THE CHAIRMAN OF PERSONAL DATA PROTECTION

Warsaw, 19

January

2022

DECISION

DKN.5131.33.2021

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. 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", following administrative proceedings initiated ex officio in the case of failure to notify about the breach of personal data protection of the persons affected by the breach, by Santander Bank Polska S.A. with headquarters in Warsaw at al. Jana Pawła II 17, President of the Office for Personal Data Protection,

1) finding a breach by Santander Bank Polska S.A. based in Warsaw, the provisions of art. 34 sec. 1 of Regulation 2016/679, consisting in the failure to notify about a breach of personal data protection, without undue delay of data subjects, is imposed on Santander Bank Polska S.A. with its registered office in Warsaw, an administrative fine in the amount of PLN 545,748 (say: five hundred and forty-five thousand seven hundred and forty-eight zlotys),

2) orders Santander Bank Polska S.A. with its registered office in Warsaw, notification - within 3 days from the date of delivery of this decision - to data subjects of a breach of the protection of their personal data, i.e. all employees of the Bank who were employed during the period in which the former employee of the Bank had unauthorized access to data collected on the ZUS Electronic Services Platform (PUE ZUS) in order to provide them with the information required in accordance with 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

On [...] February 2021, the President of the Personal Data Protection Office, hereinafter also referred to as the "President of the Personal Data Protection Office", received a notification of a data breach made by Santander Bank Polska S.A. with headquarters in Warsaw at al. Jana Pawła II 17 (hereinafter referred to as the "Bank", "Administrator"), registered under the reference number [...], informing about a breach of personal data protection of 10 500 people. The breach consisted in the fact that a former employee of the Bank, who had not been deprived of access to the ZUS Electronic Services Platform (PUE ZUS) after the end of his employment, had unauthorized access to this platform, as a result of which he could view the payer's profile of Santander Bank Polska S.A. data of the Bank's employees in the scope of their names and surnames, PESEL number, address of residence or stay and information on sick leave constituting data concerning health.

The President of UODO, in a letter of [...] February 2021, addressed Santander Bank Polska S.A. for information whether, after the termination of the employment relationship, the former employee of the Bank exercised his rights and logged into the PUE ZUS platform (in connection with an application to ZUS for access to all logs that were made at PUE ZUS by an unauthorized person). As a result of the above, it was found that this person logged in to the PUE ZUS platform five times during the said time (on the following dates: 2020-06- [...], at 21:09:54; 2020-06- [...], at 21 : 00: 42; 2020-06- [...], at 21:02:37; 2020-10- [...], at 22:01:27; 2021-02- [...], at 20:50 : 14), thus gaining unauthorized access to the personal data of the Bank's employees. At the same time, no areas were indicated that were viewed by an unauthorized person, or to what specific data and how many employees this person obtained access during logging in to the payer profile of Santander Bank Polska S.A. on the PUE ZUS platform. At the same time, the Administrator informed that he resigned from notifying the data subjects about the breach, arguing this with the fact that: "during employment, the employee had access to a much wider catalog of employee data which was related to the performance of [...] databases of all SBP employees needed to implement HR and payroll processes) ”.

Due to the lack of notification of data subjects about the breach of their personal data, in the application of [...] March 2021, the President of the Personal Data Protection Office indicated that the analysis of the breach in question taking into account the nature of the breach, its duration, data categories, number of persons, affected by the breach, as well as the applied remedies,

led to the conclusion that there had been a breach of confidentiality. Due to the fact that this breach of confidentiality concerns PESEL numbers along with names and surnames, addresses of residence or stay and information on sick leave, i.e. health data, it should be considered that it involves a high risk of violating the rights or freedoms of natural persons. For this reason, it is necessary to notify data subjects of a breach of the protection of their personal data, in accordance with the obligation expressed in art. 34 in connection with Art. 12 of Regulation 2016/679. At the same time, the President of the Personal Data Protection Office (UODO) requested specific areas of the PUE ZUS platform, which were reviewed by the former employee; indication of how many people - employees of the Bank, during the specified 5 logins, an unauthorized person - a former employee, had access to it.

In response of [...] March 2021, the Bank indicated that, based on the information provided to it by the Social Insurance Institution, which is the operator of the PUE ZUS platform, no illegal data processing was identified. The bank additionally indicated that if there was a hypothetical breach of personal data protection, then only to the extent to which the former employee had access to the data during the employment period. Therefore, in the Bank's opinion, there was no breach of personal data protection within the meaning of Art. 4 point 12 of Regulation 2016/679. Notwithstanding the foregoing, the Bank proposed to place on the Intranet of Santander Bank Polska, i.e. on the Bank's internal communication platform, a message resembling the rules for the processing of personal data, what may be a personal data breach related to the access of an unauthorized person to employees' personal data, information about possible consequences of breach of personal data protection of employees, description of measures that the Bank, as the administrator, uses to remedy breaches of personal data protection and information about the name and surname and the possibility of contacting the Data Protection Officer.

In a letter sent on [...] March 2021, the Bank confirmed the implementation of the declared actions, i.e. publishing on the Intranet the above-mentioned information, while attaching the content of this communication. However, it cannot be read from its content that, in fact, there was a breach of data protection of the Bank's employees, of a nature that was only exemplary and possible to occur, and was presented in an internal communication.

There is no doubt that the nature of this communication is general enough, primarily not relating to a specific case, but only in a figurative way presenting a certain type of infringement that could occur, without indicating that such a situation de facto took place, that the potential recipient by not identifying with the situation described in this communication - which is very likely - he will not draw any conclusions from it.

