more severe and also when the probability of their occurrence increases. In case of any doubts, the controller should report the breach, even if such caution could turn out to be excessive ”. Also in relation to the existence of a personal data breach, as already explained in this decision, there were no other factors reducing the likelihood of negative effects, such as limited traceability, the conclusion that personal data are publicly available, or the recognition of the wrong recipient as a "trusted person" ". Referring in this context to the UODO publication entitled "Responsibilities of administrators related to breaches of personal data protection", which the Company refers to in its explanations, where the supervisory body indicated that "the situation in which [...] correspondence (containing at least such data categories as name, surname and PESEL number) is provided to a person known or unknown to the administrator, as a rule is associated with a high risk for data subjects ", which in the opinion of the Company states that the supervisory body" does not exclude the situation that in certain circumstances the risk assessment may be different (the authority uses with the phrase "in principle)" and that, according to the Company, "such a different risk assessment should be applied to the data breach in question", it should be noted that the wrong recipient's declaration in a situation where the scope

of the data determines a high risk of violation of rights or freedoms natural persons, in the light of the above-mentioned arguments, cannot be treated as an exceptional circumstance except requiring the notification of a breach of personal data protection to the President of the Personal Data Protection Office and notification of the breach of the data subject. As indicated by the supervisory authority in the next sentence of the cited publication, "a different probability may be assumed in the event of delivering erroneous correspondence to a person known to the administrator (e.g. to another client of the administrator who informed about the mistake or stated that he did not use the information provided by mistake for private purposes and / or inconsistently). with the law), it does not give any guarantee that the intentions of such a person will not change now or in the future, and the possible consequences of using such data categories may be significant ”.

For a better illustration of cases of personal data breaches, where there is no obligation to notify the supervisory authority due to the fact that it may be considered that the breach is unlikely to result in a risk of violating the rights or freedoms of natural persons, one can refer to the guidelines of the Art. 29. The guidelines mention the loss of “a securely encrypted mobile device used by the controller and its employees as an example of a breach that does not require reporting to the supervisory authority. Assuming the cryptographic key is securely stored by the administrator and it is not the only copy of personal information, the personal information will be inaccessible to the attacker. This means that the breach in question will most likely not involve the risk of violating the rights and freedoms of the data subjects. If it later turns out that the cryptographic key has been compromised or the software or encryption algorithm has weaknesses, the level of risk of violating the rights and freedoms of individuals will change and reporting may become necessary. " The above situation, in which personal data is inaccessible to an unauthorized person, and the possible loss of confidentiality of this data depends on technological progress that is difficult to foresee in time, which enables the breach of cryptographic security, is incomparable to the situation in which an unauthorized person has gained access to personal data, however stated that she had not read the data and deleted the incorrectly sent correspondence. Such a circumstance, unlike in the case of secure data encryption, does not exclude the possibility of unauthorized reading of the data. The above is also supported by the inability to actually verify that the personal data has not lost the confidentiality attribute. Comparing the two cases, it cannot be concluded that the breach in question resulted in a risk of violating the rights or freedoms of natural persons, even to an extent similar to the situation indicated in the guidelines by the Article 29 Working Party, which also confirms that the risk has not been reduced to the level where it can be stated that the breach is unlikely to result in a risk to the rights or freedoms of an individual. Incidentally, it should be noted that

the Company was aware of the risk related to the electronic transmission of confidential information and personal data and in this scope - as it results from the entrustment agreement concluded - required the processor to apply adequate technical and organizational measures consisting in securing them with the use of cryptographic protection measures. . However, these measures were not applied in the infringement in question.

Referring to the example No. 15 of the breach presented in the European Data Protection Board Guidelines 01/2021 on Examples of Data Protection Breach Notifications, version 1.0 (hereinafter also referred to as: EDPB Guidelines 01/2021), for which in its explanations of [...] February 2021 r. is established by the Company, where the breach consisted in sending personal data to 15 unauthorized recipients, and then the sender (administrator) contacted the unauthorized recipients and asked for the deletion of the data and which, in the Company's opinion, shows that such a step may be considered as risk mitigation measure, it should be indicated that the scope of data covered by the infringement in the discussed example included: name, e-mail addresses and food preferences of the data subjects. As indicated in EDPB Guideline 01/2021, the risks arising from the nature, sensitivity, volume and context of these data are low and it can be concluded that the data subjects were not significantly affected by the breach. Against this background, the fact that the data controller immediately contacted recipients after becoming aware of the error could be considered a mitigating factor. On the other hand, in the event of a breach covered by this proceeding, as demonstrated above, the disclosed scope of data causes a high risk of violation of the rights or freedoms of a natural person, which entails the need to report the breach to the supervisory authority and notify the data subject about the breach.

