Warsaw, on 01

March

2023

Decision

DKN.5131.49.2021

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 art. 60, art. 101 and art. 103 of the Act of May 10, 2018 on the protection of personal data (Journal of Laws of 2019, item 1781), as well as art. 57 sec. 1 lit. a) and h), Art. 58 sec. 2 lit. e) and i), Art. 83 sec. 1 and sec. 2, art. 83 sec. 4 lit. a) in connection with art. 33 sec. 1 and art. 34 sec. 1, 2 and 4 of the Regulation of the European Parliament and of the EU Council 2016/679 of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46 / EC (general regulation on data protection) (OJ L 119 of 04.05.2016, p. 1, OJ L 127 of 23.05.2018, p. 2 and OJ L 74 of 4.03.2021, p. 35), hereinafter referred to as "Regulation 2016/679", after administrative proceedings initiated ex officio regarding the violation of the provisions on the protection of personal data by the Housing Cooperative "(...)" with its registered office in O. (ul. (...), (...) O.), President of the Personal Data Protection Office,

1) stating that the Housing Cooperative "(...)" with its registered office in O. (ul. (...), (...) O.) has violated the provisions of: a) Art. 33 sec. 1 of Regulation 2016/679, consisting in failure to notify the President of the Personal Data Protection Office of a breach of personal data protection without undue delay, no later than within 72 hours after finding the breach, and b) art. 34 sec. 1 of Regulation 2016/679, consisting in failure to notify a personal data breach without undue delay to the data subject, imposes on Spółdzielnia Mieszkaniowa "(...)" with its seat in O. (ul. (...), (…) O.) an administrative fine in the amount of PLN 51,876.00 (in words: fifty-one thousand eight hundred and seventy-six zlotys),

2) orders Spółdzielnia Mieszkaniowa "(...)" with its seat in O. (ul. (...), (…) O.) to notify - within 3 days from the date of delivery of this decision - the person whose data has been disclosed as a result of the disclosure in question , about a breach of the protection of her personal data in order to provide her 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 controller to remedy the breach - including measures to minimize its possible negative effects.

Justification

The President of the Office for Personal Data Protection, hereinafter also referred to as the "President of the UODO" or the "supervisory authority", on [...] August 2021 received information from a third party indicating that it was made available - as an unauthorized person - the notification of [. ..] of August 2021 about the suspicion of committing a crime that revealed personal data in the form of: name, surname, PESEL registration number and address of residence of the person indicated in this notification, hereinafter referred to as: "Data Subject" or "member of the Cooperative", by the Cooperative Mieszkaniowa "(...)" with its registered office in O. (ul. (...), (...) O.), hereinafter referred to as the "Administrator" or "Cooperative". A third party who, as a person professionally associated with the information media, has become an unauthorized recipient of the above. document, explained that she received the data contained therein "(...) of her own will of the vice-president of the management board [note: Spółdzielnia] (...)", she never applied for them and they were not known to her before.

In connection with the above, in the letter of [...] September 2021, the President of the UODO, pursuant to art. 58 sec. 1 lit. a) and e) of Regulation 2016/679, asked the Cooperative to clarify whether in connection with the above 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 has been a data protection violation resulting in the need to notify the President of the UODO and the persons affected by the violation. This letter also contains information on the content of art. 33 sec. 1 and 3 of Regulation 2016/679 and about possible ways of reporting a personal data breach.

The answer given by the Housing Cooperative in the letter of [...] September 2021 shows that "(...) one of the persons who is a resident in the resources of the Housing Cooperative (...), dissatisfied with the amount of service charges (water charges, independent of the Housing Cooperative) launched a negative campaign against the Housing Cooperative in local media and on the Internet, making its personal data publicly available". The administrator also explained in this letter that as a result of actions aimed at clarifying the situation, a notification was submitted on suspicion of committing a crime by the above-mentioned person, and then "(...) in order to present the true state of facts to the public, the Management Board called a press conference only for journalists, where it presented the facts and provided journalists with a photocopy of the notification of suspected crime, believing in the reliability of the journalistic profession and in the Press Law Articles 4, 11 and 12 of this

law) personal data has been deemed to be safe. This activity was recorded in the Infringement Register, the Personal Data Protection Inspector assessed that the risk of violating the rights and freedoms of a natural person who has made his personal data public is low.

