THE CHAIRMAN OF PERSONAL DATA PROTECTION

Warsaw, day 14

October

2021

DECISION

DKN.5131.16.2021

Based on Article. 104 § 1 of the Act of June 14, 1960 Code of Administrative Procedure (Journal of Laws of 2021, item 735, 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) and h), 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 sec. 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 conducting 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 by the Bank about the breach of personal data protection. Millennium S.A. [...], President of the Personal Data Protection Office,

1) finding a breach by Bank Millennium S.A. [...] regulations:

a) Art. 33 sec. 1 of Regulation 2016/679, consisting in not reporting to the President of the Personal Data Protection Office the breach of personal data protection without undue delay, no later than 72 hours after the breach has been found, and b) art. 34 sec. 1 of Regulation 2016/679, consisting in not notifying about a breach of personal data protection, without undue delay of data subjects,

imposes on Bank Millennium S.A. [...] an administrative fine in the amount of PLN 363,832 (say: three hundred and sixty-three thousand eight hundred and thirty-two zlotys),

2) orders Bank Millennium S.A. [...] notification - within 3 days from the date of notification of this decision - to Ms M. G. and Mr W. G. about a breach of the protection of their personal data in order to provide them with the information required pursuant to

Art. 34 sec. 2 of Regulation 2016/679, i.e.: a) description of the nature of the personal data breach; b) name and contact details of the data protection officer or designation of another contact point from which more information can be obtained; c) description of the possible consequences of the data breach d) a description of the measures taken or proposed by the controller to remedy the breach - including measures to minimize its possible negative effects.

Justification

The President of the Personal Data Protection Office, hereinafter also referred to as the "President of the Personal Data Protection Office", on [...] June 2019, received a complaint from Ms M. G. and Mr W. G., hereinafter referred to as: "Complainants", about irregularities in the processing of their personal data by Bank Millennium ARE. [...], hereinafter referred to as: "the Bank" or the "Administrator", consisting in the loss of documentation containing the personal data of the Complainants, provided to the Bank in connection with the procedure of opening a bank account on [...] March 2019.

In the content of the complaint, the complainants indicated that the Bank Branch in Z. had lost their personal data, provided in connection with the procedure of opening a bank account on [...] March 2019. The complainants indicated that on [...] May 2019 they had been notified of the loss of documentation containing their personal data. On [...] May 2019, the Complainants visited the Bank in order to obtain additional information on this matter, i.e. how they can avoid possible negative consequences and what they should do in this situation. The complainants did not obtain such information, and therefore submitted a complaint at the Bank's outlet.

Therefore, in a letter of [...] September 2019, the President of the Personal Data Protection Office, pursuant to Art. 58 sec. 1 lit. a) and e) of Regulation 2016/679, asked the Bank to clarify whether, in connection with the event, the Bank reported, pursuant to Art. 33 of the Regulation 2016/679, personal data breach to the President of UODO in the above scope, and if so, when and whether the Bank has fulfilled the obligation to notify data subjects about the breach of their personal data, pursuant to art. 34 sec. 1 and 2 of Regulation 2016/679. The President of the Personal Data Protection Office also asked for an indication of what categories of data the breach concerned, what are its possible consequences for the data subjects, and if and if so, what remedial measures were applied by the Bank to minimize the possible negative effects of the breach, and which took measures to prevent any future violations of a similar nature.

The response to the above, which the Bank provided in the letter of [...] October 2019, shows that on [...] April 2019, the Bank's branch sent to the Bank's Head Office a letter containing the following documents: Power of attorney granted to the

Complainant by the Complainant , Profit savings account agreement, Bank account agreement and debit card agreement, Framework agreement for the provision of financial services, Bank account agreement, Confirmation of changes to the bank account agreement, Card agreement [...], Investment survey, Investment survey result. On the above-mentioned the documents contained in particular the following data: name, surname, PESEL number, registered address, bank account numbers, CIF number (identification number assigned to the Bank's clients) of the complainant and the complainant's name, surname and PESEL number.

As it results from the submitted explanations, the parcel containing the above-mentioned the documents should reach the Bank's Head Office on [...] April 2019. On [...] April 2019, the Bank took steps to clarify with the courier company X Sp. z o.o., hereinafter referred to as: "X", delay in delivery of the above-mentioned shipment. Then, on [...] April 2019, the Bank made an official complaint regarding the failure to deliver the above-mentioned shipment. On [...] April 2019, the courier company informed the Bank about the change in the status of the above-mentioned the shipment to the status of lost, informing that despite this, it still tries to clarify the matter. On [...] May 2019, the courier company informed the Bank that it had not been able to locate the parcel and had finished searching for it.

Considering the above circumstances of the event, including the scope of data to which the incident concerned the incident, the Bank, in accordance with the methodology based on the European ENISA methodology, assessed the event as likely to cause an average risk of violating the rights and freedoms of the Complainants, therefore the Bank did not report the above-mentioned infringement to the President of the Personal Data Protection Office and did not notify persons about the breach of their personal data in accordance with art. 34 sec. 1 of Regulation 2016/679, indicating to them in the information about lost documents only very general information about the nature of the breach (without indicating the category of data covered by the breach) and measures to minimize its possible negative effects, including allowing the Complainants to use the free Alert service [... ]. This information, however, did not contain any information about the consequences of the breach of personal data protection in question (Article 33 (3) (c) of Regulation 2016/679) and the information indicated in Art. 33 sec. 3 lit. b of the Regulation 2016/679, i.e. the name and contact details of the Data Protection Officer or the designation of another contact point from which more information can be obtained. There is also no reference to the security measures applied by the Administrator in order to minimize the risk of a recurrence of the breach.

