Warsaw, day 14

March

2023

Decision

DKN.5131.45.2022

Based on Article. 104 § 1 of the Act of June 14, 1960 Code of Administrative Procedure (Journal of Laws of 2022, item 2000, as amended), art. 7 sec. 1 and 2, art. 60 and Art. 102 sec. 1 item 1 i sec. 3 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 point i), art. 83 sec. 1 - 2 and art. 83 sec. 4 lit. a) in connection with art. 33 sec. 1 and art. 34 sec. 1, 2 and 4 of the Regulation of the European Parliament and of the EU Council 2016/679 of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46 / EC (Journal EU Official Journal L 119 of May 4, 2016, p. 1, EU Official Journal L 127 of May 23, 2018, page 2 and EU Official Journal L 74 of March 4, 2021, p. 35), hereinafter also referred to as "Regulation 2016/679", after conducting administrative proceedings initiated ex officio regarding the violation of the provisions on the protection of personal data by the District Prosecutor's Office in G. with its registered office in G. at ul. (…), President of the Office for Personal Data Protection,

finding a violation by the District Prosecutor's Office in G. with its registered office in G. at ul. (…) provisions: a) art. 33 sec. 1 of Regulation 2016/679, consisting in failure to notify the President of the Personal Data Protection Office of a personal data protection breach without undue delay, no later than within 72 hours after finding the breach, b) art. 34 sec. 1 of Regulation 2016/679, consisting in failure to notify data subjects of a breach of personal data protection without undue delay,1) imposes on the District Prosecutor's Office in G. with its registered office in G. at ul. (...) an administrative fine in the amount of PLN 20,000 (in words: twenty thousand zlotys),2) orders to notify the persons whose data are contained in the files of the preparatory proceedings made available on (...) November 2020, ref. no. (…), about a breach of the protection of their personal data in order to provide them with 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 surname and contact details of the data protection officer or other contact point from which more information can be obtained; c) description of the possible consequences of the data protection breach d) description of the measures taken or proposed by the administrator to remedy the breach - including

measures to minimize its possible negative effects, within 3 days from the date of delivery of this decision.

Justification

On (...) March 2021, the President of the Office for Personal Data Protection, hereinafter also referred to as the "President of the Personal Data Protection Office", received information indicating the possibility of a breach of personal data protection at the District Prosecutor's Office in G. with its registered office in G. at ul. (...), hereinafter also referred to as the Administrator, consisting in the Administrator's transfer to a local journalist on (...) November 2020, as part of the response to the request of (...) November 2020 submitted pursuant to the Act of September 6, 2001. on access to public information (Journal of Laws of 2022, item 902), documentation from the completed preparatory proceedings with reference number (...) in the form of: 1. Notifications of suspected crime of (...) October 2018 with attachments (including the family background interview questionnaire).2. Official notes of the prosecutor of (...) October 20183. Decisions of (...) October 2018 to discontinue the investigation.4. Complaints of (...) November 2018 against the decision of the prosecutor of the District Prosecutor's Office in G. to discontinue the investigation.5. Minutes of the meeting of the District Court in G. of (...) February 2019 regarding the consideration of the complaint against the decision refusing to initiate the investigation.6. Decisions of the District Court in G. of (...) February 2019 on rejection of the complaint.

One of the persons affected by the violation is X.Y. - Head of the Ł. Commune, elected for this function in the local government elections in 2018 (in the files of the preparatory proceedings, made available to the local journalist, his previous function is indicated, i.e. councilor of the Ł. Commune). As a result of the breach, his personal data was made available in the form of name and surname, ID card series and number, PESEL number, address of residence, telephone number, information on remuneration, gender, marital status, relationship and place of employment. In addition to the above-mentioned data the personal data of his wife were also made available in terms of her name and surname, date of birth, gender, marital status, kinship, PESEL number, information on remuneration and place of employment. In addition, information on a minor child was made available in terms of name and surname, date of birth, sex, marital status, kinship, PESEL number, information about the place of study and health data in the form of (…). The scope of data provided in response to the above the application also concerned the alleged acts of the councillor, i.e. the suspicion of committing a crime consisting in submitting a false statement to the Commune Social Welfare Center in Ł. about his earnings and his wife's earnings in connection with the pending proceedings to determine the fee for his son's stay in (...) . The documents provided as part of the response to the request for

public information have not been anonymised. This journalist, immediately after receiving from the Administrator a copy of the above-mentioned documents from the files of the preparatory proceedings, reference number (...), published them - previously anonymizing personal data - on the local website at (...). In connection with the above, in the letter of (...) July 2021, the President of the UODO asked the Administrator to provide information whether in connection with the above-mentioned an analysis was made in terms of the risk of violation of the rights or freedoms of natural persons necessary to assess whether there has been a data protection breach resulting in the need to notify the supervisory authority and the data subjects.