In connection with the above explanations, the President of UODO asked the Housing Cooperative in a letter of [...] October 2021 to provide information whether the data subject has made public a notification of suspicion of committing a crime relating to him, and if so , then in what circumstances and in what part. In response to this letter, dated [...] October 2021, the Cooperative explained that it had no information whether the data subject made a photocopy of the notification of suspected crime publicly available, nor did it know whether obtained a copy.

In the absence of notification of a personal data breach to the supervisory authority and no notification of a breach of personal data protection of the person affected by the breach, on [...] November 2021, the President of the UODO instituted administrative proceedings against the Housing Cooperative ex officio in this regard. In this letter, the Administrator was additionally asked to provide a register of violations and an assessment of the level of risk carried out by the Data Protection Inspector, referred to in the letter of September 2021 of the Housing Cooperative.

In response to the above, The Housing Cooperative provided (in a letter of [...] November 2021) i.a. a photocopy of "(...)" including two entries. One of them concerned the violation of Art. "33 sec. 1 sentence 1 in principio" of Regulation 2016/679, which has been marked as not subject to the obligation to notify the supervisory authority and the obligation to notify the data subject. This entry also included the following data: - circumstances of the violation: "[...] August 2021, the President of the Housing Cooperative (...) at the press conference provided journalists with copies of the letter of notification about the possibility of committing a crime by a member of the Cooperative (...)"; - the effects of the violation : "Overlooking a photocopy of personal data and not blurring this data. In connection with Articles 4, 11 and 12 of the Press Law, an action that does not bear the characteristics of a high violation of the rights and freedoms of natural persons"; - remedial actions taken: "Additional training of employees in the principles of personal data protection".

As this information did not constitute all the data that the President of the UODO requested the Administrator to provide in the letter of [...] November 2021, on [...] December 2021 the Housing Cooperative was again requested to submission of the risk assessment carried out by the Data Protection Officer, referred to in the letter of the Housing Cooperative of [...] September 2021. By letter received by the local Office on [...] January 2022, the Housing Cooperative submitted to the supervisory

authority only a document entitled: "(...)", which did not contain information on the analysis of the risk of violation of the rights or freedoms of the data subject in the document made available to unauthorized recipients by the Data Protection Inspector.

After reviewing all the evidence collected in the case, the President of the Personal Data Protection Office considered the following: Pursuant to Art. 4 point 12 of Regulation 2016/679 "personal data breach" 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.

Article 33 par. 1 and 3 of Regulation 2016/679 provides that in the event of a personal data breach, the controller shall without undue delay - if possible, no later than 72 hours after finding the breach - report it to 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 shall be accompanied by an explanation of the reasons for the delay. 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 and 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 address the personal data breach, including, where appropriate, measures to minimize its possible negative effects.

In turn, Art. 34 sec. 1 of Regulation 2016/679 indicates that in the event of a high risk to the rights or freedoms of natural persons resulting from a breach of personal data protection, the controller is obliged to notify the data subject of the 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) 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.

Starting the analysis of the case in question, it should be pointed out that the President of the UODO in the publication entitled "Obligations of administrators related to personal data breaches" explains: "Depending on the level of risk of violating the rights

and freedoms of natural persons, the administrator is faced with different obligations towards the supervisory authority, as well as data subjects. If, as a result of the analysis, the controller found that the likelihood of a risk of violating the rights and freedoms of natural persons is low, he is not obliged to report the infringement to the President of the Office for Personal Data Protection. The indicated infringement must only be recorded in the internal register of infringements. In the event of a risk of violation of the rights and freedoms of natural persons, the administrator is obliged to notify the data protection breach to the President of the UODO, as well as to enter an entry in the internal register of violations. The occurrence of a high risk of violation of the rights and freedoms of natural persons, in addition to an entry in the register of violations, requires the administrator to take appropriate action, both towards the supervisory authority (notification of a data protection breach), but also in some cases also towards the data subjects. In the case of breaches that may cause a high risk of violating the rights or freedoms of the data subject, the GDPR introduces an additional obligation to immediately notify the data subject by the controller, unless the latter has taken preventive measures before the breach or remedial measures after the breach (Article 34 section 3 of the GDPR).