Therefore, in the Bank's opinion, there was no breach of personal data protection within the meaning of Art. 4 point 12 of Regulation 2016/679. After analyzing the above-mentioned arguments indicated by the Bank, it was necessary to submit additional explanations, to which the President of the Personal Data Protection Office called the Administrator in a letter of [...] June 2021. The content of the questions asked by the President of the Personal Data Protection Office together with the Bank's explanations below:

In response to the question of how the scope of authorizations to access IT systems is monitored, in particular those employees who have terminated their employment relationship with the administrator, the Administrator referred to the policy in force at the Bank [...]. According to this document, departure of the employee […].

In point 9C of the violation notification, the Administrator indicated the need to periodically review the accesses to the PUE ZUS platform in order to eliminate similar situations in the future, therefore the President of the Personal Data Protection Office asked for clarification on how this issue was regulated before the violation in question, or indicated in the above-mentioned . the point of action is all that was undertaken by the Administrator in this regard. The bank indicated that its employees have access to the PUE ZUS platform based on an authorization for a given employee, issued on the basis of the ZUS template. The bank sends a letter to ZUS revoking the authorization in the event of termination of an employment contract with an authorized employee. Additionally, as indicated by the Bank, the Human Resources Department maintains a list of authorized persons and a list of formally registered persons - periodically obtained from ZUS once a quarter, in order to verify the correctness of the list carried out within the Department. In addition, verification of the legitimacy of the authorizations in question is carried out after obtaining a list of authorized persons from ZUS. In the explanations provided, the Bank also added that "Before the submission of the report in question, the list of reported persons kept within the Department of Human Resources was based, without making the above-mentioned report. control activities ".

The President of the Personal Data Protection Office in the further part of the request for explanations asked whether the breach was reported by the employee affected by the incident, or by any of the other employees mentioned in the correspondence with the Social Insurance Institution, and if the above-mentioned the report was specifically made by the employee affected by the incident, whether the Administrator took steps to establish with this person the details of logging into the system, to which data categories and to the data of how many people - the Bank's employees, the person obtained unauthorized access. In response, the Bank confirmed that it received information about the breach from the person who was

the subject of the incident in question (A.), but did not attempt to contact an unauthorized person due to the fact that he is no longer an employee of the Bank and such contact could be negatively perceived by former employee.

The last question related to the content of the letter of [...] March 2021, in which the Administrator indicated that "in the opinion of the bank, there was no breach of personal data protection", while the previous explanations clearly showed unauthorized logging in to the PUE ZUS platform of a former Bank employee. The President of the Personal Data Protection Office asked for an explanation of the reasons for such a request for no violation, which was the basis of the Administrator in determining it, and asked to send an appropriate risk analysis for this violation, including an indication of what circumstances were taken into account by the Administrator during the assessment. The Bank indicated that the notification of a breach of personal data protection was made only for prudence, taking into account the lack of a complete assessment of the incident, in particular the lack of full determination of the areas (what they related to and how many employees) to which the former employee of the Bank had unauthorized access. However, due to the fact that the data available in the system includes, among others, PESEL number and name and surname, high risk - 3 on a 3-point scale, based on the guidelines of the President of the Personal Data Protection Office. However, after receiving [...] February 2021 a reply from the Social Insurance Institution, in which it refused to disclose the scope of data to which the former employee actually had access, the Bank reduced the risk scale to 1, stating that "due to the inability to verify this scope by the bank as an administrator from an external source such as ZUS - it cannot be considered that there was certainly unauthorized access to data in relation to a former bank employee ". The Bank referred to the position of the Data Protection Officer of ZUS expressed towards the Bank in an e-mail of [...] February 2021, i.e. "in the opinion of the Data Protection Officer from ZUS, for security reasons, there are no grounds to provide the bank with logs and a description of their interpretation, because recognition of their structure by unauthorized persons may potentially lead to the disclosure of legally protected ZUS information, it seems that the most effective would be for the President of the Personal Data Protection Office to ask ZUS to obtain the necessary information about the event, so as to clearly determine whether there has been a violation and its risks for data subjects ".

Due to the continued lack of notification of the breach of personal data protection of the affected persons, on [...] July 2021, the President of the Personal Data Protection Office initiated administrative proceedings against the Bank in this regard. In addition, in this letter, the President of the Personal Data Protection Office called on the Administrator to explain on what basis the Bank based its claim that the breach of personal data protection consisting in the possession by the Bank's employee, after

termination of the employment relationship, unauthorized access to employee data processed on the ZUS Electronic Services Platform ( PUE ZUS) in the scope of: names and surnames, addresses of residence or stay, PESEL number, as well as information on sick leave, i.e. health data, causes a low risk of violating the rights or freedoms of natural persons, resulting in the lack of the need to notify persons affected by the violation , together with a request to submit the risk analysis performed for this infringement.

In response to the above, in a letter of [...] July 2021, the Administrator explained that it considered a low risk of violation of the protection of the rights and freedoms of natural persons based on the following arguments:

In the opinion of the Bank, there are no unequivocally confirmed circumstances as to the scope of personal data available for inspection by an unauthorized person. The Bank indicated the statement of the former employee (A.), in which he indicates that he had "(...) unauthorized access to the personal data of the Bank's employees from the PUE ZUS platform (e.g. name, surname, addresses, PESELS, information from e-ZLA certificates) ".

