THE CHAIRMAN OF PERSONAL DATA PROTECTION

Warsaw, day 11

January

2021

DECISION

DKN.5131.7.2020

Based on Article. 104 § 1 of the Act of 14 June 1960 Code of Administrative Procedure (Journal of Laws of 2020, item 256, as amended), 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. i), art. 83 sec. 1 - 3 and art. 83 sec. 4 lit. a) in connection with Art. 33 sec. 1 of the Regulation of the European Parliament and of the EU Council 2016/679 of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46 / EC (general regulation on data protection) (Journal of Laws UE L 119 of May 4, 2016, p. 1 and Journal of Laws UE L 127 of May 23, 2018, p. 2), hereinafter also referred to as "Regulation 2016/679", failure to notify the personal data protection breach to the President of the Personal Data Protection Office by ENEA SA with headquarters in Poznań at ul. Górecka 1, President of the Office for Personal Data Protection,

finding a breach by ENEA S.A. with headquarters in Poznań at ul. Górecka 1, the provision of Art. 33 paragraph 1 of Regulation 2016/679, consisting in not reporting to the President of the Personal Data Protection Office a breach of personal data protection without undue delay, no later than 72 hours after the breach has been found, it is imposed on ENEA S.A. with headquarters in Poznań at ul. Górecka 1, an administrative fine in the amount of PLN 136,437 (in words: one hundred and thirty-six thousand four hundred and thirty-seven zlotys).

Justification

The Office for Personal Data Protection, hereinafter also referred to as "UODO", on [...] June 2020, received information about a breach of personal data protection from a person who became an unauthorized addressee of the personal data in question. The breach consisted in sending by a person associated with ENEA S.A. with its registered office in Poznań at ul. Górecka 1, hereinafter also referred to as the "Company", to the unauthorized recipient of the e-mail with an attachment containing the personal data of the addressee and two hundred and fifty-nine other persons (the Company's clients), as a result of which

there was a breach of data confidentiality in in the scope of: names, surnames, e-mail addresses, telephone numbers and information on the date of registration in […]. The person who sent (using an e-mail account other than his business account) the message along with the incorrect, unencrypted file containing personal data was (as follows from the later explanations of the Company) an associate of the company with which the contractor conducts qualitative research for the Company (P . Ltd).

In connection with the above, on [...] June 2020, the President of the Personal Data Protection Office, hereinafter also referred to as 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 the above-mentioned e-mail to an unauthorized recipient, the incident was analyzed in terms of the risk of violating the rights and freedoms of natural persons, necessary to assess whether to breach of data protection resulting in the need to notify the President of the Personal Data Protection Office and the persons concerned by the breach. 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 delivery of the letter.

In response to the above, the Company, in a letter of [...] June 2020, confirmed that a breach of personal data protection consisting in disclosure of personal data to an unauthorized recipient took place. Moreover, the Company indicated that an assessment was made in terms of the risk of violating the rights and freedoms of natural persons. On its basis, the Company concluded that there was no breach resulting in the need to notify the President of the Personal Data Protection Office, because:

1) the data was not of a special nature,

2) the administrator knows the identity of the person to whom the data has been disclosed and has received a declaration from him that he has permanently destroyed the attachment to which he was not authorized to receive.

Moreover, the Company emphasized that "due to the quick actions taken, we have eliminated the possibility that the event could have negative consequences for the data subjects".

In connection with the above-mentioned in the letter, due to the risk assessment of violation of the rights and freedoms of data subjects, the President of the Personal Data Protection Office in a letter of [...] July 2020 informed the Company that "in accordance with Art. 33 paragraph 1 above of the regulation, 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 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. " Moreover, in the letter, he indicated to the Company, inter alia, that "When assessing whether the violation results in a risk of violating the rights or freedoms of natural persons, one should take into account, inter alia, the content of recitals 75 and 85 of the above-mentioned regulation. Moreover, the Article 29 Working Party in the Guidelines on reporting personal data breaches in accordance with Regulation 2016/679 (WP250rev.01) [1] indicated that the controller, when assessing the risk to individuals resulting from the breach, should take into account »the specific circumstances of the breach, including the importance of potential impact and the likelihood of its occurrence ”and recommended that the assessment should take into account the criteria indicated in these Guidelines. In the above-mentioned The guidelines also explain 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 ””. At the same time, the President of the Personal Data Protection Office called the Company pursuant to Art. 58 sec. 1 lit. a) and e) of Regulation 2016/679 to provide information whether, in connection with the incident, the incident was re-analyzed in terms of the risk of violating the rights and 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 Data Protection Office People and persons affected by the violation, and if so, whether the results of the re-analysis are identical to the results of the previously conducted assessment by the administrator of the above-mentioned the event, and also called for explanations within 7 days from the date of delivery of the letter.