As follows from the above, if the controller detects a breach of personal data protection, it is first necessary to carry out an analysis in terms of the risk of infringement of the rights or freedoms of natural persons. The administrator is released from the obligation to notify the supervisory authority of a breach if, as a result of the conducted examination, it turns out that there is at most a low probability of a risk of infringement of the rights or freedoms of natural persons. However, it should be borne in mind that the supervisory authority will be able to ask the controller to justify the decision not to report a breach, therefore the conclusions of the analysis should be recorded in the internal register of breaches. It is worth recalling that the WP250 Guidelines[1] contain recommendations of the Article 29 Working Group regarding the requirement to report breaches to the supervisory authority.

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 the possibility 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 for data subjects, as well as whether it has applied appropriate security measures to minimize the risk of recurrence of the breach.

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) and b) of 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. On the other hand, notification of a breach to natural persons provides the opportunity to provide these persons with information on the risk associated with the breach and to indicate actions that these persons can take to protect themselves against the potential negative effects of the breach (this enables the individual to independently assess the breach in the context of the possibility of materializing negative consequences for such a person and deciding whether to apply or not to apply remedial measures). As a side note, it should be emphasized that the obligation to notify a natural person of a breach does not depend on the materialization of negative consequences for such a person, but on the very possibility of such a risk.

The mere assessment of the breach carried out by the controller in terms of the risk of infringement of the rights or freedoms of

natural persons necessary to determine whether there has been a data protection breach resulting in the need to notify the President of the UODO (Article 33(1) and (3) of Regulation 2016/679) and the persons affected by the breach (Article 34(1) and (2) of Regulation 2016/679) should be, as it should be emphasized once again, made through the prism of the person affected by the infringement. In the case in question, however, the Administrator did not prove that such a risk assessment had been made at all - in response to a two-time request to submit such an assessment, he only provided a document ("(...)"), which was of a general nature and did not refer to a specific (considered in this decision) case of a breach of the protection of the Data Subject's personal data.

The President of the UODO, assessing the risk of violating the rights or freedoms of a natural person in the case in question, stated that the breach of confidentiality of data that occurred in connection with the breach of personal data protection consisting in providing an unauthorized entity with a specific document containing personal data of a member of the Cooperative in the scope of: PESEL registration number together with the name and surname and address of residence, causes a high risk of violating the rights or freedoms of a natural person. As indicated by the Article 29 Working Group in the WP250 Guidelines: "This risk exists when a breach may lead to physical or material or non-material damage to the persons whose data has been breached. Examples of such harm include discrimination, identity theft or forgery, 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 breach of personal data protection, including the PESEL registration number along with the name and surname and address of residence, may occur in the discussed case.

Developing the above statement - referring to each of the data covered by the breach in question - it should be emphasized that the existing breach of personal data protection concerned the PESEL registration number, i.e. an eleven-digit numeric symbol, uniquely identifying a natural person, containing, among others: date of birth and gender designation, i.e. closely related to the private sphere of a natural person and also subject, as a national identification number, to exceptional protection under Art. 87 of Regulation 2016/679 - being data of a special nature and requiring such special protection. In addition, it should be taken into account that as a result of the breach of personal data protection, this registration number was made available to an unauthorized person along with the name and surname of a member of the Housing Cooperative, which is sometimes sufficient to "impersonate" the subject of this data and take out on behalf of and to the detriment of such an entity, e.g. pecuniary liabilities (vide: https://www.bik.pl/poradnik-bik/wyluznie-kretu-tak-dzialaja-oszusci - where a case is described

in which: "Only the name, surname and PESEL was enough for scammers to extort over a dozen loans for a total of tens of thousands of zlotys. Nothing else was correct: neither the ID card number nor the address of residence"). It should also not be overlooked that the analyzed infringement also covered the address of residence of a member of the Cooperative. In addition, the disclosure of these data took place in a special context: the letter containing this data was, as already mentioned, a notification of suspicion of committing a crime, which cannot be considered indifferent when assessing the risk of violating the rights or freedoms of a natural person related to the disclosure of personal data to an unauthorized recipient.