The bank has performed internal verification of access to the PUE ZUS platform, as a result of which it was established that an employee authorized to process personal data of employees, who has the same access to the PUE ZUS platform as the former employee affected by the infringement, may have access to employees' personal data to the extent indicated by of the former employee in an e-mail sent to the Bank on [...] February 2021, in which he reported his unauthorized access to personal data. However, the bank points out that it is not possible to clearly define the number of employees whose data was presented on the service screen at a given time, the former employee had access to.

After receiving a notification about unauthorized access to the PUE ZUS platform, the Bank immediately asked the Social Insurance Institution about the number of logins by an unauthorized employee to the PUE ZUS platform and a request to indicate the areas that had been viewed by him. ZUS provided information about 5 logins of a former employee, at the same time pointing out that, in the opinion of the Data Protection Officer of ZUS, for security reasons there are no grounds to provide the Bank with logs and a description of their interpretation, because knowing their structure by unauthorized persons may potentially lead to the disclosure of legally protected ZUS information .

In view of the above, the Bank applied for a liability, pursuant to Art. 78 in connection with joke. 77 § 1 of the Act of 14 June 1960 Code of Administrative Procedure (hereinafter referred to as "the Code of Administrative Procedure"), the Social Insurance Institution to provide detailed explanations regarding the former employee's access to information on the Bank's

profile at PUE ZUS, including the number of data subjects , categories of personal data of data subjects and any other entries from the ZUS Electronic Services Platform, in order to unambiguously identify what data the former employee had access to. The employee who had unauthorized access to personal data processed on the PUE ZUS platform was a long-term employee, and before the termination of employment, he held the position of [...], therefore he had access to personal data of other employees, processed by the Bank for HR and payroll purposes. This person was authorized to process personal data on behalf of the Bank, and submitted appropriate statements confirming that he was familiar with the personal data processing policy in force at the Bank as well as security and confidentiality standards.

The Bank referred to the Guidelines of the Article 29 Working Party on the reporting of personal data breaches in accordance with Regulation 2016/679 (WP250rev.01), hereinafter referred to as "WP250 Guidelines", i.e. the guidelines adopted on October 3, 2017 by the Art. 29 and then approved by the European Data Protection Board (hereinafter referred to as the "EDPB"), according to which the controller may, in certain situations, consider an unauthorized recipient of data as a "trusted". The bank recognized a former employee who had access to personal data on the PUE ZUS platform. as a "trusted" recipient, ie the Bank trusted the recipient due to the statements made by him during his employment with the Bank that he would not take any further actions regarding these data. The bank indicated that it assessed the risk in the context of the requirement specified in Art. 33 of Regulation 2016/679 and found that there are grounds for reporting a breach of personal data protection to the supervisory authority "because it is not unlikely that the breach would result in a risk of violating the rights or freedoms of natural persons". However, in the context of the obligation under Art. 34 of the Regulation 2016/679, the administrator found that the incident in question does not involve a high risk of violating the rights or freedoms of natural persons, therefore data subjects will not be notified of the violation. According to the Bank, the fact that a former employee of the Bank independently reported to the Administrator unauthorized access to the PUE ZUS platform is a circumstance in favor of the correctness of the risk assessment - "It cannot be considered that a former employee, by reporting an irregularity, could use unlawful access to the data of bank employees. . The opposite would be contrary to the principles of life experience and the principles of logic. "

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.

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.

In a situation where, as a result of a breach of personal data protection, there is a high risk of violating the rights or freedoms of natural persons, the controller is obliged under Art. 34 sec. 1 of Regulation 2016/679, without undue delay, notify the data subject of such a breach (which was not done in this case, thus violating the above-mentioned provision of Regulation 2016/679). The administrator should fulfill this obligation as soon as possible. Recital 86 of Regulation 2016/679 explains: "The controller should inform the data subject without undue delay of the breach of personal data protection if it may result in a high risk of violating the rights or freedoms of that person, so as to enable that person to take the necessary preventive measures. . Such information should include a description of the nature of the personal data breach and recommendations for the individual concerned to minimize the potential adverse effects. Information should be provided to data subjects as soon as reasonably possible, in close cooperation with the supervisory authority, respecting instructions provided by that authority or other relevant authorities such as law enforcement authorities. For example, the need to minimize the imminent risk of harm will require the immediate notification of data subjects, while the implementation of appropriate measures against the same or similar data breaches may justify subsequent notification. '

The notification must comply with the principle of transparency, i.e. it should describe in clear and simple language the nature of the breach of personal data protection (e.g. present the circumstances of the breach together with a description of the categories of data that have been breached) and contain at least the information and measures referred to in Art. 33 sec. 3 lit. b), c) and d) of Regulation 2016/679. Pursuant to recital 39 of Regulation 2016/679, "all information and messages related to

the processing of personal data should be easily accessible and understandable, i.e. formulated in clear and simple language, which is to provide data subjects with real rights, which they will know how to use" .

An important element of the information provided to data subjects is the description of the nature of the breach. The Article 29 Working Party in WP250 underlines that "It is most important that data subjects understand the nature of the breach and know what they have to do to protect themselves." Accordingly, such a description should be sufficiently detailed and clear that the persons to whom the notification is addressed can understand what happened to their personal data, why and what it means for them. Too laconic information does not fulfill this function, and thus prevents people from properly following the administrator's instructions.

In addition to the above. the description of the nature of the breach, in the notification to the data subjects, the controller should also provide, in clear and plain language, at least the following information:

the name and contact details of the data protection officer or other contact point from which more information can be obtained;

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

a description of the measures taken or proposed by the controller to address the breach, including, where appropriate, measures to minimize its possible negative effects.