In a reply of [...] July 2020, the Company explained that it had re-analyzed the risk, which showed a result similar to the analysis carried out by the administrator on [...] June 2020, i.e. it concluded that there was a low probability of infringement of rights. or the freedom of the data subjects. Annex 1 to this letter was "Analysis of secondary breach of personal data protection" illustrating the course of the Company's analysis of the risk of violating the rights or freedoms of natural persons. In the letter sent, the company also drew attention to the remedial measures it had taken, stressing that “The remedial actions made it possible to eliminate the possibility that the incident could have negative consequences for the data subjects. Significant for the result of both analyzes is the fact that the incident concerned basic data (i.e. name, surname, e-mail

address, telephone number and date of registration), and that the controller knows the identity of the person to whom personal data was disclosed by mistake. The administrator also received on [...] .06.2020 a statement from the person to whom the data were disclosed that he had permanently destroyed the attachment with personal data, to which the person was not authorized to receive. These remedies have eliminated the likelihood of a further breach of data protection in the present case. '

In connection with the above, the President of the Personal Data Protection Office (UODO) addressed the Company in a letter of [...] September 2020, in which he indicated, inter alia, that Art. 33 paragraph. 1 sentence 1 of Regulation 2016/679 states that: "In the event of a breach of personal data protection, the 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 it is unlikely that the violation would result in a risk of violating the rights or freedoms of natural persons "and stated that" Contrary to what was contained in the conclusions resulting from the analysis presented in the above-mentioned Annex 1, whether the rights or freedoms of natural persons have been violated is indifferent to the controller, whose obligation is to notify the supervisory authority of a breach of personal data protection "unless it is unlikely that this breach would result in a risk of violation of the rights or freedoms of natural persons" " . Moreover, it was emphasized that "the submission of a declaration by an identifiable person about the permanent destruction of the attachment with personal data does not eliminate the risk of breach of personal data protection at all - especially considering that the Company did not receive information on possible further disclosure of this data by an unauthorized recipient. In addition, the Company should take into account, for example, the fact that the breach of data protection took place on [...] June 2020, and the above statement (regardless of the assessment of its severity and effects) was submitted only on [...] June 2020 - if the statement submitted by an unauthorized recipient was to eliminate the risk of breach of personal data protection, this risk existed for five days ”. In this letter, the President of the Personal Data Protection Office asked the Company pursuant to Art. 58 sec. 1 lit. a) and e) of Regulation 2016/679 to submit, within 7 days from the date of delivery of this letter, explanations regarding, inter alia, what possible "Remedial actions", mentioned in the letter of [...] July 2020, not constituting obtaining from an unauthorized recipient e-mails of the declaration of permanent destruction of the attachment "made it possible to eliminate the possibility that the incident could have negative consequences for the data subjects".

By letter of [...] September 2020, the Company provided explanations, which show, inter alia, that "the Company (...) learned about the breach of data protection on [...] June 2020. On the same day, the Company's sub-supplier contacted the

unauthorized the recipient of the data, i.e. the Company immediately took remedial actions which eliminated the risk of data breach from the very first day. On [...] June 2020, the unauthorized recipient, in a telephone conversation with an employee of the Company, stated that he would permanently delete the data. Unauthorized recipient on [...] June 2020 committed to permanent deletion, and only confirmation of this action took place on [...] June 2020. remedial measures so that the risk of violating the rights and freedoms of natural persons is eliminated. Referring to subsequent remedial actions, the Company carried out an analysis to identify the causes of the data protection incident and updated the documentation on: a) Selection of suppliers (processors) under the tender procedure in force in the Company (e.g. from the agreement that suppliers contacting customers are required to use the company's e-mail domain). b) Have the supplier instructed the supplier to re-train in the correct addressing and sending of correspondence by its employees. ' In the opinion of the President of the Personal Data Protection Office, the Company did not demonstrate any additional remedial measures reducing the risk of violating the rights or freedoms of data subjects related to the event in question.