It should be noted that, in the opinion of the President of the UODO, which has been consistently raised for many years, the PESEL number is a unique identifier of a person, containing a lot of information about a given person, and its disclosure to an unauthorized person may result in a number of consequences for such a person.

It is worth pointing out here the Guidelines of the European Data Protection Board 01/2021 on examples of personal data breach notification adopted on December 14, 2021, version 2.0 (hereinafter "EDPB Guidelines 01/2021"), and specifically example number 14 (Guidelines 01/2021, case No. 14, p. 31), referring to the situation of "highly confidential personal data sent by mistake by post". In the mentioned case, the social security number, which is the equivalent of the PESEL number used in Poland, was disclosed. In the case in question, the European Data Protection Board (hereinafter "EDPB") had no doubts that the disclosed data in the field of: name and surname, e-mail address, postal address, social security number, indicate a high risk of violating the rights or freedoms of natural persons ("the involvement of their [injured persons] social security number, as well as other, more basic personal data, further increases the risk, which can be described as high"). The EDPB recognizes the importance of national identification numbers (in this case, the PESEL number), while emphasizing that this type of violation of personal data protection, i.e. including data in the form of: name and surname, e-mail address, correspondence address and social security number, requires the implementation of actions, i.e. notification of the supervisory authority and notification of the breach to the data subjects.

The latest infoDOK report (prepared as part of the Social Information Campaign of the RESERVED DOCUMENTS System, organized by the Polish Bank Association and some banks, under the auspices of the Ministry of the Interior and in cooperation with, among others, the Police and the Consumer Federation)[2] shows that that in the second quarter of 2022, 1,806 fraud attempts were recorded (including one for PLN 1.3 million). In turn, in the third quarter of 2022, attempts were made to extort 2,089 loans for a total amount of PLN 47.7 million (including one for PLN 6 million).

In addition, according to the jurisprudence, judgments in cases of fraudulent loans are not uncommon and have been issued by Polish courts in similar cases for a long time - for confirmation, you can even quote the judgment of the District Court in Łęczyca of July 27, 2016 (file reference number I C 566/15), in which fraudsters taking out a loan for someone else's data used a PESEL number, a made-up address and an incorrect ID number (invalid). In the justification of the above of the judgment, the Court stated that: "In the present case, the plaintiff (...) with its registered office in W. purchased a receivable from (...) Spółka z ograniczoną odpowiedzialnością 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 proved 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."

The situation described above largely reflects the example number 17 indicated in the EDPB Guidelines 01/2021, illustrating the case of identity theft. In this case, the situation is as follows: "The contact center of a telecommunications company receives a call from someone who poses as a customer. The alleged customer requests the company to change the email address where billing information should be sent. The contact center employee confirms the customer's identity by requesting certain personal data, in accordance with the procedures used by the company. The caller correctly indicates the fiscal number

and postal address of the requested customer (because he had access to these elements). After approval, the operator makes the requested change, and from that moment on, billing information is sent to the new e-mail address. The procedure does not provide for any notification of the previous e-mail contact. In the following month, the legal customer contacts the company, asking why he is not receiving invoices to his e-mail address, and denies all calls from him demanding that he change his e-mail address. Later, the company realizes that the information was sent to an illegal user and reverses the change."

In the opinion of the EDPB, a breach involves a high level of risk, because billing data may constitute information about the private life of the data subject (e.g. habits, contacts) and may lead to material damage (e.g. stalking, threats to physical integrity), therefore it is necessary is both the notification of the supervisory authority and the notification of the data subject.