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.

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 can also provide information that, in their opinion, notification is not necessary due to the fulfillment of the conditions set out in Art. 34 sec. 3 lit. a) and b) of Regulation 2016/679. The President of 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 makes it possible to provide these persons with information on the risk related to the breach and to indicate actions that can be taken by these persons to protect themselves against the potential negative consequences of the breach. from the materialization of negative consequences for such a person, but from 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 former employee of the Bank having unauthorized access to the Electronic Services Platform of the Social Insurance Institution, which resulted in the possibility of viewing the data of the Bank's employees on this platform in the scope of their names and surnames, PESEL numbers, addresses of residence or stay as well as information on sick leaves constituting data concerning health, 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 damage cited in the guidelines, due to the scope of data covered by this personal data breach, including the PESEL number together with the name and surname, address of

residence or stay, or information on sick leave, i.e. health data, 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 data subjects about the violation of personal data protection, 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 this case, the question of trust in an unauthorized recipient - a former employee, raises doubts. The administrator argues the lack of notification of the breach of data subjects, low risk for the rights or freedoms of these persons resulting from the fact that the entity with unauthorized access to the PUE ZUS platform was a long-term employee of the Bank, before the termination of employment, he held the position of [...], in connection with how he had access to personal data of other employees, processed by the Bank for HR and payroll purposes, which, in the Administrator's opinion, leads to the recognition of an unauthorized entity as a trusted recipient.

At this point, the Bank referred to the WP250 Guidelines, according to which, in certain situations, the administrator may consider an unauthorized recipient of data as "trusted" - "A trusted recipient is a recipient whom the administrator can trust enough to reasonably expect that this party will not read by mistake. sent data or does not obtain access to them and that he will fulfill the instruction to send them back. Even if the data has been consulted, the controller can still have confidence in the recipient that he will not take any further action with the data and that he will promptly return the data to the controller and cooperate in its recovery. In such cases, the controller may consider this issue in the risk assessment following a breach - the fact that the recipient is trusted may result in a breach not having a serious effect, but that does not mean that a breach has not taken place. ' The trusted recipient status is held by entities that operate within the structures of a given organization or are, for example, a supplier whose services the administrator constantly uses. There is an actual and often legal bond between the entities, which allows the degree of trust of the parties to be assessed. In the case of such a recipient, the controller may assume that he is aware of the applicable procedures for the protection of personal data and that he will behave in an appropriate manner. In the case in question, in the opinion of the President of the Personal Data Protection Office, there was no trusted recipient, so the Bank should have acted more carefully in the event of disclosure of data to an unauthorized person, i.e. notify the data subjects about the breach of personal data protection, assuming that the breach may cause wider effects. It cannot be considered beyond any doubt that the former employee will behave in an appropriate manner.

It is worth mentioning here the Guidelines of the European Data Protection Board 01/2021 on examples of data breach notifications, version 1.0 (hereinafter also referred to as the "EDPB Guidelines 01/2021"), and more specifically example No. 8, referring to the "Exfiltration of business data by a former employee ". The example discussed here is a situation where, during the notice period, an employee of an enterprise copies commercial data from the enterprise database, to which he has the right to access and must fulfill his obligations. A few months later, after he quits his job, he uses the data obtained in this way (mainly basic contact details) to contact the company's clients in order to attract them to the new company. While the sole purpose of the former employee who maliciously copied the data may be limited to obtaining the contact details of the company's customers for their own commercial purposes, the controller has no power to consider that the risk to data subjects is low as the controller has no guarantee. as to the employee's intention. Thus, while the consequences of a breach may be limited to the exposure of data subjects to unwanted marketing by a former employee, it is possible that there may be another, more serious breach of that data.

A similar facts (ZUS employee during employment, browsed the data of insured persons; he had access to them, but did not have the right to view them) was already considered by the District Court in Elbląg, which in its judgment of March 24, 2021 in the case file ref. . IV Pa 10/21 indicated that “The claimant's behavior, consisting in obtaining illegal access to the personal data of ZUS clients, unrelated to the performed employee duties, was a deliberate and deliberate action and as such fulfilled the conditions of a serious breach of basic employee duties. It should be emphasized that the plaintiff was trained by the employer to perform his duties, repeatedly submitted written statements confirming the knowledge of documents regarding the processing of personal data and information security at ZUS, repeatedly participated in training courses on compliance with the provisions on the protection of personal data, had knowledge about the consequences of a deliberate breach protection of personal data, and yet with her behavior, she violated not only internal regulations such as "Information security policy in the Social Insurance Institution" and "Work Regulations of the Social Insurance Institution", but also art. 4 point 12 of the Regulation of the European Parliament and of the Council (EU) 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 04.05.2016, p. 1; hereinafter referred to as GDPR) ".

Concluding from the above, it should be stated that the fact of logging into the system in the absence of authorizations must prove the lack of trust. In the case covered by the above-mentioned In the judgment, the lack of trust occurred despite the fact

that the parties were bound by an obligation relationship. Even more so, the lack of trust must take place when an unauthorized person logs into the system and, what is more, is not related to the Administrator by any relationship of obligation.