Due to the lack of notification of 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 persons, on [...] April 2021, the President of the Personal Data Protection Office initiated administrative proceedings against the Bank in this regard.

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

1. During the period in which the incident covered by the complaint took place, only the laconic Article 29 Working Party Guidelines on reporting personal data breaches in accordance with Regulation 2016/679 (WP250rev.01), i.e. the guidelines adopted on 3 October 2017 by The Article 29 Working Party and subsequently endorsed by the European Data Protection Board (hereinafter "EDPB"), which guidelines (hereinafter referred to as "WP250 Guidelines"), according to the Bank, quoted: in any way similar to it, and the same indicated in the above-mentioned of the Guidelines, examples concerned events so serious that they could suggest to the recipients that notifications pursuant to Art. 33 of the GDPR should be reserved for specific cases "; 2. The bank, pointing to the lack of in the above-mentioned of the Guidelines, a case similar to the one to which the present proceedings relate, at the same time indicated that most of the formally lost shipments remain intact, without leaving the suppliers' infrastructure, as there are often cases when shipments fall off the conveyor belt, which gives them the status of lost; 3 . In the Bank's opinion, not in every case disclosure of data in the form of a PESEL number poses a high risk to the rights and freedoms of the injured person, including the risk of identity theft; It is also difficult to agree with the far-reaching consequences of its disclosure, such as the possibility of taking a loan - such situations as a result of obtaining a PESEL number are rare, if at all possible now, and in addition, quoted: "[...] neither banks nor lenders as obliged entities on the basis of the AML regulations, for the verification of the identity document, they cannot provide financing based on the PSESEL number alone or the PESEL number in conjunction with other information "; 4. PESEL numbers of members of legal entities' bodies (e.g. members of the Bank's management board) are publicly available, however, the Bank has no information about extorting loans for their data, using the data in connection with granting a mandate, extorting insurance funds to their detriment. etc.; 5. The bank reports violations that may have resulted in the disclosure of data, including PESEL number, but it does not treat this as an absolute rule and does not adopt "global" guidelines that always require the adoption of a high-risk assessment in the event of disclosure of the PESEL number; 6. The bank referred to Art. 87 of Regulation 2016/679, according to which Member States may define specific conditions for the processing of a national identification number or other identifier of general scope, while indicating that the following quotation: "In the case of Poland, the legislator has not decided to adopt

specific rules for processing the PESEL number for private entities; some special solutions were adopted in the Act of 24 September 2010 on population records, in chapter 6 "Providing data from the PESEL register and residents' registers" for entities requesting the disclosure of data from the register itself. This does not apply to situations where the PESEL number is disclosed by the data subject, e.g. for the purpose of concluding a contract. The fact that the legislator does not see the need for further detailing of the principles of data processing from registers suggests that its processing in itself does not pose a threat to citizens ”; 7. The Bank, as a result of a pro-consumer attitude, expressed in care for the interests of the Bank's customers, informed the Complainants about the event consisting in the loss of a parcel with documents by a courier, attaching it to the information on a breach of data protection, despite the assessment of the event as having an average impact on the rights and freedoms of persons, data subjects, and thus not requiring notification to the supervisory authority, a code for free use of the […] Alert service, as a measure to minimize any negative effects of the event; 8. Following the above assessment, the Bank, after making an assessment resulting in the recognition of the average risk of breach of personal data protection, despite the lack of such an obligation, on the one hand wanted to compensate the injured parties for any inconvenience, on the other hand, to provide the Bank with the possibility of reacting in the event of a failure, despite the low probability, to use the Complainant's data in the banking system in an unauthorized manner; 9. The information from the Bank shows that the Complainants' data were not used, for example, to extort a loan or attempt to extort such a fraud, the loss of the parcel did not cause any other inconvenience, which would suggest that the Bank's assessment was correct; 10. The Bank constantly supervises the quality of services offered by X, monitors the implementation of the proposed corrective actions and organizes meetings to discuss the possibilities of further improvement of the process, obtaining information on the details of X's operational activities, e.g. that many of the shipments formally recognized as lost are shipments that e.g. they fall off their self-propelled belts in a sorting plant, labels have peeled off etc., so they never leave the X infrastructure.

Moreover, the Bank attached to the submitted explanations the assessment made in terms of the risk of violating the rights and freedoms of natural persons. On the basis of this assessment, the Bank concluded that there was no breach resulting in the need to notify the President of the Personal Data Protection Office and the persons whose personal data the breach relates to. The assessment was made with the use of the personal data breach assessment calculator, which completed file along with the assessment methodology was sent as evidence with explanations. In addition, the Bank explained that it calculates an incident score on the basis of such elements as: the context of data processing, ease of identification and the circumstances of

the breach.

The data processing context (DPC) determines the type of data that has been disclosed as well as a number of factors related to the overall context of the processing. Ease of identification (EI) determines how easily the identity of individuals can be inferred from the data related to the incident. The circumstances of the breach (CB) describe the specific circumstances of the breach of personal data protection, mainly related to the breach of data security and confidentiality, as well as all activities related to a deliberate attack on the Bank's infrastructure.