Considering the above issues, the position of the Provincial Administrative Court in Warsaw, expressed in the judgment of July 1, 2022, issued in case No. II SA/Wa 4143/21, should also be recalled. 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 a breach of personal data protection, so as to enable them to take the necessary preventive measures" (own emphasis).

As already signaled in the justification for this decision, it should also be borne in mind that the Administrator's performance of his obligation under Art. 34 sec. 1 of Regulation 2016/679 cannot be made conditional on the occurrence of a violation of the rights or freedoms of natural persons whose data is affected by the violation of personal data protection. It should be noted for the sake of order that it is similar in the case of the obligation under Art. 33 sec. 1 of Regulation 2016/679 - as stated by the Provincial Administrative Court in Warsaw in the judgment of September 22, 2021 issued in the case with reference number 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"

(however, this Court ruled similarly in the previously cited judgment of July 1, 2022, issued in case No. II SA/Wa 4143/21, and in the judgment of January 21, 2022, issued in case No. .: II SA/Wa 1353/21).

When analyzing the above, one should also not forget about the basic rules. 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 - including in situations where the protection of personal data has been breached - these values should be taken into account in the first place.

It is worth emphasizing in particular that when assessing the risk of infringement of the rights or freedoms of natural persons, which is the condition for reporting a personal data breach and notifying the data subject of a breach, the probability factor and the severity of potential negative effects should be taken into account. A high level of any of these factors affects the level of the overall rating, which determines the fulfillment of the obligations set out in Art. 33 sec. 1 and art. 34 sec. 1 of Regulation 2016/679. Bearing in mind that due to the scope of the disclosed personal data in the analyzed case, there was a possibility of materializing significant negative consequences for the data subject (as shown above), the importance of the potential impact on the rights or freedoms of a natural person should be considered high. At the same time, the probability of high risk arising as a result of the breach in question is not small and has not been eliminated. Thus, it should be stated that in connection with the breach in question, there was a high risk of violating the rights or freedoms of data subjects, which consequently determines the obligation to notify the breach of personal data protection to the supervisory authority and notify the Data Subject of the breach. The Article 29 Working Party in the WP250 Guidelines indicates 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." It should also be taken into account that in connection with the occurrence of a breach of personal data protection, there were no factors reducing the probability of negative effects, such as limited identification, a statement that personal data is publicly available (see: explanations of the Housing Cooperative of [. ..] of October 2021), or recognition of the wrong recipient as a "trusted" person.

Summarizing the above, it should be stated that in the case in question there is a high risk of violating the rights or freedoms of the person affected by the violation, which in turn results in the obligation of the Housing Cooperative to notify the personal data breach to the supervisory authority, in accordance with Art. 33 sec. 1 Regulation 2016/679, which must contain the information specified in art. 33 sec. 3 of Regulation 2016/679 and notifying that person of a breach, in accordance with Art. 34 sec. 1 Regulation 2016/679, which must contain the information specified in art. 34 sec. 2 of Regulation 2016/679.

Then, addressing the explanations of the Housing Cooperative, first of all, it should be pointed out that in connection with the violation of personal data protection in question, consisting in providing an unauthorized entity with a document containing personal data of a member of the Housing Cooperative, it is not important whether that person actually committed the acts referred to referred to in the notification submitted by the Cooperative on suspicion of committing a crime. Even if the allegations raised by the Administrator against this person are confirmed, it does not mean that their personal data should not be subject to the same protection as any other natural person in a similar situation. It does not follow from the later explanations of the Housing Cooperative that the Data Subject himself made available his personal data contained in the notification of suspected crime, so it cannot be assumed that such a circumstance could be taken into account at all when assessing the correctness of the Administrator's conduct.