When analyzing the legitimacy of the presented arguments, one should take into account the fact that legal regulations, including confidentiality obligations (authorization to process personal data on behalf of the Bank, statements confirming reading the personal data processing policy in force at the Bank as well as security and confidentiality standards), they do not guarantee the data subject 100% certainty and protection against the materialization of negative effects, because the relationships in which the entities remain are the key factor. This relationship is defined by the Art. 29 Working Party in the abovementioned Guidelines that include the concept of "trusted recipient". What is most important - the person who had unauthorized access to the personal data of the Bank's employees is currently not connected with the Administrator by any employment relationship, nor are they connected by any other relations, e.g. business relations, therefore the circumstances presented above do not have any significance in this case.

Termination of employment is tantamount to breaking the existing legal ties between the parties to the employment relationship and obliges the parties to "settle" their mutual obligations under the concluded contract. Upon termination of the employment relationship, the principle expressed in Art. 100 § 2 of the Labor Code (Journal of Laws of 2020, item 1320, as amended), i.e. the principle of the employee's special loyalty to the employer, expressed, for example, in the obligation to care for the welfare of the workplace, protect his property and keep information confidential, the disclosure of which could harm the employer. Understood in this way, the obligation to maintain loyalty results from the very fact of establishing an employment relationship and binds the parties throughout its duration, until it ceases. While the fact of being a long-term employee of the Bank, working in the Human Resources Department, having an authorization to process personal data on behalf of the Bank may indicate extensive experience and knowledge of an unauthorized entity, the fact that logging in to the PUE ZUS platform took place after the termination of the employment relationship, the frequency of these logins, and the time intervals between logons, indicate a deliberate and not accidental action of the former employee of the Bank, therefore in no way justify the employer's trust in the former employee. Moreover, from the explanatory activities carried out by the Administrator and the information obtained from ZUS on logging into the PUE ZUS platform, attached as evidence in the form of e-mail correspondence to the Bank's explanations of [...] March 2021, it appears that two other persons, as can be assumed, also former employees of the

Bank (Ms B. and Ms C.), who also had unauthorized access to the platform, did not log into it at all, which only confirms the intentionality and lack of randomness of actions of Ms A., who is the subject of the incident in question ( consisting in failure to withdraw the rights to PUE ZUS, resulting in the possibility of obtaining access to the personal data of the Bank's employees there). What's more, a similar opinion is shared by the Social Insurance Institution, whose employee in the e-mail correspondence of [...] February 2021 also indicates the lack of random logins of the former employee - "Unfortunately, you can see that there were several logins, so they were not accidental."

At this point, it should also be emphasized that the fact that the two other former employees of the Bank have not withdrawn the access rights to PUE ZUS, on the one hand, also proves a breach of personal data protection, consisting in failure to withdraw the rights to PUE ZUS, resulting in the possibility of obtaining access to the personal data of employees stored there. Bank, and on the other - confirms the ineffectiveness of the measures applied by the Bank in the event of termination of employment with a person having access to the PUE ZUS platform. Despite the lack of logins on the part of former employees: Ms B. and Ms C., the risk (which the administrator should rely on, and which has already been indicated in this decision many times) of unauthorized access was - it would be enough for one of the abovementioned employees logged into the system, the access to which was not denied, despite the existence of relevant premises.

According to the information provided by the Social Insurance Institution (Zakład Ubezpieczeń Społecznych), the first three logins (in the analyzed period […] June 2020 - […] February 2021) took place on […] June 2020, and the next […] October 2020. , while the last one with an interval of several months, because only [...] February 2021. Access to the platform was not a one-time, however, the employee informed about unauthorized access only after almost 8 months from the first login - on the same day on which the last login to the platform took place . The former employee did not report the fact of having unauthorized access to the PUE ZUS platform after the termination of the employment relationship, he continued to use it having access to personal data, including data on the health of other employees, posing a threat to the security of these people's data.

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 the possibility of making an independent assessment of the violation, which, after all, concerns their personal data and may have significant consequences for them, due to on the scope of the data covered by the infringement.

As another argument justifying the failure to notify the data subjects about the breach, the Bank indicates the lack of a precisely defined data area and group of data subjects, which makes it impossible to identify the threat. The above statement is incomprehensible, because at the same time the Bank refers to the fact of internal verification of access to the PUE ZUS platform, as a result of which it was established that the scope of data available for inspection by an employee authorized to process personal data is identical to that indicated by the former employee in the message informing about unauthorized access, which indicates that the former employee had access to the same categories of data processed as part of the PUE ZUS platform as the employed person, namely to the following data: name, surname, address of residence or stay, PESEL number and information from e-ZLA certificates, i.e. health data. Access to such a wide range of data poses a risk to the rights and freedoms of data subjects. Name and surname together with the address of residence or stay and PESEL identification number may be used by unauthorized persons, among others, to gain access to healthcare services and access health data, or to obtain loans from non-bank institutions by third parties.

Importantly, and also needs to be emphasized, in the present case it is not important whether an unauthorized person actually got acquainted with the personal data of other people, but the fact that such a risk occurred (he had the opportunity to get acquainted with these data), which in turn means that due to the scope of data, that there was a high risk of violating the rights or freedoms of data subjects. This opinion was also agreed by the Provincial Administrative Court in Warsaw in its judgment of September 22, 2021, file ref. no. II SA / Wa 791/21, ruling on the administrative fine imposed on the Medical University of Silesia in Katowice, in which the Court stated that "(...) in the case under consideration, it is not relevant whether the unauthorized recipient actually came into possession and familiarized himself with with the personal data of other people, but

the fact that such a risk has occurred, and as a consequence there has also been a potential risk of violating the rights or freedoms of data subjects ". Further, the Court also emphasizes that "the possible consequences of an event that has occurred do not have to materialize. In the wording of Art. 33 sec. 1 of Regulation 2016/679, it is 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, unless it is unlikely that the breach would result in a risk of violating the rights or freedoms of natural persons. Therefore, the circumstance raised by the Administrator that: "no information has been received by the University that could affect the change in the risk level or requiring taking other technical and organizational measures extending the catalog of actions taken" remains irrelevant to the Administrator's finding that there is an obligation on the part of the Administrator to report the violation of personal data protection to the President of the Personal Data Protection Office. in accordance with the above provision ".