Having read 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 violation would result in a risk of violating 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, where possible, the categories and approximate number of data subjects, and 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.

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 sec. 3 lit. b), c) and d) of Regulation 2016/679, i.e. a) name and contact details of the data

protection officer or designation of another contact point from which more information can be obtained; b) description of the possible consequences of a personal data breach; 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 violating 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 breach of personal data protection 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 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 negative consequences of the breach. It should be emphasized that 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.

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 the loss of documentation containing personal data of the Bank's clients in the scope of, among others: name, surname, PESEL number, registered address, bank account numbers , the CIF number (identification number assigned to the Bank's clients) of the complainant and the complainant's first and last name, PESEL number, pose a high risk of violating the rights or freedoms of 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 pursuant to Article 68 of Regulation 2016/679 by the European Personal Data Protection Board, which during the first plenary session of the EDPB approved, inter alia, the following guidelines) in WP250 Guidelines: "This risk exists where the breach may lead to physical or property damage or non-property for persons whose data has been violated. Examples of such damage include discrimination, identity theft or fraud, financial loss and damage to reputation. " There is no doubt that the examples of damages cited in the guidelines, due to the scope of data covered by this personal data breach, including the PESEL number together with the name, address or bank account numbers, may occur in the discussed case.

As a consequence, this means that there is a high risk of violation of the rights or freedoms of persons covered by the violation in question, which in turn results in the Bank being obliged to notify the breach of personal data protection to the supervisory authority, in accordance with Art. 33 sec. 1 of the Regulation 2016/679, which must contain the information specified in art. 33 sec. 3 of Regulation 2016/679 and notification of these persons 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.

When taking a stance on the Bank's explanations, it should first be pointed out that in connection with the personal data breach in question, consisting in the loss of documentation containing personal data of the Bank's customers, it is irrelevant whether the unauthorized recipient actually came into possession and became acquainted with the personal data of other persons, but the fact that there was such a risk, and consequently also a potential risk of violation of the rights or freedoms of data subjects, which should be considered high due to the scope of the data. In his explanations, the administrator emphasized that the information he had showed that the data was not used, for example, to extort a loan or attempt to extort such an extortion, the loss of the parcel did not cause any other inconvenience, therefore it concluded that the breach does not involve the risk of violating the rights or freedoms affected people. It is worth noting, however, that the Administrator foresaw that the breach may involve such a risk, as evidenced by the fact of offering an additional service [...] Alert as part of measures to remedy the

breach - according to the Bank, this would allow him to take an appropriate response in the event of if, as he himself points out, "despite the low probability, the Complainants' data would be used in the banking system in an unauthorized manner". At this point, it should be pointed out again that for the obligation to notify about a breach of personal data protection of data subjects, it is not necessary to materialize the negative consequences of the breach, the mere possibility (risk) of such consequences is sufficient in this respect, which in the present case , in the opinion of the supervisory authority, is high. Therefore, the circumstance raised by the Administrator that the following quotation is: "The information of the Bank shows that the Complainants' data were not used, for example, to extort a loan or attempt to extort such a loan, the loss of the parcel did not cause any other inconvenience [...]" and "the Bank did not receive any information about the Complainants' damage in connection with the event ", is irrelevant to the fact that there is an obligation on the part of the controller to report the breach of personal data protection to the President of the Personal Data Protection Office, pursuant to Art. 33 sec. 1 of the Regulation 2016/679, as well as due to the scope of personal data covered by the violation, notifications of data subjects about the violation.

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 is clear from Art. 33 sec. 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 or 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 importance of 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 sec. 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 data subjects, 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 data subjects, which in turn determines the obligation to report the breach of personal data protection to the supervisory authority and notify these persons about the breach. The Article 29 Working Party

in WP250 points out that “when assessing the risk 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 likelihood 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 occurrence of a breach of personal data protection, there were no factors reducing the probability of negative consequences, such as limited possibility of identification, finding that personal data are publicly available, or recognizing the wrong recipient as a "trusted" person.

The fact that the Bank did not notify the President of the Personal Data Protection Office in question to the President of the Personal Data Protection Office is all the more incomprehensible as the Administrator himself assumed an average level of this risk in the assessment of the risk of violation of the rights or freedoms of the Complainants. The risk of violating the rights or freedoms of natural persons determined at this level, contrary to the Bank's assertion, does not exclude the obligation referred to in Art. 33 sec. 1 of Regulation 2016/679. Therefore, according to the result of its own risk analysis carried out in connection with the breach, the bank should at least notify the supervisory authority of the breach, which, and it should be emphasized again, it did not do so.

The President of the Personal Data Protection Office in the publication entitled "Responsibilities of controllers related to breaches of personal data protection" indicates: "Depending on the level of risk of violation of the rights and freedoms of natural persons, the controller has to deal differently with its obligations towards the supervisory authority and data subjects. If, as a result of the analysis, the controller concluded that the probability of the risk of violating the rights and freedoms of natural persons is low, the controller is not obliged to report the violation to the President of the Personal Data Protection Office. The indicated infringement must only be entered into the internal register of infringements. In the event of a risk of violation of the rights and freedoms of natural persons, the administrator is obliged to report the breach of data protection to the President of the Personal Data Protection Office, as well as to enter an entry in the internal register of violations. The occurrence of a high risk of violation of the rights and freedoms of natural persons, in addition to an entry in the register of violations, requires the controller to take appropriate action, both against the supervisory authority (notification of a data breach), and in some cases also against data subjects. In the event of violations that may result in a high risk of violating the rights or freedoms of the data subject, the GDPR introduces an additional obligation to immediately notify the data subject by the controller, unless the

controller has taken preventive measures before the violation or remedial measures after the violation has occurred (Article 34 paragraph 3 of the GDPR) "(publication available at https://uodo.gov.pl/pl/134/1029).