In the case in question, the Data Subject's personal data was disclosed to a person professionally related to the news media, hence the Administrator, when submitting explanations, pointed in particular to the content of art. 4, 11 and 12 of the Act of January 26, 1984. Press Law (Journal of Laws of 2018, item 1914), hereinafter referred to as the "Press Law". It follows from these provisions (to the extent that they would apply to the analyzed case at all) that entrepreneurs and entities not included in the public finance sector and not operating for profit are obliged to provide the press with information about their activities, unless, under separate regulations, the information is not is secret or does not violate the right to privacy (Article 4(1) of the Press Law). The journalist is entitled to obtain information in the scope referred to in Art. 4 of the Press Law, and information on behalf of organizational units shall be provided by the heads of these units, their deputies, spokespersons or other authorized persons, within the limits of the duties entrusted to them in this regard (Article 11(1) and (2) of the Press Law). In addition, a journalist is obliged to exercise particular diligence and reliability when collecting and using press materials, in particular to check the truthfulness of the information obtained or to indicate its source, as well as to protect personal rights, as well as the interests of informants acting in good faith and other persons who place their trust in him (Article 12(1)(1) and (2) of

the Press Law). In the analyzed case, however, it is important that the third party to whom the said data of the member of the Housing Cooperative was made available did not request access to it at all, which it clearly indicated in the information addressed to the supervisory authority of [...] August 2021. As indicated judicature (M. Brzozowska-Pasieka [in:] M. Olszyński, J. Pasieka, M. Brzozowska-Pasieka, Press law. Practical commentary, Warsaw 2013, art. 4): »The press law does not define or introduce specific regulations regarding a journalist's request for press information. However, it indirectly points to some elements of such a conclusion. (…) The request should be specific enough to specify the scope or subject of the requested information. It must also be precise so that it can be considered at all. (...) In one of the judicates, the court stated that the application must be detailed enough for the entity obliged to provide information to determine what specific information is of interest to the applicant - the press, i.e. what "segment" of the business activity of the entrepreneur and the failed entity to the public finance sector, the press wants information. In other words, a request for press release is a request for access to facts, i.e. to what happened in the activity or in connection with the activity of the entity obliged to provide information. Otherwise, the entity obliged to provide information could not comply with the provisions of Art. 4 of the Act - Press Law (decision of the Provincial Administrative Court in Warsaw of October 30, 2008, II SA/Wa 1885/2007, LexisNexis No. 2357813)". In this case, no such request was submitted by a third party, so the Administrator's action in the field of providing her with personal data of a member of a Housing Cooperative can be considered at least "excessive". Moreover, this disclosure was made in violation of the Administrator's obligation to protect this data.

In view of the above, it should be stated that in the situation in question, there are no grounds to conclude that the Administrator, for any reason, is released from the obligation to report a breach of personal data protection to the supervisory authority in accordance with art. 33 sec. 1 of Regulation 2016/679 and the obligation to notify the person to whom the data covered by this breach relates to it (in accordance with Article 34(1) of this regulation). In the circumstances of the case under review, it cannot be reasonably claimed that it is unlikely that this breach will result in a risk of violating the rights or freedoms of the Data Subject. This infringement concerned the name, surname, PESEL registration number and address of residence of the above-mentioned persons. persons contained in the specific document, and also from the letter of the Housing Cooperative dated [...] September 2021, it appears that the notification containing this data on suspicion of committing a crime by the Data Subject has been made available to more than one person. In the opinion of the supervisory authority, there is therefore no justification for the Housing Cooperative's failure to perform its obligations under the above provisions.

Finally, referring to the Administrator's obligation specified in art. 34 sec. 2 of Regulation 2016/679, the President of the UODO stated that the Administrator (taking into account the nature of the breach and the categories of data that was breached) should indicate to the data subject the most likely negative consequences of the breach of their personal data. Certainly, in the event of a breach of such data as name, surname and PESEL registration number, it is necessary to indicate, first of all, the possible theft or falsification of identity by third parties obtaining, to the detriment of the person whose data was breached, loans from non-bank institutions or fraudulent insurance or insurance funds, which may result in negative consequences related to an attempt to attribute responsibility to the data subject for such fraud. The description of the possible consequences should reflect the risk of violating the rights or freedoms of that person, so as to enable him to take the necessary preventive measures.

At this point, it should be noted that pursuant to 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.