The mere fact that there is no precisely defined group of employees affected by the breach does not constitute an obstacle to the fulfillment of the obligation under Art. 34 of Regulation 2016/679, if only because the form of providing information on a personal data breach in the case in question, taking into account the lack of a precisely defined group of entities affected by the breach, may be a public announcement, e.g. posted on the Intranet. In this regard, WP250 Guidelines should be taken into account, which state that: "controllers should choose methods that ensure the best chance of properly communicating information to all affected individuals. In some circumstances, this may mean that the administrator will use a range of communication methods rather than just one contact channel. " Therefore, it should be noted that the data controller does not have to limit himself to only one form of notification, but may use in each individual case such a form that is able to effectively notify individuals about the occurrence of a breach. The message on the website should be visible directly on the website, without the need to open additional subpages.

Moreover, according to the correspondence sent by the Administrator on [...] March 2021, related to the posted message, such content is published on the Bank's internal communication platform. It should be emphasized, however, that the information published on the Intranet does not actually refer to the personal data breach in question, because it is only general information, which is certainly a lot on the Bank's internal communication platform, about the type of personal data breach, which may be access by an unauthorized person to the personal data of employees, its possible consequences or remedial measures, therefore - this information is in no way tantamount to the fulfillment of the obligation referred to in art. 34 sec. 1 of Regulation

2016/679.

It does not appear from the content of the Communication that it relates to a specific breach and therefore the data subjects had no reason to treat it as relating to them and to react accordingly. Moreover, the message was addressed only to the current employees of the Bank as using the internal communication platform, while all persons who were employed at the Bank during the period in which access to data for an unauthorized person was open, and who are currently may not work in it anymore.

At this point, it should be pointed out again that for the obligation to notify about a breach of personal data protection to 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. The above assessment is also influenced by the long period of access of the former employee of the Bank to the PUE ZUS platform, which lasted 8 months, during which the former employee logged in to this platform several times, gaining access to the personal data of the Bank's employees on it in the scope of their personal data. names and surnames, PESEL numbers, addresses of residence or stay as well as sick leaves, which constitute data concerning health.

Referring to the evidence requests indicated by the Bank in the letter of [...] July 2021 pursuant to Art. 78 § 1 of the Code of Administrative Procedure, i.e .:

1) taking evidence from the testimony of witness A. about the fact of using the access to the PUE ZUS platform and to determine whether the former employee of the Bank read personal data on the PUE ZUS platform in the period from [...] June 2020 to [...] February 2021, and if so, to what extent; possibly: asking the authority to obtain information in writing whether, as a former employee of the Bank, he / she read personal data on the PUE ZUS platform in the period from [...] June 2020 to [...] February 2021, and if yes, to what extent;

2) the obligation of the operator of the PUE ZUS platform, i.e. the Social Insurance Institution, to present logs and all records of the IT system - the PUE ZUS platform - in order to determine which personal data A. was familiarized with when accessing PUE ZUS on the dates from the date of termination of the relationship work, ie from […] until the employee is withdrawn from PUE ZUS rights, ie […];

3) taking evidence from the opinion of an IT expert to determine which personal data A. read when accessing PUE ZUS on the dates from the date of termination of the employment relationship, i.e. from [...] to the date the employee is withdrawn from

PUE ZUS, ie until […], they should be regarded as irrelevant as they concern irrelevant circumstances; for the obligation under Art. 34 sec. 1 of Regulation 2016/679, what is important is the very risk of unauthorized access that occurred in the present case, and which has already been demonstrated many times in this decision.

Pursuant to Art. 78 § 1 of the Code of Civil Procedure, the authority conducting the proceedings is obliged to accept a party's request for evidence, if the subject of evidence is a circumstance relevant to the case. The doctrine assumes that the assessment of whether the subject of evidence is a circumstance relevant to the case or not rests with the authority, not with the party. This means that the authority conducting the proceedings is not bound by the party's evidentiary requests. On the other hand, the authority is bound in this respect by the provisions of substantive law, which constitute the basis for the decision. [1] Therefore, it will be up to the authority to decide whether to admit the evidence or not. There is no doubt that the authority should first consider whether a given circumstance for which a party has invoked evidence requires proving.

Pursuant to the judgment of the Supreme Administrative Court of August 4, 2017 (reference number I OSK 1607/16, LEX No. 2345355), in each proceeding, the authority is required to collect evidence relevant to the resolution of a given case and to make the necessary factual findings on this basis. What factual findings are necessary to settle the case, however, is determined by the correctly laid down provisions of substantive law, and not by the subjective opinion of the party. No authority conducting the proceedings is obliged to take all the evidence requested by a party. The means of evidence indicated by it cannot be omitted only if the disputed facts relevant to the resolution of the case have not been clarified. As a result, only failure to establish the circumstances relevant to the case can be considered a breach of the procedural rules, which could affect the content of the factual findings and, consequently, the content of the decision concluding the proceedings in a given case. Provided for in art. 78 of the Code of Administrative Procedure the party's right is limited due to the purposefulness and speed of the proceedings. The authority may disregard the request for taking evidence if it is to delay the case (judgment of the Supreme Administrative Court of 29 November 2016, file no. II GSK 3322/15, LEX no. 2230883).