The supervisor did not agree with the Bank's position presented in the letter of [...] May 2021, according to which the Bank stated that in practice it is not possible to use the data from the shipment remaining in warehouse X intact. The mere fact that the parcel was not found despite the lapse of more than 2 years since it was lost by the postal operator and the fact that X in fact already on [...] May 2019 informed that it had not been able to locate the parcel and had finished searching for it, is a sufficient argument for recognition that there has been a breach of personal data protection and that there has been a risk of unauthorized access to personal data. Therefore, the reasons why the Bank is convinced that the shipment is in the sorting plant X and "waiting to be found" are not fully understood.

The above assessment is also not affected by the fact that the proceeding concerns the disclosure of data that, in the Bank's opinion, in practice, most likely, have never been disclosed to unauthorized persons and are waiting to be found in the sorting plant X. The submitted explanations show that on [...] May 2019 . the courier company X informed that it had not been able to locate the parcel and had finished searching for it, therefore there were no grounds to conclude that the parcel was definitely in arrears in the warehouse of X intact and that it was not possible to use the data contained therein, not found there. Due to the fact that the Administrator has no knowledge of where the shipment is currently located and what happened to the personal data of data subjects it contains, it should be assumed that there has been a security breach resulting in the risk of unauthorized disclosure of personal data, and the scope of these data determines that there is a high risk of violating the rights or freedoms of natural persons.

To better illustrate cases of personal data breaches, where there is no obligation to report to the supervisory authority due to the fact that it can be considered that the breach is unlikely to result in a risk of violating the rights or freedoms of natural persons, reference can be made to the WP250 Guidelines. As an example of a breach that does not require reporting to the supervisory authority, these guidelines mention the loss of "a securely encrypted mobile device used by the administrator and his employees. 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 allows breaking cryptographic security, is incomparable to a situation in which documents with personal data of the Bank's customers have been lost and despite the passage of time, they were not found. 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 by the Article 29 Working Party in the WP250 Guidelines, which also confirms that the risk has not been reduced to a level where state that the breach is unlikely to result in a risk of violation of the rights or freedoms of an individual.

In its explanations, the Bank referred to, for example, No. 15 presented in the Guidelines of the European Data Protection Board 01/2021 on examples of data breach notifications, version 1.0 (hereinafter also referred to as "EDPB Guideline 01/2021"), in which the breach was based on sending by e-mail to 15 unauthorized recipients a list of 15 hotel guests containing their personal data in the field of names, e-mail addresses and food preferences (in the case of two guests). As indicated by the EDPB, in these specific circumstances the risks arising from the nature, sensitivity, volume and context of the data disclosed are low and it can be concluded that the breach did not have a significant impact on the data subjects. The EDPB also considered that in this context, the fact that the controller immediately contacted recipients after becoming aware of the error could be considered a mitigating factor. The Bank referred to this example because, in its opinion, the facts presented therein are analogous to that considered in the present case. However, this position cannot be accepted because - as has been shown above - in the event of a breach covered by this proceeding, the disclosed scope of data causes - contrary to the one presented in the EDPB Guidelines 01/2021 - a high risk of violating the rights or freedoms of natural persons.

The following examples provided in the EDPB Guidelines 01/2021, according to which notification may be waived, should be considered equally inaccurate: example No. 9 and example No. 13.

In example 13, where the retailer incorrectly sends both orders and bills containing personal data to the wrong customers due to the lack of special categories of personal data or other data, the misuse of which may lead to significant negative consequences, there was no high risk violation of the rights or freedoms of natural persons, however, in this case, the scope of

the data provided includes only: name and surname, address and information on the purchased item and its price.

The Bank's argumentation in the context of the lack of legitimacy of reporting a breach of personal data protection to the President of the Personal Data Protection Office, which, in the Bank's opinion, is supported by the fact that the data was sent to an erroneous, yet trusted recipient, such as X for the Bank, referring to example No. 9 in the Guidelines, is completely incomprehensible. EDPB 01/2021. In the discussed example, relating to the accidental transfer of data to a trusted third party, no analogy can be found in this case, in which we are not dealing with the transfer of data to a trusted recipient, because X was not the recipient of the lost correspondence, but the postal operator, via whose Bank sent the parcel with documents containing personal data. Moreover, also in this case, the scope of data, which is limited only to: contact details and data related to the insurance itself (type of insurance, amount), is diametrically different from that which is the subject of the data breach in question.

Here we should mention the example No. 16 presented in the EDPB Guideline 01/2021, which is closer to the violation in question. As it follows from the EDPB Guidelines 01/2021 for this example, the insurance group, as part of offering car insurance, sent correspondence to the wrong recipient 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. Also example no. 12 refers to a breach (theft of a paper diary from a drug rehabilitation center, which contained, among others, health data of patients admitted to the facility), which due to, inter alia, the scope of disclosed categories of personal data causes a high risk of violating the rights or freedoms of natural persons.