In the absence of notification of the breach of personal data protection to the President of the Personal Data Protection Office, on [...] October 2020, the President of the Personal Data Protection Office initiated administrative proceedings against the Company (letter reference: [...]).

In response to the notification of the initiation of administrative proceedings, the Company, by letter of [...] October 2020, informed that:

1. As a result of the violation, there was no physical damage, property damage or non-material damage to natural persons, such as control over own personal data or limitation of rights, discrimination, theft or falsification of identity, financial loss, unauthorized reversal of pseudonymization, violation of good name, violation the confidentiality of personal data protected by professional secrecy or other economic or social damage referred to in recital 85 of the GDPR Preamble. In view of the above, bearing in mind the principle of accountability and based on a risk analysis conducted by the data protection officer of ENEA S.A. and an external Law Firm (specializing in the provisions on the protection of personal data, to which the Company applied for support), the Company decided that it is unlikely that this breach could cause a risk of violating the rights or freedoms of clients whose personal data was in the mistakenly sent database .

2. In addition to permanent cooperation with the contractor, ie P. Sp. z o.o., in order to clarify the circumstances of the event, including receipt of significant statements, ENEA S.A. verified that the processing entity, ie P. Sp. z o.o. or subcontractors of

the processor, to other violations. As part of this verification [...] Enea S.A. contacted persons whose data was in the possession of P. Sp. z o.o. in order to determine from which e-mail addresses the persons performing the order on the part of P. Sp. z o.o. contacted customers and what was the quality of the services provided. The company has also drawn civil law consequences in relation to the Contractor. It is clear from the above that Enea SA, as the data controller, took, apart from all necessary actions necessary to clarify the case, also additional actions to reliably and thoroughly explain the event in question and to check whether there were any other events that could result in violation of rights and the freedom of individuals.

In addition, to the above-mentioned The company attached the letter "a second statement on the deletion of personal data, issued by Mr. (...) who obtained unauthorized access to the personal data of ENEA S.A. clients. as a result of an error by Mr. (...), working on the tests on the part of the Contractor ENEA S.A. ie P. Sp. z o.o. The indicated declaration confirms that the data of ENEA S.A.'s clients: a) were immediately deleted by Mr. (...), b) were not copied or made available to other persons by Mr. (...) ".

Consequently, in the opinion of the Company's data protection officer, there was no need to report the infringement to the President of the Personal Data Protection Office in this case.

Due to the fact that the above-mentioned letters addressed to the Office for Personal Data Protection were signed by the data protection officer, and not by the representatives of the Company in accordance with the representation method disclosed in the Register of Entrepreneurs kept by the National Court Register, on [...] December 2020 In the year, the Company was asked, inter alia, to provide the local Office with the missing document: a power of attorney granted to an employee of the Company responding to correspondence addressed to the administrator by the President of the Office for Personal Data Protection. In response, the Company sent the above-mentioned letter to the Office for Personal Data Protection on [...] December 2020 (previously sent on [...] October 2020 and then signed by the data protection officer), dated on [...] December 2020 the signatures of two members of the management board of the Company. The letter of [...] December 2020 also contains, inter alia, an explanation that "(...) all letters sent to the Personal Data Protection Office and signed by IOD Enea S.A. are previously consulted and approved by the Administrator".

In response to the notification on the collection of evidence sent to the Company on [...] January 2021, on [...] January 2021, the Company sent a letter in which it maintained the current positions presented in correspondence with the Office for Personal Data Protection from June 2020, and also referred to, inter alia, to the issue of not reporting the incident to the President of the

Personal Data Protection Office. The company indicated that the analyzes of the incident were carried out on the basis of the guidelines of the European Union Agency for Network and Information Security (ENISA), 2013, Recommendations for a methodology of the assessment of severity of personal data breaches and that by applying them, it obtained a risk score at the WN level <2 that is: "People will not be affected by the breach or will cause minor inconvenience." The company also drew attention to the "key components of the risk analysis", pointing to (quoted):