In response, in the letter of (...) August 2021, the Administrator informed the President of the UODO, inter alia, that: "(...) [In response to the letter of Z.Z. he was provided with scans of some documents from the files, except that they were not anonymised. Only one person has been given this information. Then Z.Z. submitted a notification to the Prosecutor's Office of a crime regarding the unauthorized disclosure of some personal data of the Head of the Commune of Ł. by failing to anonymise this data. Based on the decision of the District Prosecutor's Office in N., the proceedings in this case were conducted by the District Prosecutor's Office in Z., under Ref. (…). These proceedings, conducted in terms of committing an act under Art. 231 § 1 k.k., ended with a decision of (...).I.2021. about refusal to initiate an investigation. The information obtained shows that the decision is final, as X.Y. did not file a complaint" and "the Prosecutor's Office considered whether there had been a breach of personal data protection, resulting in the need to notify the President of the Office for Personal Data Protection and the persons concerned by the incident. It was deemed not to be necessary."

The President of the UODO did not agree to the above-mentioned position and therefore, acting on the basis of art. 61 § 1 and 4 of the Act of June 14, 1960, the Administrative Procedure Code (Journal of Laws of 2022, item 2000, as amended), hereinafter also referred to as "KPA", in connection with Art. 58 sec. 2 lit. e) of Regulation 2016/679, in a letter of (...) September 2022, he instituted ex officio administrative proceedings against the District Prosecutor's Office in G. regarding the failure to notify the personal data breach to the President of the UODO and the failure to notify the breach of personal data protection of the persons concerned infringement. At the same time, the President of the UODO asked the Administrator to indicate: 1) whether, in connection with the situation, an analysis of the event was made in terms of the risk of violation of the rights or freedoms of natural persons necessary to assess whether there was a data protection violation resulting in the need to notify the President of the Office for Personal Data Protection and persons affected by the breach, if yes, for providing this analysis, and if not, the justification for not conducting it; 2) the scope of data made available to an unauthorized person as a

result of the event and the number of persons to whom the data relates; 3) whether the persons concerned the breach have been notified of the breach of their personal data, if so, the provision of an anonymized notification along with the date of its sending and the means of communication used.

In response to the letter informing about the initiation of administrative proceedings, the Administrator, in a letter of (...) October 2022, informed the President of the UODO that "(...) on this matter, the local Office has already contacted me in a letter of (...).VII.2021. ref. (…). I then replied in a letter of (...).VIII.2021. a copy of which I am sending. I fully uphold the position contained therein." The administrator did not answer the questions asked regarding the scope of personal data made available to an unauthorized person and the number of persons to whom the data pertains.

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

The subject of these proceedings is the violation by the Administrator of the provisions of art. 33 sec. 1 and art. 34 sec. 1 and 2 of Regulation 2016/679, in connection with the submission, as part of the response to the request for access to public information, of documentation from the completed preparatory proceedings with reference number (...), containing personal data of natural persons that have not been anonymized. The above action does not belong to the tasks of the prosecutor's office referred to in Art. 3 of the Act of January 28, 2016. Law on the Public Prosecutor's Office (Journal of Laws of 2022, item 1257, as amended), therefore this case was resolved based on the provisions of Regulation 2016/679, and not the Act of 14 of December 2018 on the protection of personal data processed in connection with preventing and combating crime (Journal of Laws of 2019, item 125, as amended).

In accordance with 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 sent, stored or otherwise processed.

Article 33 of Regulation 2016/679 provides that in the event of a personal data breach, the data controller shall without undue delay - if possible, not later than 72 hours after finding the breach - notify the supervisory authority competent in accordance with Art. 55, unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons. The notification submitted to the supervisory authority after 72 hours is accompanied by an explanation of the reasons for the delay (paragraph 1). The notification referred to in section 1, must at least: a) describe the nature of the personal data protection breach,

including, if possible, indicate the categories and approximate number of data subjects, as well as the categories and approximate number of personal data entries affected by the breach; b) contain the name and surname and contact details of the data protection officer or the designation of another contact point from which more information can be obtained; c) describe the possible consequences of a personal data breach; d) describe the measures taken or proposed by the controller to remedy the personal data breach, including, where appropriate, measures to minimize its possible negative effects (paragraph 3).

In turn, Art. 34 sec. 1 of Regulation 2016/679 indicates that in a situation where a personal data breach may result in a high risk of violating the rights or freedoms of natural persons, the controller is obliged to notify the data subject of such a breach without undue delay. In accordance with art. 34 sec. 2 of Regulation 2016/679, the correct notification should: 1) describe the nature of the personal data protection breach in a 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 surname and contact details of the data protection officer or designation of another contact point from which more information can be obtained; b. a description of the possible consequences of a 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.

Notification of personal data breaches by controllers is an effective tool contributing to a real improvement in the security of personal data processing. When reporting a breach to the supervisory authority, controllers inform the President of the UODO whether, in their opinion, there was a high risk of infringement of the rights or freedoms of data subjects and - if such a risk occurred - whether they provided relevant information to natural persons affected by the breach. In justified cases, they may also provide information that, in their opinion, notification is not necessary due to the fulfillment of the conditions set out in art. 34 sec. 3 lit. a) - letter c) Regulation 2016/679. The President of the UODO verifies the assessment made by the administrator and may - if the administrator has not notified the data subjects - request such notification from him. Reporting a breach of personal data protection allows the supervisory authority to react appropriately, which may limit the effects of such breaches, because the controller is obliged to take effective measures to ensure the protection of individuals and their personal data, which, on the one hand, will allow to control the effectiveness of existing solutions, and on the other hand, to assess modifications and improvements to prevent irregularities similar to those covered by the breach.