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 clearly identifies a natural person, and in connection with the data regarding the registered address, bank account numbers, as well as the CIF number (identification number assigned to the Bank's clients) may cause significant consequences for the person whose personal data has been disclosed. Referring the above to the breach in question, it should be noted that the Bank's obligation was not only to report the breach of data protection to the President of the Personal Data Protection Office, but also to notify the data subjects of the breach.

The above assessment is also not affected by the fact that "the Bank is currently considering changes to the agreement with X,

pursuant to which X will, at the Bank's request, continue to search for the Bank's parcels considered lost" and that due to the constantly improved process of handling correspondence in the Bank itself " recently, the Bank prepared additional trainings on safe and correct sending of parcels for branch employees ". The data was lost, which directly exposed them to the possibility of disclosure to unauthorized persons, and which in turn means (which should be emphasized again) that there has been a security breach resulting in the risk of losing the confidentiality of personal data, and the scope of this data, including the PESEL registration number, determines that there was a high risk of violating the rights or freedoms of natural persons. Analyzing the possibility of changing the contract with X, or conducting additional trainings by the Administrator should be considered a measure taken by the Administrator to minimize the risk of this type of breach in the future, and not an action to minimize the risk of violating the rights or freedoms of the data subjects.

In the explanations contained in the letter of [...] May 2021, the Bank indicated that "PESEL numbers are publicly available for members of legal entities' bodies (eg members of the Bank's management board). Therefore, the bank has no information about fraudulent loans for their data, use of data in connection with granting a fine, extorting insurance funds to their detriment, concluding civil law contracts, registering pre-paid cards or obtaining access to medical documentation. It is not possible to confirm the use of data in the case of participatory budgets, although it should be emphasized that the impact of such use would have to be minimal ". In light of the above-mentioned According to the argument of the Bank, it should be pointed out that in the present case we are not dealing with the situation described above, because the data of the Complainants are not publicly available in the Court and Economic Monitor or the National Court Register. The Article 29 Working Party in WP250 Guidelines for situations where reporting of breaches is not necessary indicates, for example, a situation where personal data is already publicly available and the disclosure of such data does not pose a probable risk to the individual. 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 occurring for the data subjects.

The bank also refers to Art. 87 of Regulation 2016/679, according to which Member States may define specific conditions for the processing of a national identification number or other identifier of general scope, indicating at the same time that the Polish legislator has not decided to adopt specific rules for the processing of a PESEL number for private entities. In the opinion of the Bank, quotation: "certain special solutions were adopted in the Act of 24 September 2010 on population records, in chapter 6" Providing data from the PESEL register and residents' registers "for entities requesting the disclosure of data

from the register itself. This does not apply to situations where the PESEL number is disclosed by the data subject, e.g. for the purpose of concluding a contract. The fact that the legislator does not see the need for further detailing of the rules of data processing from registers suggests that its processing itself does not pose a threat to citizens ”.

Publishing the PESEL number, which is the national identification number in Poland, is an extremely important issue for the President of the Personal Data Protection Office. At this point, the President of the Personal Data Protection Office would like to emphasize that, for example, already in 2019, he asked the Minister of Justice to amend the Act of August 20, 1997 on the National Court Register (Journal of Laws of 2018, item 986, as amended). Article 35 (1) of this Act stipulates that whenever a natural person is entered in the National Court Register, the surname and first names as well as the identifier assigned in the population registration system (PESEL number) are entered there. At the same time, Art. 8 of the above Act assumes the openness of the National Court Register and its unconditional general availability. In his speech, the President of UODO pointed to the necessity to verify the concept of absolute transparency of the PESEL number, currently operating on the basis of the National Court Register. Understanding the reasons for which the PESEL number functions as an open data (security of business transactions), he indicated that these solutions were introduced many years ago, and the need to comply with the provisions of Regulation 2016/679 in the Polish legal system favors the re-verification of this concept. Each disclosure of the PESEL number to the public also affects the private sphere. In the case of the National Court Register, this also applies to persons who no longer perform functions in entities listed there, such as former attorneys or former proxies. The PESEL number of a person disclosed in the National Court Register makes it publicly available information.

Pursuant to the regulations currently in force, disclosing the PESEL number in the National Court Register, as well as in a qualified electronic signature, is permitted by law, however, in the opinion of the President of the Personal Data Protection Office, these provisions, ensuring the legality of such data processing, should be modified, as they raise doubts in terms of compliance with Art. . 87 of the Regulation 2016/679. Pursuant to the said provision, the state may define specific conditions for the processing of the national identification number, but only with appropriate safeguards for the rights and freedoms of the data subject, as provided for by this regulation. Taking into account the above regulations, the President of the Personal Data Protection Office (UODO) [...] in June 2019 sent an application to the Minister of Digitization for statutory changes regarding a qualified electronic signature. He pointed out that while it is justified to use a PESEL number in the case of verification of a person applying for a qualified electronic signature certificate, disclosure of the PESEL number to other persons raises doubts

as a consequence of using an electronic signature. The President of the Personal Data Protection Office pointed out that the processing of a PESEL number without maintaining appropriate security rules poses a number of threats to the privacy of a natural person. Disclosed in many places, it facilitates identity theft as well as profiling a person without their knowledge and consent. In response to the above-mentioned request, the supervisory authority received information on [...] July 2019 that the Ministry of Digital Affairs declares that it will review the regulations on identifiers used in electronic signatures.