1. Type and level of data sensitivity - unauthorized disclosure of personal data pertained to name, surname, e-mail address, telephone number and information on the registration date. The above-mentioned scope of data that was unauthorized disclosure constitutes basic data, not behavioral data (falling within the scope of the so-called behavioral data). We also point out that data on a person's behavior can be obtained by profiling, as referred to in art. 4 pts 4 GDPR. However, as part of our activities, we do not conduct profiling, and the mere information about the date of registration in [...] is not a sufficient condition to recognize that we are dealing with information about preferences. Moreover, it should be clearly stated that customers register with […] as they receive discount coupons, so it is even less possible to speak of any specific information regarding preferences here. It would be different in the case of indicating, for example, the scope of purchases made, which, however, was not covered by the database in question.

2. Possibility of identification - basing on ENISA, we note that the analyzed facts existed. Limited possibility of identification - occurs when the circle of recipients is small and in the scope of data there is no PESEL registration data. We would like to emphasize that the unauthorized recipient immediately deleted the data to which he gained access as a result of a subcontractor's mistake. Moreover, he also submitted a declaration of confidentiality.

Moreover, in the above-mentioned in a letter of [...] January 2021, describing the remedial measures taken, the Company stated, inter alia, that it terminated the contract with P. Sp. z o.o. due to the failure to meet the safety standards to which P. Sp. z o.o. was obliged by an agreement with the Company and "introduced stricter requirements regarding the minimum technical and organizational measures to be met by the Contractor (despite the fact that the existing ones were compliant with the applicable legal standards)". The company also filed for "the non-imposition of a penalty or its extraordinary mitigation" due to its taking the necessary measures to "limit or even eliminate the effects of this violation".

After reading 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 provide 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) contain the name and contact details of the data protection officer, or designate 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.

The content of the above-mentioned provisions of Regulation 2016/679 shows that in the event of a breach of personal data protection on the part of the data controller, an obligation arises to report it to the President of the Personal Data Protection Office, if the breach involves a risk of violating the rights or freedoms of natural persons - regardless of the level of this risk.

In the case in question, which is clear from the findings made, an e-mail with an attachment in the form of an unencrypted file containing personal data of the recipient of the message and two hundred and fifty-nine other persons (names, e-mail addresses, phone numbers) was sent to the unauthorized recipient. phone numbers, as well as information about the date of registration). This means that there was a security breach leading to the accidental disclosure of the data of two hundred and fifty-nine persons to an unauthorized person, and thus a breach of the confidentiality of these persons' data, which makes a personal data breach.

Violation of the protection of personal data (data confidentiality) that occurred in this case, contrary to the claims of the Company contained in the correspondence addressed to the President of the Personal Data Protection Office, results in the risk of violating the rights or freedoms of natural persons. As indicated by the Article 29 Working Party in the guidelines on reporting personal data breaches in accordance with Regulation 2016/679, hereinafter also referred to as "guidelines": "When

assessing the risk to individuals resulting from the breach, the controller should therefore take into account the specific circumstances of the breach, including the importance of the potential impact and the likelihood of it occurring. The Article 29 Working Party therefore recommends that the assessment should take into account the following criteria: (…) Number of individuals affected by the Breach A Breach may only affect one person, several or several thousand or many more. Typically, the potential impact of a breach increases with the number of people affected. However, depending on the nature of the personal data and the context in which they were disclosed, a breach could have serious consequences for up to one individual. Again, the most important thing is to analyze the likelihood of consequences for the people affected by the breach and how severe the consequences will be. ' There is no doubt that in the case at hand, the infringement concerns many people, which significantly increases the gravity of the infringement and the probability of materialization of threats related to the infringement. Another important factor for such a risk assessment is the possibility of easy identification of persons whose data was affected by the breach, based on the disclosed data - the fact that the breach did not reveal, for example, PESEL identification numbers of persons affected by it, does not mean that these persons cannot be identify. As a consequence, this means that there is a risk of violation of the rights or freedoms of the persons covered by the violation, which in turn results in the emergence of the Company, as the data controller, of an obligation to report the violation of personal data protection to the supervisory authority, 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.