Reference should be made here to the example No. 16 of the European Data Protection Board Guideline 01/2021, which is closer to the breach in question. As it follows from the EDPB Guidelines 01/2021 for this example, the insurance group, as part of offering car insurance, sent to the wrong recipient correspondence containing personal data in the form of name, surname, address, date of birth, registration plate number and the classification of the insurance rate for the current and next year. . The guidelines indicate that the wrong recipient should be informed that he cannot use the information read out, and yet that the breach should also be reported to the supervisory authority.

It should be emphasized, however, that the examples from the above-mentioned the guidelines do not cover the national context, in which the disclosure of the PESEL number together with the name and surname uniquely identifies a natural person, and in combination with data on financial / property status may cause significant consequences for the person whose

personal data have been disclosed. Referring the above to the violation in question, it should be noted that the Company's obligation was not only to report the data breach to the President of the Personal Data Protection Office, but also to notify the data subject about the breach.

In addition, the reasons why the Company re-engaged forces and resources to obtain an additional statement from an unauthorized recipient, as well as accepting by it that the only possible action of the administrator in this situation may be to demonstrate that circumstances arise in connection with these statements, are not fully understood. reducing the probability of negative consequences of the breach for the data subject. Bearing in mind the principle of fairness and transparency of data processing expressed in art. 5 sec. 1 letter a) of Regulation 2016/679 and the position of the Art. 29 Working Group contained in the above-mentioned fragment of the guidelines, as well as in relation to the submission to the Company by the President of the Personal Data Protection Office in a letter of [...] December 2020, information on the obligations incumbent on the administrator in connection with the breach of protection data, as well as information on how the Company may report a breach, or finally, due to the initiation of administrative proceedings regarding the obligation to report the breach to the supervisory body and notify the data subject about the breach, it may come as a surprise that the Company did not take any action to in order to fulfill the administrator's obligations under Art. 33 paragraph 1 and art. 34 sec. 1 of Regulation 2016/679. It should be emphasized that providing the data subject with information, inter alia, about the measures it can take to minimize the possible negative effects of the breach significantly reduces the possibility of their occurrence, which is of incomparably greater importance for the security of the data subject's data than an additional statement by the wrong recipient.

In addition, it should be pointed out that adopting the position according to which obtaining an appropriate statement from the wrong recipient would make it unlikely that the breach would result in a risk of violating the rights or freedoms of natural persons, would cancel the obligation imposed by the legislator to notify the data subject and the supervisory authority about breach. Instead of notifying the President of the Personal Data Protection Office and the data subject, the administrators would use forces and resources to obtain an appropriate statement - as was the case in the case at hand - recognizing that this exempts them from the obligation to report a breach of data protection to the supervisory authority, as well as from notifying the person. the data subject about the breach. Indeed, it should be pointed out, as it is published on the UODO website in the annual Reports on the activities of the President of the Personal Data Protection Office, that the vast majority of reports submitted to the President of the Personal Data Protection Office concern the disclosure of data to an unauthorized person,

including sending correspondence to the wrong recipient . Failure to submit a notification due to obtaining a declaration of an unauthorized person would significantly reduce the level of security of the processed data. This is because it would deprive the supervisory authority of information on breaches of personal data protection, allowing for an appropriate reaction that may limit the effects of such breaches, and deprive data subjects of the possibility of counteracting the negative effects of the breach, which in turn would translate into a significant reduction in the level of protection of the rights or freedoms of these persons.

It should be emphasized that the assessment of the risk of violating the rights or freedoms of a natural person should be made through the prism of the endangered person, and not the interests of the controller. Based on the breach notification, the individual can himself assess whether, in his opinion, the security incident may have negative consequences for him and take appropriate remedial action. Also, based on the information provided by the administrator regarding the description of the nature of the breach and the measures taken or proposed to remedy the breach, a natural person may assess whether, after the breach, the data administrator still guarantees the proper processing of his personal data in a manner that ensures security. On the basis of such an assessment, it may decide, for example, to resign from the administrator's services or in the event of the occurrence of the premises referred to in art. 17 of Regulation 2016/679 to exercise the right to delete data.