Taking into account the above examples of the activities of the President of the Personal Data Protection Office who take possible and appropriate steps to protect the national identification number - PESEL, there is no doubt that the PESEL number, i.e. an eleven-digit numeric symbol, uniquely identifying a natural person, containing the date of birth, sequence number, the gender designation and the control number, i.e. closely related to the private sphere of a natural person and also subject to, as a national identification number, exceptional protection under Art. 87 of Regulation 2016/679 is a data of a special nature and requires such special protection. Special protection of personal data, including in particular the PESEL number, is also required from institutions of public trust, which undoubtedly include the party to the proceedings in question.

Still referring to the submitted explanations, the Controller argues that the breach has not been reported to the supervisory authority by the lack of precise guidelines as to the type of breaches to be reported. In addition, the examples of breaches subject to reporting included in the WP250 Guidelines, in the opinion of the Administrator, concerned events so serious that he had the impression that the notification obligation provided for in Art. 33 of Regulation 2016/679 is reserved for special cases (the Administrator cites examples of reported violations, which refer to a large scale of the event, or a violation relating to a specific category of personal data - medical data).

At this point, first of all, it should be emphasized that, neither under the 2016/679 regulation nor any other legal act, there is an exhaustive list of events classified as a breach of personal data protection. Article 4 (12) of Regulation 2016/679 provides that a breach of personal data protection is understood as: a breach of security, leading to accidental or unlawful destruction, loss, modification, unauthorized disclosure or unauthorized access to personal data transmitted, stored or otherwise way processed. Included in the above-mentioned provision, the enumeration of processing operations is purely exemplary, as each processing operation may involve a breach of data security.

If the controller detects a breach of personal data protection, it is first necessary to analyze the risk of violating the rights or freedoms of natural persons. The controller is released from the obligation to notify the supervisory body about a breach if, as

a result of the conducted examination, it turns out that there is no probability of a risk of violation of the rights or freedoms of natural persons. However, it should be borne in mind that the supervisory authority will be able to ask the administrator to justify the decision not to report the breach, therefore the conclusions of the analysis should be recorded in the internal record of breaches. At the same time, it should be emphasized that the WP250 Guidelines referred to by the Administrator include the recommendations of the Article 29 Working Party regarding the requirement to report breaches to the supervisory authority.
On the other hand, the lack of relevant guidelines in the above-mentioned scope should mean that the controller, guided by the necessity to fulfill his obligations referred to in Regulation 2016/679 and the good of persons at risk of violating their rights or freedoms, will report to the authority supervisory authority, any event which raises doubts that may have any consequences for the data subject, and notifies these persons about breaches involving high risk. The above applies in particular to the Bank which, being an entity of public trust, should create higher standards in this respect.
First of all, however, in the period in which the infringement took place, similar cases were reported to the supervisory body, and violations from the banking / insurance sector, as shown in the Report on the activities of the President of the Personal Data Protection Office in 2019, were among the most frequent supervisory authority.
It should be pointed out, what is actually 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 loss of documentation containing personal data, mainly in paper form, by postal operators or entities providing courier services ("There was also an upward trend in reports of personal data breaches consisting in the loss of paper documentation by postal operators and courier service providers. In cases of personal data breaches caused by the loss or incorrect delivery of postal items, the President of UODO indicated that it is the sender who should inform the supervisory authority about such breaches as the administrator of personal data processed in connection with the performance of its tasks "), as is the case this case. At that time, as also shown in the Report, as part of remedial actions, the administrators reviewed the contracts concluded with these entities and determined the causes of the events that occurred.
It should be emphasized again that the assessment of the risk of violating the rights or freedoms of a natural person should be made through the prism of the person at risk, 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 controller still guarantees proper processing of his personal data in a manner ensuring their security. On the basis of such an assessment, it may decide, for example, to resign from the services of the administrator or in the event of the occurrence of the premises referred to in art. 17 of Regulation 2016/679, use 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.

In addition, referring to the consequences that may be associated with the disclosure of the PESEL number, including in particular identity theft, which the Administrator refers to many times in his explanations, writing that: "in the opinion of the Bank, the disclosure of data in the form of a PESEL number is not always causes a high risk for the rights and freedoms of the injured person, including the risk of identity theft ", or" neither banks nor lenders, as entities obliged under the AML regulations to verify an identity document, cannot provide financing based on the PSESEL number or PESEL number alone in conjunction with other information […] ", the President of the Personal Data Protection Office would like to emphasize that the phenomenon of identity theft continues to intensify, as evidenced by signals from victims and administrators who report violations in this respect, constantly being sent to the Office.

In the opinion of the President of the Personal Data Protection Office, the Controller, taking into account the nature of the breach and the categories of data that have been breached, should indicate to the data subjects the most likely negative consequences of breaching their personal data.

Certainly, in the event of a breach of data such as name, surname and PESEL number, it is necessary to indicate, first of all, the possible theft or falsification of identity by obtaining by third parties, to the detriment of persons whose data was violated, loans from non-bank institutions or extortion of insurance or funds from insurance, which may have negative consequences

related to an attempt to attribute responsibility to data subjects for the commission of such fraud. The description of possible consequences should reflect the risk of violating the rights or freedoms of this person, so as to enable him to take the necessary preventive measures. Importantly, Bank Millennium S.A. in the case of notifications to data subjects attached to the reported breaches of personal data protection (in the scope of disclosure of the PESEL number), each time indicates the consequence of "identity theft or falsification", therefore, in the opinion of the President of the Personal Data Protection Office, the complete marginalization of this risk is incomprehensible in the explanations submitted by the Bank in the course of these proceedings and indicating that "such situations as a result of obtaining a PESEL number are rare, if at all possible at all".