Summarizing the above argumentation of the supervisory authority comprehensively, it should be stated that the Administrator - despite updating himself in the circumstances of the analyzed case of his duties - 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 subject without undue delay of a breach of the protection of his data, in accordance with art. 34 sec. 1 of Regulation 2016/679, which means a violation of these provisions by the Cooperative.

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 Cooperative based on Art. 83 sec. 4 lit. a) of Regulation 2016/679, which states, among others, 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.

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 Housing Cooperative, 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 imposed administrative fine:

1. 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 this case, a violation of the provision of Art. 33 sec. 1 of Regulation 2016/679 (consisting in failure to notify the President of the Office for Personal Data Protection of a breach of personal data protection without undue delay, no later than within 72 hours after finding the breach) and art. 34 sec. 1 of the Regulation 2016/679 (consisting in not notifying a personal data breach without undue delay to the data subject). They are related to the event consisting in the disclosure of a document (notice of suspected crime) containing personal data of a member of a Housing Cooperative in the form of: PESEL number with name and surname and address of residence, which makes it of considerable importance and serious nature, because the event this may lead to material or non-material damage to the person whose data has been breached, and the probability of their occurrence is high. It is true that in the present case the breach of personal data protection concerned only one person, but the President of the UODO considers the long duration of the breach of Regulation 2016/679 by the Housing Cooperative to be an aggravating circumstance. Several months have passed since the Administrator became aware of the breach until the date of this decision, during which the risk of violating the rights or freedoms of the person affected by the breach could materialize, and which the person could not prevent due to the failure of the Cooperative to notify the breach of protection personal data to the President of the UODO and the obligation to notify the data subject about it.

2. 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 cooperative made a conscious decision not to notify the President of the UODO or the data subject of the breach. There is no doubt that the Cooperative, when processing

personal data on a massive scale, must have knowledge in the field of personal data protection, including knowledge of the consequences of finding a breach of personal data protection resulting in a high risk of violating the rights or freedoms of natural persons (and this knowledge may be required not only from administrator, but also from the data protection officer appointed by him). Being aware of this, the Administrator decided, however, to resign from reporting the infringement to the President of the UODO and notifying the data subject, despite the fact that the President of the UODO first informed the Housing Cooperative 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 subject of the breach should raise at least doubts about the Administrator's position.

3. 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 Personal Data Protection Office found the cooperation with the Housing Cooperative to be unsatisfactory. 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 the data subject 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 person affected by the infringement) were not taken by the Housing Cooperative even after the President of the UODO initiated administrative proceedings in the case.

4. Categories of personal data affected by the breach (Article 83(2)(g) of Regulation 2016/679); Personal data made available to an unauthorized person do not belong to the special categories of personal data referred to in Art. 9 of Regulation 2016/679, however, the fact that the document made available (notification of suspected crime) contains a wide range of them (name and surname, address of residence, PESEL registration number), 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 clearly identifies a natural person in a way that allows the negative effects of the violation (e.g. identity theft, loan extortion) to be assigned to that particular person.

When determining the amount of the administrative fine, the President of the UODO found no grounds to take into account mitigating circumstances affecting the final fine. All the conditions listed in art. 83 sec. 2 lit. a -j of Regulation 2016/679, in the opinion of the supervisory authority, constitute either aggravating or only neutral premises. Also applying the premise mentioned in art. 83 sec. 2 lit. k of Regulation 2016/679 (ordering to take into account any other aggravating or mitigating factors applicable to the circumstances of the case), no mitigating circumstances were found, only neutral ones (which was noted below in point 7 regarding financial benefits obtained directly or indirectly in connection with the infringement or avoided losses).

The fact that the President of the UODO applied sanctions in the form of an administrative fine in this case, as well as its amount, had no impact on the other ones 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. The degree of responsibility of the administrator, 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. The manner in which the supervisory authority found out about the infringement (Article 83(2)(h) of Regulation 2016/679); 33 sec. 1 and art. 34 sec. 1 of Regulation 2016/679 related to the event consisting in the Administrator making available a document containing personal data of a member of the Cooperative, the President of the UODO was informed by a third party.