In the case in question, the protection of personal data of three persons was breached, in connection with the transfer by the Administrator, as part of the response to the request submitted under the Act of September 6, 2001 on access to public

information (Journal of Laws of 2022, item . 902), non-anonymized documentation from completed preparatory proceedings with reference number (...). As the Administrator himself pointed out, the local journalist was "provided with (...) scans of some documents from the files, except that they were not anonymised". The breach covered the personal data of three people (including a child). The data made available include, in particular, name and surname, PESEL number, date of birth and degree of kinship, and in the case of a child also data subject to special protection under Art. 9 sec. 1 of Regulation 2016/679 (health data in the form of (...) and undoubtedly allow for very easy identification of these people.

In view of the above, it should be considered that, contrary to the Administrator's claims, as a result of the event in question, the confidentiality of data of natural persons was breached due to the provision of incorrectly anonymized documents. Unless the President of the UODO does not question the availability of documentation in the mode of access to public information, the principles of personal data protection must also be observed when making it available. It should be emphasized that the result of making non-anonymized documentation available was the disclosure of personal data contained in its content to a person not authorized to receive it, which resulted in a breach of personal data protection. However, from the Administrator's explanations, it should be concluded that due to the refusal to initiate an investigation in this regard by the District Prosecutor's Office in Z., he concluded that there was no violation of personal data protection. However, the administrator did not provide, despite the supervisory authority's request, any analysis in this regard, and thus did not document that he had carried out an analysis of the risk of violating the rights or freedoms of natural persons covered by the personal data breach in question, the result of which would entitle him to conclude that "in this The prosecutor's office considered whether there had been a breach of personal data protection, resulting in the need to notify the President of the Office for Personal Data Protection and the persons concerned by the incident. It was deemed not to be necessary." At the same time, it needs to be emphasized that the refusal to initiate proceedings cannot constitute grounds for assuming that in connection with the above there was no violation of the protection of personal data by the event and replace a reliable risk analysis of the rights or freedoms of natural persons. The assessment made by the District Prosecutor's Office in Z. was based on the provisions of criminal law, while the assessment whether there has been a breach of personal data protection and whether it is associated with a high risk of violating the rights or freedoms of natural persons must be made on the basis of the provisions of Regulation 2016/679 .

It should be emphasized that the assessment of the risk of violating the rights or freedoms of a natural person should be made through the prism of the person at risk, and not the interests of the administrator. This is particularly important as, based on the

notification of a breach, a natural person can assess for himself whether, in his opinion, a security incident may cause 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, the individual may assess whether, after the breach, the data controller still guarantees the proper processing of his personal data in a manner that ensures their security. Failure to notify a natural person of a breach in the event of a high risk of infringement of their rights or freedoms deprives them not only of the possibility of an appropriate response to the breach, but also of the possibility of independent assessment of the breach, which after all concerns their personal data and may have significant consequences for them. On the other hand, the lack of notification of 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 infringement for the rights or freedoms of a natural person, but also in particular in verifying whether the controller has taken appropriate measures to remedy the breach and minimize negative effects on data subjects, as well as whether it has applied appropriate security measures to minimize the risk of recurrence of the breach.

In the facts of the case in question, it should be stated that the Administrator did not assess the risk of violation of the rights or freedoms of natural persons in connection with the violation of personal data protection based on objective criteria, and also failed to demonstrate, in accordance with the accountability principle referred to in art. 5 sec. 2 of Regulation 2016/679, that it is unlikely that this infringement could result in a risk of infringement of the rights or freedoms of natural persons.

At the same time, due to the wide range of disclosed data (including name and surname and PESEL registration number, and in the case of a child, also health data), it should be stated that as a result of the event, there was a high risk of violating the rights and freedoms of natural persons. As indicated by the Article 29 Working Group in the Guidelines for reporting personal data breaches in accordance with Regulation 2016/679 (WP250rev.01), hereinafter referred to as the "WP250 Guidelines", "This risk exists when the breach may lead to physical damage or damage property or non-property for persons whose data has been breached. Examples of such damage include discrimination, identity theft or falsification, financial loss, and damage to reputation"[1]. In addition, the Article 29 Working Group in the WP250 Guidelines indicated that the administrator, when assessing the risk for natural persons resulting from the breach, should take into account the specific circumstances of the breach, including the weight of the potential impact and the likelihood of its occurrence, and recommended that during the assessment, the indicated in these guidelines should be taken into account criteria[2]. The WP250 Guidelines also explain that

when assessing the risk that may arise as a result of a breach, the controller should take into account the weight of the potential impact on the rights and freedoms of natural persons and the likelihood of its occurrence. Of course, the risk increases when the consequences of a breach are more severe, as well as when the likelihood of their occurrence increases. In case of any doubts, the administrator should report the breach, even if such caution could turn out to be excessive.