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 specified in Art. 34 sec. 3 lit. a) and b) of Regulation 2016/679. The President of the Personal Data Protection Office 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 WP250 Working Party in WP250 states: “When reporting a breach to a supervisory authority, controllers may consult the supervisory authority on whether relevant information should be provided to affected individuals in a given case. The supervisory authority may require the controller to inform relevant individuals about a breach. Notifying individuals about a breach enables the controller to provide these persons with information on the risks associated with the breach and to indicate actions that these individuals 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 a situation where, as a result of a breach of personal data protection, there is a high 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, and in cases of high risk of breach rights or freedoms, including data subjects. The administrator 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 personal data breach, 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 data subjects, the Bank should have provided

data subjects with the best possible protection of personal data without undue delay. To achieve this goal, it is necessary to indicate at least the information listed in Art. 34 sec. 2 of the Regulation 2016/679, from which the Bank did not fulfill this obligation. Therefore, when deciding not to notify the supervisory authority and the data subjects of the breach, in practice they deprived these persons of reliable information about the breach and the possibility of counteracting potential damage, provided without undue delay.

It should be emphasized here that the information about lost documents sent to the Complainants by the Bank does not contain the elements referred to in Art. 34 sec. 2 of Regulation 2016/679, which means that it cannot be considered a notification of a personal data breach. Correct notification should, in clear and simple language, describe the nature of the personal data breach and contain at least the information and measures referred to in Art. 33 sec. 3 lit. b), c) and d) of Regulation 2016/679. Meanwhile, the information sent to the Complainants contained only a very general description of the nature of the infringement (without indicating the categories of data covered by the infringement) and measures to minimize its possible negative effects, including allowing the Complainants to benefit from the free Alert service […]. In the above-mentioned However, the letter did not contain a description of the possible consequences that may be associated with the breach of personal data protection in question, as well as information on the name and surname and contact details of the data protection officer or the designation of another contact point from which more information can be obtained. There is also no reference to the security measures applied by the Administrator in order to minimize the risk of a recurrence of the breach.

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 Bank did not notify the personal data breach to the supervisory body in compliance with the obligation under Art. 33 sec. 1 of the Regulation 2016/679 and did not notify the data subjects of a breach of their data protection without undue delay, in accordance with art. 34 sec. 1 of the Regulation 2016/679, which means the Bank's breach of these provisions.

Pursuant to Art. 34 sec. 4 of Regulation 2016/679, if the controller has not yet notified the data subjects of 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 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 shows that each supervisory authority has the right to remedy the need for the controller to notify data subjects of a data breach.

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 circumstances justifying the imposition of an administrative fine on the Bank 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 Bank, 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, which necessitate the application of this type of sanction in the present case and which had an aggravating effect on the size of the imposed administrative fine:

1. The nature and gravity of the violation (Article 83 (2) (a) of Regulation 2016/679). The violation found in this case consisting in the loss of documentation containing personal data of the Bank's customers in the form of: PESEL number with name and surname, registered address, bank account number, CIF number (identification number assigned to the Bank's clients), is of considerable importance and serious nature, as it may lead to property or non-property damage to persons whose data has been breached, and the probability of their occurrence is high.

2. 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. More than 2 years have elapsed from the Bank becoming aware of a

breach of personal data protection to the date of this decision, during which the risk of violating the rights or freedoms of persons affected by the breach could be realized, and which these persons could not counteract due to the Bank's failure to comply with the obligation to report a breach of personal data protection to the President of the Personal Data Protection Office and the obligation to properly notify data subjects about the breach. It is true that the Administrator suggested that the injured parties use the Alert service, as part of measures to remedy the breach of personal data protection, [...], however, in the letter sent, he did not indicate such important information as the possible consequences of the breach of personal data protection, or the name and surname and the contact details of the data protection officer from whom these persons could obtain more information. The information on lost documents also does not indicate the category of personal data covered by the breach, which should contain a description of the nature of the breach. In the letter sent, the administrator did not mention the security measures applied by him in order to minimize the risk of recurrence of the breach.

Intentional nature of the infringement (Article 83 (2) (b) of Regulation 2016/679) In line with the Article 29 Working Party's Guidelines on the application and setting of administrative fines for the purposes of Regulation 2016/679 WP253 (adopted on 3 October 2017), hereinafter referred to as the "WP253 Guidelines", intent "includes both knowledge and deliberate action in relation to the characteristics of the offense". The bank made a conscious decision not to notify the President of the Personal Data Protection Office and the data subjects about the breach. Therefore, there is no doubt that the Bank, when processing personal data on a massive scale, has a high level of knowledge in the field of personal data protection, including knowledge of the consequences of finding a personal data breach resulting in a ("average", in the opinion of the Bank itself) risk of violating the rights and freedoms of persons physical. Having such knowledge, after carrying out a risk analysis, the Bank expressed the will (made a conscious and free decision) to resign from reporting the infringement to the President of the Personal Data Protection Office and informing the data subjects. This will was revealed and was consistently sustained by the Bank in the proceedings before the President of the Personal Data Protection Office, during which the President of the Personal Data Protection Office first informed the Bank about the obligations incumbent on the controller in connection with the breach of data protection and about the possibility of a high risk violation of rights and freedoms. the persons concerned by the violation. Finally, the mere initiation of this procedure by the President of the Personal Data Protection Office on the obligation to notify the breach of personal data protection to the supervisory authority and to notify the data subjects of the breach, should at least raise doubts for the Bank as to its own assessment of the effects of the breach. And as indicated in the WP250

Guidelines, which the Bank itself referred to in its explanations, and as already mentioned above, "in case of any doubts, the administrator should report the breach, even if such caution could turn out to be excessive".