5. Compliance with 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 under 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 Administrator's disadvantage 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 or losses avoided directly or indirectly in connection with the infringement (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.

In the opinion of the President of the UODO, the applied administrative fine fulfills 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 fact that the Housing Cooperative, which processes personal data professionally and on a massive scale, will fulfill its obligations in the field of personal data

protection in the future, in particular in the field of reporting a data protection breach personal data to the President of the UODO and notification of a breach of personal data protection of persons affected by the breach.

In the opinion of the President of the UODO, the administrative fine will fulfill a repressive function, as it will be a response to the violation by the Housing Cooperative 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 point out to both the Housing Cooperative and other data administrators that it is reprehensible to disregard 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, and also eliminate or at least reduce these effects.

Pursuant to the content of art. 103 of the Act of May 10, 2018 on the protection of personal data (Journal of Laws of 2019, item 1781), hereinafter referred to as "uodo", the equivalent of the amounts expressed in euros referred to in art. 83 of Regulation 2016/679, is calculated in PLN according to the average euro exchange rate announced by the National Bank of Poland in the table of exchange rates as at January 28 of each year, and if in a given year the National Bank of Poland does not publish the average euro exchange rate on January 28 - according to the average euro exchange rate announced in the exchange rate table of the National Bank of Poland, which is the closest after that date.

Considering the above, the President of the UODO, pursuant to art. 83 sec. 4 lit. a) in connection with art. 103 of the uodo, for the infringement described in the operative part of this decision, imposed on the Cooperative - using the average euro exchange rate of January 30, 2023 (EUR 1 = PLN 4.7160) - an administrative fine in the amount of PLN 51,876 (equivalent to PLN 11,000 ,- EUR).

In the opinion of the President of the UODO, the fine applied in the amount of PLN 51,876 (in words: fifty-one thousand eight hundred and seventy-six zlotys) meets the conditions referred to in art. 83 sec. 1 of Regulation 2016/679 due to the seriousness of the 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. Referring to the amount of the administrative fine imposed on the Housing Cooperative, the President of the UODO decided that it was proportionate to the Administrator's financial situation and would not constitute an excessive burden for him. The financial statement presented by the Cooperative shows that the net revenues from sales and equated to them in 2021 amounted to PLN (...), therefore the amount of the administrative fine imposed in this case is approximately (...) % of the above. the amount of revenue from the

previous financial year. At the same time, it is worth emphasizing that the amount of the imposed penalty of PLN 51,876 is only 0.11% of the maximum amount of the penalty that the President of the UODO could - applying in accordance with Art. 83 sec. 4 of Regulation 2016/679, a static maximum penalty (i.e. EUR 10,000,000) - impose on the Cooperative for the violations found in this case. When assessing the amount of the fine imposed in this case, the size of the punished entity should also be taken into account, which may also be evidenced by the fact that (according to the data provided on the website of the Housing Cooperative at: (…)) the usable area of the resources of the Housing Cooperative at the end of 2021 amounted to (...) m² in total (with (...) people registered in the flats), and, as of the same day, the Housing Cooperative owned (...) ha of land.

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 authority to the degree of infringement of the administrator's obligations, but on the other hand, it does not cause a situation where the need to pay a financial penalty will have negative consequences, in the form of a significant reduction in employment or a significant decrease in the turnover of the Housing Cooperative. According to the President of the UODO, the Housing Cooperative should and is able to bear the consequences of its negligence in the field of data protection, as evidenced by, for example, the financial report of the Housing Cooperative, sent to the President of the UODO on [...] November 2022.

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 reporting personal data breaches in accordance with Regulation 2016/679 (WP250rev.01), hereinafter referred to as the WP250 Guidelines.

[2] https://www.zbp.pl/raporty-i-publikacje/raporty-cyclic/raport-infodok

Print article

Metadata

Provider:

Inspection and Infringement Department

Produced information:

John Nowak

2023-03-01

Entered the information:

Wioletta Golanska

2023-03-24 12:51:06

Recently modified:

Edith Magziar

2023-04-04 12:25:06