There is no doubt that the examples of damages referred to in the WP250 Guidelines, due to the scope of data covered by this personal data protection violation, including the PESEL registration number with the name and surname and address of residence, may occur in the discussed case.

At this point, it should be pointed out that the PESEL number, i.e. an eleven-digit numeric symbol containing the date of birth, serial number, gender designation and control number, uniquely identifies a specific natural person, and therefore is closely related to the private sphere of a natural person and, as a consequence, is subject to also, as a national identification number, exceptional protection under Art. 87 of Regulation 2016/679. Due to the fact that the PESEL number is a data of a special nature, its disclosure to unauthorized entities may result in a high risk of violating the rights or freedoms of natural persons (vide: tak-pracaja-oszusci - where a case was described in which: "Only the name, surname and PESEL number were enough for the scammers to extort several loans in total for tens of thousands of zlotys. Nothing else matched: neither the ID card number nor the address of residence" .

The European Data Protection Board in Guidelines 01/2021 on examples of reporting breaches of the personal data breach notification, Version 2.0, adopted on December 14, 2021 (hereinafter referred to as "Guidelines 01/2021"), aimed at supplementing the WP250 Guidelines, presented the common experience of the supervisory authorities of the European Economic Area since the entry into force of Regulation 2016/2019. Guidelines 01/2021 provide an example (example Guidelines 01/2021, case No. 14, p. 31) referring to the situation of "sending highly confidential personal data by mistake". In the mentioned case, the social security number, which is the equivalent of the PESEL number used in Poland, was disclosed. In the given example, it is clearly indicated that "The number of people affected by the breach is significant, and the use of the social security number, as well as other, more basic personal data, further increases the risk, which can be described as high.[3]"

The European Data Protection Council has no doubts that an individually assigned number that uniquely identifies a natural person should be subject to special protection, and its disclosure to unauthorized entities may involve a high risk of violating

the rights or freedoms of natural persons.

The fact that data unambiguously identifying a natural person may cause a high risk of violating rights or freedoms is also indicated by the European Data Protection Board in other examples provided in the Guidelines 01/2021. Points 65 and 66 of Guidelines 01/2021 indicate: "(...) The breached data allow for unambiguous identification of data subjects and contain other information about them (including gender, date and place of birth), moreover, they may be used by attacker to guess customer passwords or to conduct a spear phishing campaign targeted at the bank's customers. For these reasons, it was considered that a data protection breach is likely to result in a high risk of violating the rights and freedoms of all data subjects. Therefore, it is possible that material damage (e.g. financial loss) and intangible damage (e.g. identity theft or fraud) may occur. In turn, point 96 indicates that "When assessing the risk, the controller should take into account the potential consequences and negative effects of a breach of confidentiality. As a result of the breach, data subjects may fall victim to identity fraud related to the data available on the stolen device, therefore the risk is considered high.

Similar doubts (that the disclosure of the PESEL number together with other personal data may result in a high risk of violating the rights or freedoms of natural persons) were also not expressed by the Voivodeship Administrative Court in Warsaw, which in its judgment of September 22, 2021, file ref. II SA/Wa 791/21, stated that "There is no doubt that the examples of damage referred to in the guidelines may occur in the case of persons whose personal data - in some cases, including the PESEL registration number or ID card series and number - have been recorded on shared recordings. Not without significance for such an assessment is the possibility, based on the disclosed data, to identify persons whose data has been affected by the breach.". The Court further pointed out in the aforementioned judgment - "Data has been made available to unauthorized persons, which means that there has been a security breach leading to unauthorized disclosure of personal data, and the scope of these data, including in some cases also the PESEL registration number or the series and number of the ID card, determines the that there was a high risk of violating the rights or freedoms of natural persons." The PESEL number serves as the identification data of each person and is commonly used in contacts with various institutions and in legal circulation. The PESEL number together with the name and surname unambiguously identify a natural person in a way that allows the negative effects of the violation (e.g. identity theft, loan extortion) to be attributed to that particular person.

Considering the above issues, the position of the Provincial Administrative Court in Warsaw, expressed in the judgment of July 1, 2022, issued in the case with reference number II SA/Wa 4143/21. In the justification of this judgment, the Court stated that:

"One should agree with the President of the UODO that the loss of confidentiality of the PESEL number in connection with personal data such as: name and surname, registered address, bank account numbers and the identification number assigned to the Bank's customers - CIF number , involves a high risk of violating the rights or freedoms of natural persons. In the event of a breach of such data as name, surname and PESEL number, identity theft or falsification is possible, resulting in negative consequences for the data subjects. Therefore, in the case in question, the Bank should, without undue delay, pursuant to Art. 34 sec. 1 of the GDPR, notify the data subjects of the breach of personal data protection, so as to enable them to take the necessary preventive measures." The Provincial Administrative Court in Warsaw issued a similar opinion in the judgment of August 31, 2022, file ref. II SA/Wa 2993/21, indicating that "(...) the authority correctly assumed that there was a high risk of violating the rights and freedoms of persons affected by the violation in question due to the possibility of easy identification of persons whose data was disclosed on the basis of the disclosed data affected by the infringement. This data is the name and surname, correspondence address, telephone number, PESEL number of persons with Polish citizenship. In this situation, the controller was obliged to notify the data subjects of the breach without undue delay."