4. 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 that the Bank's cooperation with him was unsatisfactory. This assessment concerns the Bank's response to the letters 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, and finally to the initiation of administrative proceedings regarding the obligation to report a breach of personal data protection and notification of the breach of data subjects. 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 persons affected by the infringement) were not taken by the Bank even after the President of the Personal Data Protection Office initiated the administrative procedure in the case.

5. The categories of personal data concerned by the infringement (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, registered address, PESEL number, bank account numbers and identification number assigned to the Bank's customers - CIF number), is associated with a high risk of violating the rights or freedoms of natural persons.

6. The way in which the supervisory authority learned about the breach (Article 83 (2) (h) of Regulation 2016/679). About the breach of personal data protection being the subject of this case, i.e. the loss of documentation containing personal data by the courier company X processed by the Bank acting as the administrator of these data, the President of the Personal Data Protection Office has not been informed in accordance with the procedure provided for in such situations, specified in Art. 33 of the Regulation 2016/679. The fact that there is no information about a breach of data protection provided by the controller obliged to provide such information to the President of the Personal Data Protection Office should be considered as incriminating that 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 .:

1. Number of data subjects affected (Art. 83 (2) (a) of Regulation 2016/679). In the present case it was established that the

personal data of only two persons was breached. Such a number of people affected by the infringement, especially in view of the fact that the Bank - due to the scale and scope of its activities - processes personal data of a very large number of clients, should be considered small, which undoubtedly constitutes a mitigating circumstance in the present case.

2. Actions taken by the controller or processor to minimize the damage suffered by data subjects (Article 83 (2) (c) of Regulation 2016/679). The controller provided data subjects with certain information about the breach, including including its nature (but without such relevant information as the scope of personal data covered by the breach) and indicated measures to minimize its possible negative effects, enabling data subjects to benefit from the free Alert service […]. Such action of the Administrator deserves to be noticed and accepted, however, it is in no case tantamount to the fulfillment of the obligation referred to in art. 34 sec. 1 of Regulation 2016/679.

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:

1.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; 2. 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 Bank were found in this respect; 3. 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 did not apply the measures referred to in the provision indicated above; 4. 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; 5. financial gains or losses avoided directly or indirectly from the breach (Art.83 (2) (k)) - the controller was not found to have gained any gains from the breach or avoided financial losses.

In the opinion of the President of the Personal Data Protection Office, the administrative fine applied 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 Bank, which processes personal data professionally and on a mass scale, in the future will fulfill its obligations in the field of personal data protection, in particular with regard to reporting a personal data breach. 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 Bank'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 the Bank 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 painful 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 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 as of 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, which 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, the Bank imposed on the Bank - using the average EUR exchange rate of January 28, 2021 (EUR 1 = PLN 4.5479) - an administrative fine in the amount of PLN 363,832 (equivalent to EUR 80,000).

In the opinion of the President of the Personal Data Protection Office, the applied fine in the amount of PLN 363,832 (in words: three hundred sixty three thousand eight hundred and thirty two zlotys) meets, in the established circumstances of this case, the conditions referred to in Art. 83 sec. 1 of Regulation 2016/679 due to the seriousness of the infringement found in the context of the basic objective of Regulation 2016/679 - 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 Bank, the President of the Office for Personal Data Protection decided that it is proportional to the financial situation of the Bank and

will not constitute an excessive burden for it. It should be noted here that the Bank is the parent entity of the Bank Millennium Capital Group, constituting an "enterprise" within the meaning of recital 150 of Regulation 2016/679. As stated in WP253: "In order to impose effective, proportionate and dissuasive fines, the supervisory authority uses the definition of an undertaking adopted by the CJEU for the purposes of applying Art. 101 and 102 TFEU, namely that the concept of an enterprise is to be understood as an economic unit that may be formed by the parent company and all subsidiaries involved. " The "Consolidated Annual Report of the Bank Millennium Group for 2020" posted on the Bank's website [...] shows that the revenues from the core activities of the Bank Millennium Group in 2020 amounted to approx. in this case, an administrative fine represents approximately 0.011% of the total annual worldwide turnover of the company in the previous financial year. At the same time, it is worth emphasizing that the amount of the imposed fine (PLN 363,832.00) is only 0.55% of the maximum amount of the fine that the President of the Personal Data Protection Office could - in accordance with Art. 83 sec. 4 of the Regulation 2016/679, the 2% threshold calculated on the total annual turnover - impose on the Bank for the infringements found in this case

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 breach 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 Bank's turnover. According to the President of the Personal Data Protection Office, the Bank should and is able to bear the consequences of its negligence in the field of data protection, as evidenced by, for example, the Bank's financial statements sent to the President of the Personal Data Protection Office on [...] May 2021.

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

2021-11-08