Failure to notify a natural person in the event of a high risk of violation of their rights or freedoms deprives them not only of the possibility of an appropriate response to the violation, but also of the possibility of making an independent assessment of the violation, which, after all, concerns their personal data and may have significant consequences for them. On the other hand, failure to notify a personal data breach deprives the supervisory authority of an appropriate response to the breach, which manifests itself not only in assessing the risk of breach for the rights or freedoms of a natural person, but also in particular in verifying whether the controller has applied appropriate measures to remedy the breach and minimize negative consequences. the consequences for the data subjects as well as whether it has applied appropriate security measures to minimize the risk of a recurrence of the breach.

The supervisory authority did not share the position of the Company, presented in the letter of [...] February 2021, according to which the Company has no legal or actual possibility to notify the data subject about the breach, due to the lack of current contact details (address data) of that person however, an attempt to obtain such data would violate the principle of data minimization. In presenting the above position in extensive arguments, the Company omitted significant contractual provisions binding it with the processor, ie X Sp. z o.o. As evidenced by the evidence gathered in the case, the Company concluded an

agency agreement with X, the integral part of which is an attachment constituting an agreement to entrust the processing of personal data (marked as: "[...]"). Pursuant to the provisions of § 7 point 3 of the concluded data processing agreement, the agent, ie X undertakes to assist ERGO Hestia in fulfilling the obligations set out in art. 32-36 GDPR; in particular, the Agent undertakes to provide ERGO Hestia with information and carry out instructions regarding, inter alia, cases of breach of personal data protection and notifying the supervisory authority or data subjects about it. Thus, on the basis of the above provision, the Company may instruct the agent to provide information on the contact details of the data subject, as well as instruct the processor to notify on behalf of the Company of a breach of personal data protection of the data subject, and thus fill in the obligation on the Company obligation under Art. 34 sec. 1 of Regulation 2016/679.

It should be emphasized that, as it results from the established facts, the breach occurred as a result of accidental sending of an e-mail containing personal data to the e-mail address of another person in connection with the offer by the insurance agent who is also the processing entity of the Company (ie X Sp. z o. o.) insurance offered by the Company. Both the error in sending the message to a different e-mail address, as well as the information provided that the data subject is a current customer of X Sp. z o.o. proves that the processing entity is in possession of the contact details of the person whose personal data the breach relates to. In addition, as it results from the collected evidence, the Company and the processor, for communication with the data subject, provided a communication channel in the form of e-mail correspondence. If the processor is not in possession of other contact details, there are no obstacles for the notification to be sent to the e-mail address of that person. In addition, it should be noted that the Company, in accordance with the provisions of § 3 point 5 of the data processing agreement linking it with X, required that the correspondence sent be secured with the use of cryptographic protection measures. However, as it follows from the excerpt from the document "[...]" in force at X Sp. z o. o., which was attached as evidence to the Company's letter of [...] February 2021, "documents sent to clients or entities with whom we cooperate should be secured with a password, and the password sent by other means of communication (e.g. via SMS or via SMS). during a telephone conversation. ”The above proves that the processor should be able to contact the data subject, also via communication channels other than e-mail correspondence. concern, the Article 29 Working Party in the guidelines on reporting personal data breaches in accordance with Regulation 2016/679 indicated that "if the controller is not able to notify a given natural person about the breach, because the stored data is insufficient to contact that person, in this particular case, the controller should inform it as soon as reasonably practicable e feasible (e.g. if a natural person makes use of the services

provided for in Art. 15 of the right to access your personal data and will provide the administrator with additional information required to contact her) ”.

Considering the above, the position of the Company about the inability to notify the data subject about the breach is not justified. In addition, responding to the Company's doubts as to the lack of a legal basis for processing the contact details of the data subject, i.e. the relevant recipient, it should be indicated that the Company did not have the above doubts when obtaining from the processor - immediately after finding the infringement - the personal data of the wrong recipient.

It should also be emphasized that the obligation to notify the data subject about a breach of personal data protection that causes a high risk of violation of rights or freedoms is an obligation resulting from legal provisions, which means there is a legal basis for the processing of personal data necessary for the proper implementation of this obligation, i.e. e.g. to process the contact details of the data subject.