From the latest report infoDOK[4] (prepared as part of the Social Information Campaign of the DOKUMENTY RESERVED System, organized by the Polish Bank Association and some banks, under the auspices of the Ministry of the Interior and Administration and in cooperation with, among others, the Police and the Consumer Federation) , shows that in the third quarter of 2022, 2089 fraud attempts for loans and credits were recorded. Throughout 2020, 6,884 fraud attempts were recorded for the amount of PLN 253.8 million, and throughout 2021, 8,096 fraud attempts were recorded for loans for the total amount of PLN 336.6 million. This means that the entire year of 2021 in terms of the number of phishing attempts and their amounts was significantly more dangerous than the previous one: there was a 17% increase in the number of phishing attempts and a 32% increase in the total amount of these phishing attempts.

In addition, as it results from the jurisprudence, judgments in credit fraud cases are not uncommon and have been issued by Polish courts in similar cases for a long time - for example, the judgment of the District Court in Łęczyca of July 27, 2016 (reference number I C 566/15), in which fraudsters taking out a loan for someone else's data used a PESEL number, a fictitious address and an incorrect ID number (invalid). In the justification of the above of the judgment, the Court stated that: "In the case in question, the plaintiff (...) with its registered office in W. purchased a receivable from (...) Limited Liability Company S.K.A. with its registered office in W. A party to the loan agreement of May 5, 2014 was a person who used the data

of J. R. (...) Spółka z ograniczoną odpowiedzialnością S.K.A. in an unauthorized manner. with its registered office in W. transferred the amount of PLN 500 to the indicated bank account.

The key issue in this case was to establish that the defendant did not conclude a loan agreement, which was the allegation raised by the defendant throughout the proceedings.

The evidence proceedings conducted and the analysis of the documents attached by the plaintiff result in the fact that it can be unequivocally stated that in the case under consideration the defendant was not a party to the loan agreement concluded on May 5, 2014. Although the PESEL number of the defendant J.R. was used for its conclusion, the indicated place of residence does not correspond to the place of residence of the defendant. Defendant J.R. never lived in W. The loan amount was transferred to an account that was not owned by the defendant. On the date of concluding the loan agreement, the ID card No. (...) expired on March 15, 2014. Also, the mobile phone number indicated in the loan agreement and its attachments does not match the actual telephone numbers used and still being used by the defendant.

In the circumstances of the case under consideration, the Court found that the defendant had demonstrated that it was not a party to the loan agreement being the subject of these proceedings. Agreements concluded by means of distance communication should require detailed, thorough verification, and such verification carried out in the case in question leads to the conclusion that the defendant was not a party to the loan agreement."

An additional threat to the rights or freedoms of natural persons is related to the disclosure of data on the child's health in connection with information about his/her stay in (...), e.g. discrimination of the child, persecution and humiliation by peers.

The obligation to report a breach of personal data protection specified in art. 33 sec. 1 of Regulation 2016/679 is also not dependent on whether the risk of violating the rights or freedoms of natural persons has materialized. As indicated by the Provincial Administrative Court in Warsaw in the justification for the judgment of September 22, 2021, file ref. II SA/Wa 791/21, “It should be emphasized that the possible consequences of the event do not have to materialize. In the content of art. 33 sec. 1 of Regulation 2016/679 indicates that the mere occurrence of a personal data breach, which involves the risk of violating the rights or freedoms of natural persons, implies the obligation to notify the breach to the competent supervisory authority, unless it is unlikely that the breach will result in a risk of violating the rights or freedoms natural persons”. The Provincial Administrative Court in Warsaw made a similar statement in the judgment of January 21, 2022, file ref. II SA/Wa 1353/21, stating that "(...) the possible consequences of a personal data breach do not have to materialize - because in art. 33 sec. 1 of

the GDPR, it says that the mere occurrence of a personal data breach, which involves the risk of violating the rights or freedoms of natural persons, implies the obligation to report the breach to the competent supervisory authority. The fact, raised by the Company, that as a result of the breach there was no physical damage or damage to natural persons is irrelevant to the conclusion that there is an obligation on the part of the Company to notify the President of the Personal Data Protection Office of a breach of personal data protection, in accordance with the above-mentioned recipe."

It is also irrelevant that the data has been made available to one identified person. The data has been made available to an unauthorized person, which means that there has been a security breach leading to unauthorized disclosure of personal data, and the scope of this data (including, among others, the PESEL registration number) determines the high risk of violation of the rights or freedoms of natural persons. Making data available to even one identified person may lead to an increase in the scale of the infringement and thus the risk of violating the rights or freedoms of the data subjects. At the same time, the Administrator has not demonstrated, in accordance with the accountability principle referred to in art. 5 sec. 2 of Regulation 2016/679 that a local journalist to whom non-anonymised documents from the files of the preparatory proceedings with reference number (...), can be considered as the so-called trusted recipient.