In the case at hand, as already mentioned, the personal data of two hundred and fifty-nine persons was disclosed in the form of: names, surnames, e-mail addresses, telephone numbers, and information on the registration date. Disclosure of such data is not associated with a high risk of violation of the rights or freedoms of natural persons, which is determined by, inter alia, the circumstance raised by the Company that as a result of a breach of personal data protection, no data on the behavior of these persons (their preferences) were disclosed (and thus, the Company was not obliged to notify the data subjects of the breach, pursuant to Art. 34 of Regulation 2016/679), however, this risk exists in such a case - hence the need to notify the President of the Personal Data Protection Office of the infringement. The possible risk related to the event that has occurred is, in particular, the loss of data subjects' control over their data. These data may, for example, be used by persons who come into their possession, e.g. for unwanted by data subjects, contacts by e-mail or telephone - also those during which attempts will be made to obtain additional data of these persons. Finally, using this data, accounts can be set up in various types of social

networking sites and internet portals, which may have a negative impact on the perception of these people in their professional or family environment, and even lead to their discrimination. Therefore, the above means that in the case of the personal data breach in question, there is a risk of violating the rights or freedoms of natural persons.

It is worth emphasizing that the possible consequences of the event that occurred do not have to materialize - in the content of Art. 33 paragraph 1 of Regulation 2016/679, it was indicated that the mere occurrence of a breach of personal data protection, which involves the risk of violating the rights or freedoms of natural persons, implies an obligation to notify the breach to the competent supervisory authority. Therefore, the circumstance raised by the Company that the following quotation: "as a result of the breach, there was no physical damage, property or non-material damage to natural persons, such as control over own personal data or limitation of rights, discrimination, theft or falsification of identity, financial loss, unauthorized reversal of pseudonymisation, breach of good name, breach of confidentiality of personal data protected by professional secrecy or other economic or social damage referred to in recital 85 of the GDPR Preamble "is not relevant for the determination of the Company's obligation to report the breach of personal data protection to the President of the Personal Data Protection Office, in accordance with Art. 33 paragraph 1 of Regulation 2016/679.

For the above assessment of the risk of violation of the rights or freedoms of natural persons related to the event, the fact of requesting an unauthorized recipient to permanently delete the correspondence received, or even submitting a declaration by that person about its permanent removal, is not affected. Even in spite of the declarations made in the case at hand, there is no certainty that before these activities the person did not e.g. make a photocopy or did not record the personal data contained in the document in another way, e.g. by writing them down. Therefore, the mere performance of activities indicated in the declarations submitted by an unauthorized recipient does not provide any guarantees 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 the persons whose data was affected by the breach. The same applies to a possible declaration of destruction of the correspondence received, because the Company cannot actually verify it. 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 and treating an unauthorized recipient as a "trusted recipient", which determines the existence of a risk of violation of rights or freedoms for the persons covered by the violation in question. In order to establish the existence on the part of the Company of the obligation to notify the President of the Personal Data Protection Office of the above-mentioned breach of personal data protection, in accordance with art. 33 paragraph 1 of Regulation 2016/679, it is also irrelevant that the Company has taken actions to minimize the risk of recurrence of the breach, as indicated in correspondence with the supervisory body, in particular in response to the notification of initiation of administrative proceedings and in the letter of [...] January 2021. The nature of these activities indicates that they are to prevent the occurrence of such violations in the future; On the other hand, these activities do not in any way affect the assessment that due to the occurrence of the data protection breach in question there is a risk of violation of rights and freedoms. Moreover, 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".

At the same time, it should be emphasized that the Company, allowing the possibility of using e-mail for communication with the client, should be aware of the risks related to, for example, attaching an incorrect attachment to the message sent. The existence of these risks, in the absence of actions of the data controller aimed at minimizing them by implementing appropriate organizational and technical measures, such as encryption of documents sent in this way, directly leads to the risk of violating the rights or freedoms of natural persons whose data through such communication channel are sent.

In a situation where, as a result of a breach of personal data protection, there is a risk of violation of the rights or 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. 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. '

Consequently, it should be stated that the Company did not notify the supervisory body of the breach of personal data protection within the period specified in Art. 33 paragraph 1 of the Regulation 2016/679, which means the Company's breach of this provision.