It should be pointed out that the Company has not performed a proper analysis in terms of the risk of violating the rights or freedoms of natural persons necessary to assess whether there has been a breach of personal data protection, resulting in the need to notify the President of the Personal Data Protection Office and the persons affected by the breach, which resulted in the failure to notify the breach of personal data protection. the supervisory authority without undue delay, if possible, no later than 72 hours after the infringement has been identified, pursuant to Art. 33 paragraph 1 of the Regulation 2016/679 and the lack of immediate notification of the breach of the data subject, in accordance with art. 34 sec. 1 of Regulation 2016/679.

However, in the event of any doubts that require an explanatory procedure enabling the transfer of information referred to in Art. 33 paragraph 3 of Regulation 2016/679, the Company could, pursuant to Art. 33 paragraph 4 of the Regulation 2016/679, make a preliminary notification, and then provide information successively without undue delay. However, the company did not perform such activities. Thus, in the absence of notification of a breach of personal data protection to the supervisory body, the allegations of the Company set out in the letter of [...] February 2021 that the supervisory body did not question the risk caused by the breach before and after the initiation of administrative proceedings, despite the supervisory body's lack of an obligation to do so and apart from the procedure provided for such situations, are not justified. In addition, it should be noted that the fact that the analysis presented by the Company in connection with the breach of personal data protection may raise doubts of the supervisory body was evidenced by, for example, the initiation of administrative proceedings regarding the failure to report the breach to the President of the Personal Data Protection Office and the failure to notify the data subject about the breach.

However, a detailed reference to this analysis could only be made in the decision issued in connection with this proceeding. It should be emphasized once again that when reporting a breach to the supervisory authority, the administrators inform the President of Personal Data Protection whether, in their opinion, there is a high risk of violation of the rights or freedoms of data subjects and - if such a risk occurred - whether they provided relevant information to natural persons to whom the breach has an impact. In justified cases, they may also provide information that, in their opinion, notification is not necessary due to the fulfillment of the conditions set out in Art. 34 sec. 3 lit. a) and b) of Regulation 2016/679. The President of UODO verifies the assessment made by the administrator and may - if the administrator has not notified the person - request such a notification from him. In the absence of notification of a breach of personal data protection, the President of the Office for Personal Data Protection is deprived of the possibility of reliable verification. The Article 29 Working Party in its guidelines states: “When reporting a breach to a supervisory authority, controllers may consult with the supervisory authority on whether relevant information should be provided to the affected individuals in a given case. The supervisory authority may require the controller to inform relevant individuals about a breach. Notifying natural persons about the breach enables the controller to inform those persons about the risks associated with the breach and to indicate actions that these persons can take to protect themselves from the potential consequences of the breach. " "At the same time, it should be emphasized that failure to comply with the obligation to notify a natural person or a supervisory authority may potentially result in imposing a penalty on the controller pursuant to Art. 83 ". In the case in question, as evidenced by the collected evidence, the Company had doubts as to the risk of violating the rights or freedoms of a natural person, which is confirmed by re-asking the wrong addressee to submit an additional statement or to re-assess the risk using the form available on the website [...], and yet it has not notified the personal data breach to the supervisory authority, not to mention the breach notification of the data subject.

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 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 violation of rights or freedoms, including data subjects. The controller should fulfill this obligation as soon as possible. Recital 85 of the preamble to Regulation 2016/679 explains: "In the absence of an adequate and prompt response, a breach of personal data protection may result in physical harm, property or non-material damage to natural persons, such as loss of control over own personal data or limitation of rights, discrimination, theft or falsification of identity, 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. Therefore, as soon as it becomes aware of a breach of personal data protection, the controller should notify it to the supervisory authority without undue delay, if practicable, no later than 72 hours after the breach has been discovered, unless the controller can demonstrate in accordance with the accountability principle that it is unlikely to be, that the breach could result in a risk of violation of the rights or freedoms of natural persons. If the notification cannot be made within 72 hours, the notification should be accompanied by an explanation of the reasons for the delay and the information may be provided gradually without further undue delay. '

In turn, 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 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. (...) ".

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 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 care for the interests of the data subject, the Company 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 the Regulation 2016/679, which the Company did not fulfill. Therefore, when deciding not to notify the supervisory body and the data subject about the breach, the company effectively deprived that

person of reliable information about the breach and the possibility of counteracting potential damage, provided without undue delay.