In a situation where, as a result of a personal data breach, there is a high risk of violating the rights or freedoms of natural persons, the controller is obliged to implement all appropriate technical and organizational measures to immediately identify a personal data breach and quickly inform the supervisory authority, as well as persons whose data applies. The controller should fulfill this obligation as soon as possible.

Recital 85 of the preamble to Regulation 2016/679 explains: "In the absence of an appropriate and prompt response, a personal data breach may result in physical, material or non-material damage to individuals, such as loss of control over their own personal data or limitation of rights, discrimination, theft or falsification of identity, financial loss, unauthorized reversal of pseudonymisation, damage to reputation, breach of confidentiality of personal data protected by professional secrecy or any other significant economic or social damage. Therefore, immediately after becoming aware of a personal data breach, the controller should report it to the supervisory authority without undue delay, if feasible, no later than 72 hours after becoming aware of the breach, unless the controller can demonstrate in accordance with the accountability principle that it is unlikely that the breach could result in a risk to the rights and 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 states: "The controller should inform the data subject without undue delay of a breach of personal data protection, if it may cause 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 contain a description of the nature of the personal data breach and recommendations for a given natural person as to minimizing 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 data subjects to be informed immediately, while the implementation of appropriate measures against the same or similar data breaches may justify later notification.'

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. Article 34 par. 1 and 2 of Regulation 2016/679 aims 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) of Regulation 2016/679 (cf. Witold Chomiczewski [in:] GDPR. General Data Protection Regulation. Commentary. 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 a breach of personal data protection and 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 controller should have provided data subjects with the best possible protection of personal data without undue delay. To achieve this goal, it is necessary to at least indicate the information listed in art. 34 sec. 2 of Regulation 2016/679, which the administrator failed to fulfill. Therefore, by deciding not to notify the supervisory authority and the data subjects of the breach, the controller, in practice, deprived these persons of reliable information about the breach and the ability to counteract potential damage, provided without undue delay.

When applying the provisions of Regulation 2016/679, it should be borne in mind that the purpose of this regulation (expressed in Article 1(2)) is to protect the fundamental rights and freedoms of natural persons, in particular their right to the protection of personal data, and that the protection of natural persons in connection with the processing of personal data is one of the

fundamental rights (first sentence of recital 1 of the preamble). In case of any doubts, e.g. as to the performance of duties by administrators - not only in a situation where personal data protection has been breached, but also when developing technical and organizational security measures to prevent them - these values should be taken into account in the first place.

As a consequence, it should be stated that the Administrator did not report a breach of personal data protection to the supervisory authority in performance of the obligation under Art. 33 sec. 1 of Regulation 2016/679 and did not notify the data subjects without undue delay of the breach of the protection of their data, in accordance with art. 34 sec. 1 of Regulation 2016/679, which means a violation of these provisions by the Administrator.

In accordance with art. 34 sec. 4 of Regulation 2016/679, if the controller has not yet notified the data subject of a personal data breach, the supervisory authority - taking into account the likelihood that this personal data breach will cause a high risk - may request it or may state that that one of the conditions referred to in sec. 3. In turn, from the content of art. 58 sec. 2 lit. e) of Regulation 2016/679 shows that each supervisory authority has a corrective power in the form of ordering the controller to notify the data subject of a data protection breach.

In addition, in accordance with 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 corrective measures provided for in art. 58 sec. 2 of Regulation 2016/679, an administrative fine pursuant to Art. 83 of Regulation 2016/679, depending on the circumstances of a particular case. The President of the UODO states that in the considered case there were premises justifying the imposition of an administrative fine on the Administrator based on Art. 83 sec. 4 lit. a) of Regulation 2016/679, which states, among other things, that a 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 global turnover from the previous financial year, with the higher amount applicable. However, from art. 102 sec. 1 of the Act of May 10, 2018 on the Protection of Personal Data (Journal of Laws of 2019, item 1781), it follows that the President of the UODO may impose, by way of a decision, administrative fines of up to PLN 100,000 on: public finance sector entities referred to in art. 9 points 1-12 and 14 of the Act of August 27, 2009 on public finance, a research institute or the National Bank of Poland. From sec. 3 of this article also shows that the administrative fines referred to, inter alia, in sec. 1, the President of the Office imposes on the basis and under the conditions specified in Art. 83 of Regulation 2016/679.