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 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 application of this type of sanction in the present case and having an aggravating effect on the amount of the fine imposed:

a) The number of data subjects affected (Article 83 (2) (a) of Regulation 2016/679); The violation found in the present case

concerns two hundred and fifty-nine persons and involves the risk of violating their rights or freedoms.

b) Duration of the infringement (Article 83 (2) (a) of Regulation 2016/679); The President of UODO considers the long duration of the infringement to be an aggravating circumstance. Since the Company became aware of a breach of personal data protection, that is from [...] June 2020 until the date of this decision, the Company has not fulfilled the obligation under Art. 33 of the Regulation 2016/679.

c) 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 about the infringement, despite receiving information about the event from an unauthorized recipient and letters from the President of the Personal Data Protection Office the possibility of the risk of violating the rights or freedoms of the persons affected by the violation in the present case.

d) The degree of responsibility of the administrator, 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 found was related to the lack of implementation or incorrect implementation by the Company of organizational and technical measures ensuring data security, i.e. encryption of files containing personal data that are sent in electronic messages.

e) The degree of cooperation with the supervisory body in order to remove the infringement and mitigate its possible negative effects (Article 83 (2) (f) of Regulation 2016/679); In this case, the President of the Personal Data Protection Office found that the Company's cooperation with it was unsatisfactory. This assessment concerns the reaction of the Company to the letters of the President of the Personal Data Protection Office pointing to the possible risk of violating the rights or freedoms of persons affected by the violation in this case. Correct, in the opinion of the President of the Personal Data Protection Office (UODO), the Company did not take the action (notification of the infringement to the President of the Personal Data Protection Office).

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. actions taken by the controller to minimize the damage suffered by the data subjects (Article 83 (2) (c) of Regulation 2016 / 679) - the Company turned to an unauthorized 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 fact that the President of the Office applied a sanction in the form of an administrative fine, as well as its amount, was not

affected by other sanctions specified in Art. 83 sec. 2 of Regulation 2016/679, the circumstances, i.e .:

a) the nature and gravity of the breach - the breach found in the present case is not of a significant and serious nature - the risk of violating the rights or freedoms of data subjects is not high (Article 83 (2) (a) of Regulation 2016/679);

b) relevant previous violations of the provisions of Regulation 2016/679 by the Company (Article 83 (2) (e) of Regulation 2016/679);

c) the categories of personal data concerned by the breach - personal data made available to an unauthorized person do not belong to specific categories of personal data referred to in art. 9 of the Regulation 2016/679, however, their scope (first and last names, telephone numbers, e-mail addresses and information on the date of registration) is associated with the risk of violating the rights or freedoms of natural persons (Article 83 (2) (g) of Regulation 2016 / 679);

d) the way in which the supervisory body learned about the breach - about the breach of personal data protection being the subject of this case, i.e. about the disclosure to an unauthorized person of personal data processed by the Company acting as the data controller, the President of the Personal Data Protection Office was not informed in accordance with the provisions for such data the situation with the procedure set out in Art. 33 of Regulation 2016/679 (Article 83 (2) (h) of Regulation 2016/679);

e) 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);

(f) 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);

g) financial benefits gained directly or indirectly as a result of the infringement or avoided losses (Article 83 (2) (k) of Regulation 2016/679).

In the opinion of the President of the Personal Data Protection Office (UODO), 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.

We are dealing with a breach of data protection both when an event occurs as a result of deliberate action and when it is caused inadvertently - the fact that the breach occurred as a result of a mistake does not release the administrator from the obligations set out in Art. 33 paragraph 1 of Regulation 2016/679 - hence the application of an administrative fine in this case is justified.

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 that the disrespect of the controllers' obligations related to the occurrence of a breach of personal data protection, and aimed at preventing its negative and often painful consequences for the persons affected by the breach, as well as removing these effects or at least a limitation.

Pursuant to art. 103 of the Act of 10 May 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 to that date.

In connection with the above, it should be noted that a fine of PLN 136,437 (in words: one hundred and thirty-six thousand four hundred and thirty-seven zlotys), which is the equivalent of EUR 30,000 (average EUR exchange rate from January 28, 2021 - PLN 4.5479) , 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.

In this factual and legal state, the President of the Personal Data Protection Office resolved as in the sentence.

[1] https://www.uodo.gov.pl/pl/10/12.

2021-02-23