When applying the provisions of Regulation 2016/679, it should be borne in mind that the purpose of this regulation (expressed in Article 1 (2)) is to protect the fundamental rights and freedoms of natural persons, in particular their right to the protection of personal data, and that the protection of natural persons in connection with the processing of personal data is one of the fundamental rights (first sentence of Recital 1). In case of any doubts, e.g. as to the performance of obligations by administrators - not only in a situation where there has been a breach of personal data protection, but also when developing technical and organizational security measures to prevent them - these values should be taken into account in the first place.

Consequently, it should be stated that the Company has not notified the breach of personal data protection to the supervisory body in compliance with the obligation under Art. 33 paragraph 1 of Regulation 2016/679 and did not notify the data subject without undue delay of the breach of data protection, in accordance with art. 34 sec. 1 of the Regulation 2016/679, which means the Company's breach of these provisions.

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 - taking into account the probability that this breach of personal data protection will result in a high risk - may request it or may state that that one of the conditions referred to in sec. 3. In turn, from the content of Art. 58 sec. 2 lit. e) of Regulation 2016/679 it follows that each supervisory authority has the right to remedy the need for the controller to notify the data subject about a breach of data protection.

Moreover, pursuant to Art. 58 sec. 2 lit. i) of Regulation 2016/679, each supervisory authority has the power to apply, in addition to or instead of other remedial measures provided for in Art. 58 sec. 2 of Regulation 2016/679, an administrative fine under Art. 83 of the Regulation 2016/679, depending on the circumstances of the specific case. The President of the Personal Data Protection Office states that in the case under consideration there are premises justifying the imposition of an administrative fine on the Company pursuant to Art. 83 sec. 4 lit. a) of Regulation 2016/679 stating, inter alia, that the breach of the administrator's obligations referred to in art. 33 and 34 of Regulation 2016/679 is subject to an administrative fine of up to EUR 10,000,000, and in the case of an enterprise - up to 2% of its total annual worldwide turnover from the previous financial year, with the higher amount being applicable.

Pursuant to art. 83 sec. 2 of Regulation 2016/679, administrative fines shall be imposed, depending on the circumstances of

each individual case, in addition to or instead of the measures referred to in Art. 58 sec. 2 lit. a) - h) and lit. j) Regulation 2016/679. When deciding to impose an administrative fine on the Company, the President of the Personal Data Protection Office - pursuant to Art. 83 sec. 2 lit. a) - k) of Regulation 2016/679 - took into account the following circumstances of the case, necessitating the need to apply this type of sanction in the present case and having an aggravating effect on the size of the imposed administrative fine:

Nature and gravity of the infringement (Article 83 (2) (a) of Regulation 2016/679).

The violation found in this case consisting in providing an unauthorized person with personal data in the form of: PESEL number along with name and surname, city, postal code and data on the financial / property situation of the data subject in the form of: insurance period, subject of insurance (home), insurance product [...], the sum insured / guarantee sum in the amount appropriate to the selected option and the amount of the premium appropriate to the selected insurance option, is of significant importance and serious nature, as it may lead to property or non-material damage to the person whose data has been breached, and the probability of such damage occurrence is high.

Duration of the infringement (Article 83 (2) (a) of Regulation 2016/679).

The President of the Personal Data Protection Office recognizes the long duration of the infringement as an aggravating circumstance. Several months elapsed from the Company becoming aware of the breach of personal data protection until the date of issuing this decision, during which the risk of violating the rights or freedoms of the affected person could be realized, and which the person could not counteract due to the failure by the Company to fulfill its obligation. reporting a breach of personal data protection to the President of the Personal Data Protection Office and the obligation to notify it about the breach.

Intentional nature of the infringement (Article 83 (2) (b) of Regulation 2016/679).

The company made a conscious decision not to notify the President of the Personal Data Protection Office and the data subject about the breach, despite receiving information about the event from the processor and a letter from the President of the Personal Data Protection Office (UODO) addressed to it informing about the obligations incumbent on the controller in connection with the breach of data protection, such as also information on how the Company may report a breach, or finally, due to the initiation of administrative proceedings regarding the obligation to report a breach of personal data protection to the supervisory authority and notify the data subject about the breach. Such omission in this respect, despite the obligation to act "without undue delay", made it impossible for a natural person to take action as soon as possible to protect himself against any

negative effects of the breach, which in turn does not affect their effectiveness in the event of doing so. obligation by the Company.

The degree of cooperation with the supervisory authority in order to remove the breach and mitigate its possible negative effects (Article 83 (2) (f) of Regulation 2016/679).