Pursuant to the content of art. 83 sec. 2 of Regulation 2016/679, administrative fines are 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 point. j) Regulation 2016/679. When deciding to impose an administrative fine on the Administrator, the President of the UODO - pursuant to art. 83 sec. 2 lit. a) - k) of Regulation 2016/679 - took into account the following circumstances of the case, which make it necessary to apply this type of sanction in this case and have an aggravating effect on the amount of the fine imposed:

a) The nature, gravity and duration of the infringement, taking into account the nature, scope or purpose of the given processing, 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 is of considerable weight and serious nature, because the notification of personal data breaches by data controllers is an effective tool contributing to a real improvement in the security of personal data processing. First of all, on the basis of the information provided by the controllers in the personal data breach notifications, the supervisory authority may assess whether the controller correctly analyzed the impact of the breach on the rights or freedoms of the data subjects affected by the breach, and, consequently, whether there is a high risk of breach rights or freedoms of natural persons and it is necessary to notify these persons of a breach of their data. Correctly performed by the administrators the obligations set out in art. 33 sec. 1 and 34 sec. 2 of Regulation 2016/679 also allow for limiting the negative effects of such breaches and eliminating or at least reducing the risk of such breaches in the future, as controllers are obliged to take actions that will ensure proper protection of personal data by applying appropriate security measures and controlling their effectiveness. In addition, it should be emphasized that failure to notify data subjects of a breach of the protection of their personal data may lead to material or non-material damage, and the probability of their occurrence is high. The President of the UODO considers the long duration of the infringement to be an aggravating circumstance. Twenty-seven months have passed since the Administrator became aware of the breach of personal data protection until the date of this decision, during which the risk of violating the rights or freedoms of persons affected by the breach could materialize, and which these persons could not prevent due to the Administrator's failure to comply with the obligation to notify them of a breach.

b) Intentional nature of the infringement (Article 83(2)(b) of Regulation 2016/679). In accordance with the Guidelines of the Article 29 Working Party on the application and determination of administrative fines for the purposes of Regulation No. 2016/679 WP253 (adopted on 3 October 2017, approved by the EDPB on May 25, 2018), intent "includes both knowledge and intentional action in connection with the characteristics of the prohibited act". The administrator made a conscious decision not to notify the President of the UODO and the data subjects of the breach. Special protection of personal data, including, in

particular, the PESEL number, is required from public trust institutions, which undoubtedly include the Administrator. Being aware of this, the Administrator decided, however, to resign from reporting the infringement to the President of the UODO and notifying the data subjects, despite the fact that the President of the UODO first informed the Administrator about the obligations incumbent on the administrator in connection with the breach of data protection. After all, the mere initiation by the President of the UODO of these proceedings regarding the obligation to report a personal data breach to the supervisory authority and notify the data subjects of the breach should raise at least doubts with the Controller as to the correctness of its position.

c) The degree of cooperation with the supervisory authority in order to remove the infringement and mitigate its possible negative effects (Article 83(2)(f) of Regulation 2016/679). In this case, the President of the UODO considered the Administrator's cooperation with it unsatisfactory and disregarding it attitude towards his actions. This assessment concerns the Administrator's reaction to the letters of the President of the UODO informing about the obligations incumbent on the administrator in connection with the breach of data protection, or finally to the initiation of administrative proceedings regarding the obligation to notify the breach of personal data protection and notify data subjects of the breach. In the opinion of the President of the UODO, actions that were correct (notifying the infringement to the President of the UODO and notifying the persons affected by the infringement) were not taken by the Administrator even after the President of the UODO initiated administrative proceedings in the case. The administrator limited himself to referring only to his previous explanations.

d) Categories of personal data to which the violation concerned (Article 83(2)(g) of Regulation 2016/679). Personal data made available to an unauthorized person, apart from data regarding name and surname, ID card series and number, address of residence, PESEL registration number date of birth, telephone number, information on remuneration, gender, marital status, degree of kinship, place of employment, information on the place of study and data on alleged acts, also include data on special categories of data referred to in art. 9 sec. 1 of Regulation 2016/679, i.e. health data in the form of (…). Such a scope of data made available to an unauthorized person is associated with a high risk of violating the rights or freedoms of natural persons. PESEL number, i.e. an eleven-digit numerical symbol that uniquely identifies a natural person, containing the date of birth, serial number, gender designation and control number, and therefore closely related to the private sphere of a natural person and also subject to exceptional protection as a national identification number under Art. 87 of Regulation 2016/679, is data of a special nature and requires such special protection. There is no other such specific data that would unambiguously

identify a natural person. It is not without reason that the PESEL number serves as the identification data of each person and is commonly used in contacts with various institutions and in legal circulation. The PESEL number together with the name and surname unambiguously identify a natural person in a way that allows the negative effects of the violation (e.g. identity theft, loan extortion) to be attributed to that particular person.

When determining the amount of the administrative fine, the President of the UODO found no grounds to take into account the mitigating circumstances affecting the final penalty. The fact that the President of the UODO applied a sanction in the form of an administrative fine in this case, as well as its amount, had no other influence , indicated in art. 83 sec. 2 of Regulation 2016/679, circumstances:

1. Actions taken by the administrator to minimize the damage suffered by the data subjects (Article 83(2)(c) of Regulation 2016/679). Based on the evidence collected in the case, no such actions were taken by the Administrator.

2. Level of administrator's responsibility, taking into account the technical and organizational measures implemented by him pursuant to art. 25 and 32 (Article 83(2)(d) of Regulation 2016/679). The infringement assessed in these proceedings (failure to notify the President of the UODO of a breach of personal data protection and failure to notify data subjects of a breach of personal data protection) is not related to the applicable by the administrator using technical and organizational means.