The President of the Personal Data Protection Office found the evidence requests indicated by the Administrator to be unjustified, because in his opinion the evidence gathered in the case is sufficient to resolve the case, and the circumstances being the subject of the evidence are irrelevant to the case, while the authority is not obliged to take into account all the party's requests.

Both from the e-mail correspondence of the statement of a former employee of the Bank, Ms A., about the unauthorized

access to personal data of the Bank's employees on the PUE ZUS platform, with the following quotation: "I am a former employee of Santander Bank Polska SA, I worked at the Human Resources Department, employment relationship ended […] (I resigned […]). I report unauthorized access to personal data of the Bank's employees from the PUE ZUS platform (e.g. name, addresses, PESELES, information from e-ZLA certificates). I had this access due to the authorization granted to me on behalf of the Employer ", as well as the internal verification carried out by the Bank, aimed at comparing the scope of data to which the person authorized to process personal data of employees on the PUE ZUS platform has access with the scope of data, to which the former employee of the Bank had access to on this platform, it clearly shows what data the former employee of the Bank could have access to, i.e. names and surnames, addresses of residence or stay, PESEL number, as well as information on sick leaves, i.e. health data , Bank employees. The extract from the PUE ZUS system logs confirms that the former employee of the Bank logged in to the PUE ZUS platform five times for the payer profile of Santander Bank Polska S.A., thus gaining unauthorized access to the personal data of the Bank's employees.

Therefore, taking into account the above, it should be considered that the evidence submitted by the Bank in the scope of: hearing witness A. for the use of access to the PUE ZUS platform, obligation of the Social Insurance Institution, as the operator of the PUE ZUS platform, to present logs and all system records information technology - the PUE ZUS platform and taking evidence from the opinion of an IT expert to determine which personal data A. read as part of the access to the PUE ZUS platform on the dates from the date of termination of the employment relationship, i.e. from [...] to the date of withdrawal from the employee rights in PUE ZUS, ie until [...], relate to circumstances not relevant to the case, and thus their implementation would be pointless.

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. '

Reliable, effective and transparent notification of the data subject about the breach of personal data protection may contribute to activating the data subject, and thus minimizing its negative effects for him. Such notification is also an expression of the data administrator's care and concern for the interests of the data subject, and thus may strengthen the trust in the controller.

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 concern for the interests of data subjects, the controller should, without undue delay, provide data subjects with the best possible protection of personal data. 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.

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 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.

The above reasoning is confirmed by the judgment of the Provincial Administrative Court in Warsaw of September 22, 2021 (file reference number II SA / Wa 791/21), in which the Court, when deciding on the imposition of an administrative fine in connection with the violation of the provisions on the protection of personal data, referred to the above-mentioned the above issue, additionally pointing out that "When assessing whether there are risks of violating human rights or freedoms, the administrator should take into account all possible damage and harm that may result from a given event for natural persons (such as: S. Jandt [in:] DS.-GVO ..., edited by J. Kuhling, B. Buchner, p. 617; Y. Reif [in:] DS.- GVO ..., edited by P. Gola, p. 496 ). They may in particular consist in losing control over your own personal data, negative image consequences, the possibility of another person concluding contracts using the personal data of another natural person, financial losses or, finally,

negative social perception, which may be a consequence of making some personal data public. For the risk to occur, it is not necessary for the final loss or harm resulting from a given breach of personal data protection (as above, p. 616) ”.

Consequently, it should be stated that the Bank did not notify the data subjects of a breach of their data protection without undue delay, pursuant to Art. 34 sec. 1 of the Regulation 2016/679, which means the Bank's breach of this provision.

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, necessitating the application of such sanctions in the present case and having an aggravating impact on the size of the imposed administrative fine:

1. The nature, gravity and duration of the breach, taking into account the nature, scope or purpose of the processing in question, the number of data subjects affected and the extent of the damage suffered by them (Article 83 (2) (a) of Regulation 2016/679). in the present case, the breach consisting in the failure to notify the breach of personal data protection without

undue delay to the data subjects is of considerable importance and serious nature, as the lack of knowledge of the breach of data subjects and thus their inability to take remedial action and appropriate steps to protect your rights, may lead to property or non-material damage to the data breached persons, and the probability of their occurrence is high. The long duration of this infringement is also not without significance. 11 months during which the risk of violating the rights or freedoms of persons affected by the violation could be realized, and which these people could not counteract due to the Bank's failure to comply with the obligation to notify data subjects about the violation.

Additionally, an aggravating circumstance should be considered the fact that the breach, consisting in not notifying persons about the breach of their personal data protection, covered the personal data of many persons, as it concerned all employees of the Bank, i.e. as it results from the notification of the breach, about 10 500 people, and despite the fact that that in the present case there is no evidence that persons accessed by an unauthorized person suffered material damage, the very breach of the confidentiality of their data is a non-pecuniary damage (harm) to them. Natural persons whose data has been obtained in an unauthorized manner may at least feel the fear of losing control over their personal data, identity theft or identity fraud, discrimination, and finally financial loss.