In the present case, the President of the Personal Data Protection Office found the cooperation with him on the part of the Company unsatisfactory. This assessment concerns the reaction of the Company to the letter of the President of the Personal Data Protection Office informing about the obligations incumbent on the controller in connection with the breach of data protection, as well as information on how the Company may report the breach, and finally, in the case of initiating administrative proceedings regarding the obligation to report a breach of data protection. personal data and notification of the data subject's breach. Correct, in the opinion of the President of the Personal Data Protection Office (UODO), the actions (notification of the infringement to the President of the Personal Data Protection Office and notification of the person affected by the infringement) were not initiated by the Company even after the President of the Personal Data Protection Office initiated the administrative procedure in the matter.

Categories of personal data affected by the breach (Article 83 (2) (g) of Regulation 2016/679).

Personal data made available to an unauthorized person do not belong to special categories of personal data referred to in art. 9 of Regulation 2016/679, however, their wide scope (name and surname, city, postal code, PESEL number, data on the financial / property status of the data subject in the form of the subject and product of insurance - house against fire and random events, civil liability in private life , option of extending the scope of insurance, sum insured / guaranteed sum, amount of premiums, insurance period), is associated with a high risk of violating the rights and freedoms of natural persons.

How the supervisory authority learned about the breach (Article 83 (2) (h) of Regulation 2016/679).

The President of the Personal Data Protection Office (UODO) was not informed about the breach of the protection of personal data being the subject of this case, i.e. disclosure of personal data processed by the Company as the data controller to an unauthorized person, in accordance with the procedure specified in Art. 33 of the Regulation 2016/679. The fact that there is no information about a breach of data protection from the controller obliged to provide such information to the President of the Personal Data Protection Office should be considered as incriminating this controller.

When determining the amount of the administrative fine, the President of the Personal Data Protection Office also took into

account the mitigating circumstances affecting the final penalty, i.e .:

Number of data subjects affected (Article 83 (2) (a) of Regulation 2016/679).

In the present case, it was established that the breach concerned the personal data of only one person. Such a number of persons affected by the infringement, especially in view of the fact that the Company - due to the scale and scope of its activities - processes the personal data of a very large number of clients (insured persons and policyholders), should be considered small, which undoubtedly constitutes a mitigating circumstance in the present case .

Actions taken by the controller or processor to minimize the damage suffered by data subjects (Article 83 (2) (c) of Regulation 2016/679).

The company approached the wrong recipient with a request to permanently delete the correspondence received. Such activity of the Company deserves recognition and approval, however, it is by no means tantamount to the guarantee of the actual removal of personal data by an unauthorized person and does not exclude possible negative consequences of their use for data subjects.

The sanctions in the form of an administrative fine, as well as its amount, were not affected by the other sanctions indicated in Art. 83 sec. 2 of Regulation 2016/679, the circumstances:

a) the degree of responsibility of the controller, taking into account technical and organizational measures implemented by him pursuant to Art. 25 and 32 (Article 83 (2) (d) of Regulation 2016/679) - the breach assessed in this proceeding (failure to notify the President of the Personal Data Protection Office of the breach of personal data protection and failure to notify about the breach of personal data protection of the data subjects) is not related to the by the administrator with technical and organizational measures;

b) relevant previous violations of the provisions of Regulation 2016/679 by the administrator (Article 83 (2) (e) of Regulation 2016/679) - no previous violations of the provisions of Regulation 2016/679 by the Company were found;

c) compliance with previously applied measures in the same case, referred to in Art. 58 sec. 2 of Regulation 2016/679 (Article 83 (2) (i) of Regulation 2016/679) - in this case, the President of the Personal Data Protection Office has not previously applied the measures referred to in the indicated provision;

(d) adherence to approved codes of conduct pursuant to Art. 40 of the Regulation 2016/679 or approved certification mechanisms pursuant to Art. 42 of Regulation 2016/679 (Article 83 (2) (j) of Regulation 2016/679) - the administrator does not

apply approved codes of conduct or approved certification mechanisms ;;

e) financial gains or losses avoided, directly or indirectly, as a result of the breach (Article 83 (2) (k)) - the controller was not found to obtain any gains or avoided financial losses from the breach.

In the opinion of the President of the Personal Data Protection Office, the applied administrative fine performs the functions referred to in Art. 83 sec. 1 of Regulation 2016/679, i.e. it is effective, proportionate and dissuasive in this individual case.