3. Relevant previous violations of the provisions of Regulation 2016/679 on the part of the administrator (Article 83(2)(e) of Regulation 2016/679). The President of the UODO did not find any previous violations of the provisions on the protection of personal data by the Administrator, in connection with there is no basis for treating this circumstance as aggravating. And since such a state (compliance with the provisions on the protection of personal data) is a natural state resulting from the legal obligations incumbent on the Administrator, it also cannot have a mitigating effect on the assessment of the infringement made by the President of the UODO.

4. How the supervisory authority found out about the infringement (Article 83(2)(h) of Regulation 2016/679). On the occurrence of the said violation of the provisions of art. 33 sec. 1 and art. 34 sec. 1 of Regulation 2016/679, i.e. disclosure of personal data processed by the Administrator to an unauthorized person, the President of the UODO was informed by a third party.

5. Observance of the measures previously applied in the same case referred to in Art. 58 sec. 2 of Regulation 2016/679 (Article 83(2)(i) of Regulation 2016/679). Before issuing this decision, the President of the UODO did not apply any measures listed in art. 58 sec. 2 of Regulation 2016/679, therefore the Administrator was not obliged to take any actions related to their

application, and which actions, subject to the assessment of the President of the UODO, could have an aggravating or mitigating impact on the assessment of the violation found.

6. Application of approved codes of conduct pursuant to Art. 40 of Regulation 2016/679 or approved certification mechanisms under Art. 42 of Regulation 2016/679 (Article 83(2)(j) of Regulation 2016/679). The administrator does not use the instruments referred to in Art. 40 and art. 42 of Regulation 2016/679. However, their adoption, implementation and application is not - as stipulated in the provisions of Regulation 2016/679 - mandatory for controllers and processors, therefore the circumstance of their non-application cannot be considered to the disadvantage of the Controller in this case. In favor of the Administrator, however, the circumstance of adopting and applying such instruments as measures guaranteeing a higher than standard level of protection of personal data being processed could be taken into account.

7. Financial benefits achieved directly or indirectly in connection with the infringement or losses avoided (Article 83(2)(k) of Regulation 2016/679). precipitate. Therefore, there are no grounds for treating this circumstance as incriminating the Administrator. The finding of measurable financial benefits resulting from the violation of the provisions of Regulation 2016/679 should be assessed definitely negatively. On the other hand, failure by the Administrator to achieve such benefits, as a natural state, independent of the infringement and its effects, is a circumstance that, by nature, cannot be a mitigating factor for the Administrator. This is confirmed by the wording of Art. 83 sec. 2 lit. k) of Regulation 2016/679, which requires the supervisory authority to pay due attention to the benefits "achieved" - occurred on the part of the entity committing the infringement.

8. Other aggravating or mitigating factors applicable to the circumstances of the case (Article 83(2)(k) of Regulation 2016/679).

The President of the UODO, examining the case comprehensively, did not notice any circumstances other than those described above that could affect the assessment of the infringement and the amount of the adjudicated administrative fine.

In the opinion of the President of the UODO, the applied administrative fine fulfills, in the circumstances of this case, 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 will lead to the Administrator fulfilling its obligations in the field of personal data protection in the future, in particular in the field of reporting a personal data breach to the President of the UODO and notifying about a breach of personal data protection of persons affected by the infringement.

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 Administrator's violation of the provisions of Regulation 2016/679. It will also have a preventive function; in the opinion of the President of the UODO, it will indicate to both the Administrator and other data administrators the reprehensibleness of disregarding the obligations of administrators related to the occurrence of a breach of personal data protection, and aimed at preventing its negative effects, often severe for the persons affected by the breach, as well as removing or at least reducing these effects.

In connection with the above, it should be pointed out that the administrative fine in the amount of PLN 20,000 (say: twenty thousand zlotys) meets the conditions referred to in Art. 83 sec. 1 of Regulation 2016/679, due to the seriousness of the violation 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. At the same time, the amount of the administrative fine imposed by this decision on the administrator being a unit of the public finance sector (public authorities, including government administration bodies, state control and law enforcement bodies, as well as courts and tribunals - indicated in Article 9 point 1 of the Act of August 27, 2009 on public finances), falls within the specified in art. 102 sec. 1 of the Act of May 10, 2018 on the protection of personal data (Journal of Laws of 2019, item 1781), the limit is PLN 100,000.

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

[1] Guidelines of the Article 29 Working Party on the notification of personal data breaches under Regulation 2016/679, adopted on October 3, 2017, last amended and adopted on February 6, 2018, approved by the European Data Protection Board in on May 25, 2018, p. 27

[2] Ibidem, p. 28.

[3] Guidelines 01/2021 on examples of personal data breach notification adopted on December 14, 2021, version 2.0 by the European Data Protection Board, page 32

[4]

https://www.zbp.pl/getmedia/731d1b29-3b2d-4dcf-9310-20aec2923725/infodok-2022-07-09-wydanie-51-sklad-221025-gk06

Print article

Metadata

Provider:

Inspection and Infringement Department

Produced information:

John Nowak

2023-03-14

Entered the information:

Wioletta Golanska

2023-04-06 09:48:47

Recently modified:

Edith Magziar

2023-05-10 11:58:28