2. 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", intention "includes both knowledge and deliberate action, in connection with the characteristics of the offense". The bank made a conscious decision not to notify data subjects. There is no doubt that the Bank, while processing personal data on a massive scale, has a high level of knowledge in the field of personal data protection, including knowledge about the consequences of finding a personal data breach resulting in the risk of violating the rights or freedoms of natural persons. Having such knowledge, after carrying out a risk analysis, the Bank made an informed decision to refrain from notifying data subjects about a breach of their personal data. 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 or freedoms. the persons concerned by the violation. Finally, the mere initiation of this proceeding by the President of the Personal Data Protection Office on the obligation to notify the data subjects of the breach should raise doubts for the Bank as to its own

assessment of the effects of the breach. And as indicated in the WP250 Guidelines, "in case of any doubts, the controller should report the breach, even if such caution could prove excessive."

3. Relevant previous violations of the provisions of Regulation 2016/679 by the administrator (Article 83 (2) (e) of Regulation 2016/679). Previous violations of the provisions of Regulation 2016/679 were found by the Bank in the scope of Art. 6 sec. 1 of Regulation 2016/679, art. 21 sec. 3 in conjunction joke. 12 sec. 3 of the Regulation 2016/679 (case reference: [...], date of the decision: [...] December 2020) and Art. 6 sec. 1 in conjunction joke. 5 sec. 1 lit. f of the Regulation 2016/679 (case reference number: [...], date of the decision: [...] .04.2021) - in both cases the President of the Personal Data Protection Office for violation of the above-mentioned regulations were provided by Santander Bank Polska S.A. based in Warsaw reminders. In the WP253 Guidelines, the Article 29 Working Party indicates that this criterion is intended to assess the business history of the infringer, therefore "Supervisory authorities should take into account the fact that the scope of such an assessment may be quite broad, as any type of breaches of the regulation, even if different from the one currently being investigated by the supervisory authority, could be 'relevant' to the assessment as it could indicate a general level of insufficient knowledge or a disregard for data protection rules. '

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 reaction 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 notify the data subjects about the breach. Correct, in the opinion of the President of the Personal Data Protection Office, the actions which could result in no negative consequences for the rights of the persons concerned or a more limited impact of these consequences than could be the case, 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 violation (Article 83 (2) (g) of Regulation 2016/679). the risk of violation of the rights or freedoms of natural persons, related to the need to notify the data subjects of the violation, constitute a wide range (name and surname, address of residence or stay, PESEL number), and also belong to specific categories of personal data referred to in art. 9 of Regulation 2016/679, because they include health data (information on sick leaves), which is associated

with a high risk of violating the rights or freedoms of natural persons. Failure to notify data subjects of a breach of the confidentiality of their personal data must be assessed more severely when it concerns personal data of a specific category. The sanctions imposed by the President of the Personal Data Protection Office in the present case in the form of an administrative fine, as well as its amount, had no influence on the other sanctions indicated in Art. 83 sec. 2 of Regulation 2016/679, the circumstances:

a) actions taken by the administrator to minimize the damage suffered by data subjects (Article 83 (2) (c) of Regulation 2016/679) - the administrator took steps to clarify the matter, as it asked the Social Insurance Institution to provide all logs that were made at PUE ZUS by an unauthorized person, however, it should be indicated that these activities did not contribute to minimizing the damage suffered by the data subjects or securing the rights of these persons, in particular by notifying them of a breach of personal data protection ;

b) 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 about the breach of personal data protection of data subjects) is not related to the technical and organizational measures applied by the controller;

c) how the supervisory authority learned about the breach (Article 83 (2) (h) of Regulation 2016/679) - about the breach of Art. 34 sec. 1 of Regulation 2016/679, consisting in failure to notify about a breach of the protection of personal data of data subjects, the supervisory authority obtained information from the breach notification sent by the Administrator, in which, due to the scope of the data, there was a high risk of violating the rights or freedoms of persons affected by this breach, resulting in the Bank's obligation to notify these persons of a breach of the protection of their personal data, the obligation of which, as indicated in the content of the notification and further correspondence in this matter, the Bank did not intend to fulfill. Importantly, the notification of a breach of personal data protection by the Bank to the President of the Personal Data Protection Office constitutes the fulfillment by the administrator of his obligation referred to in Art. 33 of the Regulation 2016/679, and in accordance with the WP253 Guidelines, “Simple compliance with this obligation by the administrator cannot be interpreted as a weakening / mitigating factor. Likewise, a controller / processor that has shown negligence because it has failed to notify or at least failed to provide full details of the breach as a result of an incorrect assessment of the extent of the breach may, in the opinion of the supervisory authority, merit a more severe sanction - in other words, it is unlikely to be

breached. considered minor ";

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

(e) 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;

(f) financial gains or losses avoided, directly or indirectly, from the breach (Article 83 (2) (k)) - the controller was not found to have gained any gains or avoided financial losses from the breach.

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, professionally and on a mass scale processing personal data, will in the future fulfill its obligations in the field of personal data protection, in particular with regard to notifying about a breach of data protection. the personal data of the persons concerned by the violation.

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 545,748 (equivalent to EUR 120,000).

In the opinion of the President of the Personal Data Protection Office, the applied fine in the amount of PLN 545,748 (in words: five hundred and forty-five thousand seven hundred and forty-eight zlotys) meets 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. From the sent "Annual Report of Santander Bank Polska S.A. for 2020 ”shows that the Bank's revenues from the Bank's operations in 2020 amounted to approx. PLN 5 billion, therefore the amount of the administrative fine imposed in this case is approx. 0.011% of the total annual global turnover of the company from the previous financial year. At the same time, it is worth emphasizing that the amount of the imposed fine (PLN 545,748.00) is only 1.2% 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 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 [...] July 2021.

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

2022-02-01