It should be emphasized that the penalty will be effective if its imposition leads to the fact that the Company, which processes personal data professionally and on a mass scale, will in the future fulfill its obligations in the field of personal data protection, in particular with regard to reporting a breach of personal data protection. President of the Personal Data Protection Office and notifying about a breach of personal data protection of persons affected by the breach.

In the opinion of the President of the Personal Data Protection Office, the administrative fine will fulfill a repressive function, as it will be a response to the Company's breach of the provisions of Regulation 2016/679. It will also fulfill a preventive function; in the opinion of the President of the Personal Data Protection Office, he will indicate to both the Company and other data administrators the reprehensibility of disregarding the obligations of administrators related to the occurrence of a breach of personal data protection, and aimed at preventing its negative and often severe consequences for the persons affected by the breach, as well as removing these effects or at least limiting them.

Pursuant to art. 103 of the Act of May 10, 2018 on the Protection of Personal Data (Journal of Laws of 2019, item 1781), the equivalent of the amounts expressed in euro, referred to in Art. 83 of the Regulation 2016/679, are calculated in PLN according to the average EUR exchange rate announced by the National Bank of Poland in the exchange rate table on January 28 of each year, and if the National Bank of Poland does not announce the average EUR exchange rate on January 28 in a given year - according to the average euro exchange rate announced in the table of exchange rates of the National Bank of Poland that is closest after that date.

Bearing in mind the above, the President of the Personal Data Protection Office, pursuant to art. 83 sec. 4 lit. a) in connection with Art. 103 of the Act of May 10, 2018 on the Protection of Personal Data, for the violation described in the operative part of this decision, imposed on the Company - using the average EUR exchange rate of January 28, 2021 (EUR 1 = PLN 4.5479) - an administrative fine in the amount of PLN 159,176 (which is equivalent to EUR 35,000).

In the opinion of the President of the Personal Data Protection Office, the applied fine in the amount of PLN 159,176 (in words:

one hundred and fifty-nine thousand one hundred and seventy-six zlotys) meets the conditions referred to in Art. 83 sec. 1 of Regulation 2016/679 due to the seriousness of the breach found in the context of the basic objective of Regulation 2016/679 - the protection of fundamental rights and freedoms of natural persons, in particular the right to the protection of personal data. Referring to the amount of the administrative fine imposed on the Company, the President of the Office for Personal Data Protection decided that it is proportional to the financial situation of the Company and will not constitute an excessive burden for it.

The amount of the fine has been set at such a level that, on the one hand, it constitutes an adequate reaction of the supervisory body to the degree of violation of the administrator's obligations, on the other hand, it does not result in a situation in which the necessity to pay a financial penalty will entail negative consequences, in the form of a significant reduction in employment or a significant decrease in the Company's turnover. According to the President of the Personal Data Protection Office, the Company should and is able to bear the consequences of its negligence in the field of data protection, as evidenced by, for example, the Company's financial statements for the period from [...] January 2020 to [...] December 2020, sent to the President of the Personal Data Protection Office on […] February 2021

In this factual and legal state, 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: 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 2019, item 2325, as amended). A party (natural person, legal person, other organizational unit without legal personality) has the right to apply for the right to 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.

Pursuant to Art. 105 paragraph. 1 of the Act of May 10, 2018 on the Protection of Personal Data (Journal of Laws of 2019, item 1781), the administrative fine must be paid within 14 days from the date of expiry of the deadline for lodging a complaint to the Provincial Administrative Court, or from on the day the ruling of the administrative court becomes legally binding, to the bank account of the Personal Data Protection Office at NBP O / O Warsaw no. 28 1010 1010 0028 8622 3100 0000. Moreover,

pursuant to Art. 105 paragraph. 2 above of the Act, the President of the Personal Data Protection Office may, at the justified request of the punished entity, postpone the date of payment of the administrative fine or divide it into installments. In the event of postponing the payment of the administrative fine or dividing it into installments, the President of the Personal Data Protection Office shall charge interest on the unpaid amount on an annual basis, using a reduced rate of late payment interest, announced pursuant to Art. 56d of the Act of August 29, 1997 - Tax Ordinance (Journal of Laws of 2020, item 1325, as amended), from the day following the date of submitting the application.

Pursuant to Art. 74 of the Act of May 10, 2018 on the Protection of Personal Data (Journal of Laws of 2019, item 1781), the submission of a complaint by a party to the administrative court suspends the execution of the decision on the administrative fine.

2021-06-21