THE CHAIRMAN OF PERSONAL DATA PROTECTION

Warsaw, 09

of December

2020

DECISION

DKN.5131.5.2020

Based on Article. 104 § 1 of the Act of June 14, 1960, Code of Administrative Procedure (Journal of Laws of 2020, item 256, as amended), art. 7 sec. 1 and art. 60, art. 101 and art. 103 of the Act of May 10, 2018 on the Protection of Personal Data (Journal of Laws of 2019, item 1781), as well as Art. 57 sec. 1 lit. a), art. 58 sec. 2 lit. i), art. 83 sec. 1-3 and art. 83 sec. 4 lit. a) in connection with Art. 33 paragraph 1 and art. 34 sec. 1 and 2 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 the protection of data) (Journal of Laws UE L 119 of 04/05/2016, p. 1, as amended), hereinafter also referred to as "Regulation 2016/679", after conducting administrative proceedings regarding the failure to notify the personal data breach to the President of the Office Personal Data Protection and the lack of notification of a breach of personal data protection of persons affected by the breach by TUiR WARTA SA based in W., President of the Personal Data Protection Office,

finding a breach by TUiR WARTA S.A. based in W. regulations:

1.Art. 33 paragraph 1 of Regulation 2016/679, consisting in not reporting the breach of personal data protection to the President of the Personal Data Protection Office without undue delay, no later than within 72 hours after the breach has been found,

2.Art. 34 sec. 1 of Regulation 2016/679, consisting in failure to notify about a breach of personal data protection, without undue delay of data subjects,

imposes on TUiR WARTA S.A. with its seat in W. a fine of PLN 85,588 (say: eighty-five thousand five hundred and eighty-eight zlotys).

Justification

The Personal Data Protection Office, hereinafter also referred to as "UODO", received information on a breach of personal

data protection on [...] May 2020. The breach consisted in sending by e-mail by the insurance agent (P. U. J. K. with its seat in O.), being the processing entity for TUiR WARTA S.A. based in W., hereinafter also referred to as the "Company", an insurance policy containing personal data to an unauthorized addressee, as a result of which there was a breach of confidentiality of two persons in terms of names, surnames, residential or correspondence addresses, PESEL numbers, telephone numbers, e-mail addresses and information regarding the subject of insurance (passenger car), scope of insurance, payment, assignment, as well as additional provisions resulting from the contract. The supervisory body was informed about the breach of personal data protection by an unauthorized addressee who came into possession of documents not intended for him containing the above-mentioned personal data.

In connection with the above, on [...] June 2020, the President of the Personal Data Protection Office, hereinafter also referred to as the "President of the Personal Data Protection Office", pursuant to Art. 58 sec. 1 lit. a) and e) of Regulation 2016/679 of the European Parliament and of the Council and of the EU Council 2016/679 of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95 / 46 / EC (general regulation on data protection) (Journal of Laws UE L 119 of 04/05/2016, p. 1, as amended), hereinafter also referred to as "Regulation 2016/679", asked the Company for clarification whether, in connection with the shipment of electronic correspondence to an unauthorized recipient, an analysis has been made in terms of the risk of violation of the rights and freedoms of natural persons, necessary to assess whether there has been a breach of data protection resulting in the need to notify the President of the Personal Data Protection Office (Article 33 (1) and (3) of Regulation 2016 / 679) and the persons concerned by the infringement (Article 34 (1) and (2) of Regulation 2016/679). In the letter, the President of the Personal Data Protection Office indicated to the Company how to report the violation and called for explanations within 7 days from the date of receipt of the letter.

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

1.the client himself provided an incorrect e-mail address to which the insurance policy document was sent, 2. the unauthorized

recipient turned to the Company, so it can be concluded that he is aware of the regulations and the importance of the information he received.

Based on the above arguments, the Company assumed the lack of a high probability of negative effects for data subjects through unauthorized use of their data and indicated the remedy in the form of sending a request to an unauthorized recipient to permanently delete the message together with a request for feedback confirming its removal.

In connection with the above-mentioned in the letter, due to the risk assessment of violation of the rights and freedoms of data subjects, the President of the Personal Data Protection Office in the letter of [...] August 2020 indicated to the Company that in accordance with Art. 4 point 12 of Regulation 2016/679, a breach of personal data protection is 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". The President of the Personal Data Protection Office also noted that we are dealing with a breach of data protection both when an event occurs as a result of deliberate action and when it is caused by inadvertent action. In connection with the above, the fact that the breach occurred as a result of an error of the client who provided the agent with an incorrect e-mail address cannot affect the assessment of this event and qualifying it as a personal data breach. Its effect is the disclosure of personal data to an unauthorized person, which means that the confidentiality of the data has been breached. Moreover, due to the fact that the indicated breach of data confidentiality concerns PESEL numbers together with names and surnames, residential addresses, telephone numbers and e-mail addresses, it should be considered that it may involve a high risk of violating the rights or freedoms of natural persons. . At the same time, the President of the Personal Data Protection Office again called the Company to perform an analysis in terms of the risk of violation of the rights and freedoms of natural persons necessary to assess whether there has been a breach of data protection resulting in the need to notify the President of the Personal Data Protection Office and the persons affected by the infringement and to send explanations within 7 days from the date of delivery of the letter. .

In its response of [...] September 2020, the Company again indicated that in its opinion, in the case in question, there was no high risk of violating the rights and freedoms of data subjects, because the data was disclosed only to an unauthorized recipient who himself asked the Company with the incident notification, which shows that he is aware of the regulations and the importance of the information he has received. Therefore, in the opinion of the Company, the probability of using this information in an unauthorized manner or causing other damage is low. As proof of the above, the Company presented a

completed risk assessment form and correspondence with the unauthorized recipient, in which he was asked to permanently delete the message.

Due to the lack of notification of the breach of personal data protection to the President of the Personal Data Protection Office and the lack of notification of the breach of personal data protection of persons affected by the breach, on [...] October 2020, the President of the Personal Data Protection Office initiated administrative proceedings against the Company (letter reference: [...]) .

After the initiation of administrative proceedings in this case, on [...] October 2020, the Company notified the President of the Personal Data Protection Office of the breach of personal data protection by sending a form containing a detailed description of the event (administrator's reference number [...]). The form also contained information that on [...] October 2020, the Company notified two data subjects of a breach of personal data protection and the anonymised content of the notification.

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

Art. 33 sec. 1 and 3 of Regulation 2016/679 provide that in the event of a breach of personal data protection, the data controller shall, without undue delay - if possible, no later than 72 hours after finding the breach - report it to the competent supervisory authority pursuant to Art. 55, unless it is unlikely that the breach would result in a risk of violation of the rights or freedoms of natural persons. The notification submitted to the supervisory authority after 72 hours shall be accompanied by an explanation of the reasons for the delay. The notification referred to in para. 1, must at least: a) describe the nature of the personal data breach, including, if possible, the categories and approximate number of data subjects, as well as the categories and approximate number of personal data entries affected by the breach; (b) include the name 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 the breach of personal data protection; (d) describe the measures taken or proposed by the controller to address the personal data breach, including, where appropriate, measures to minimize its possible negative effects.

In turn, Art. 34 sec. 1 of Regulation 2016/679 indicates that in a situation of high risk for the rights and freedoms of natural persons resulting from the breach of personal data protection, the controller is obliged to notify the data subject about the breach without undue delay. Pursuant to Art. 34 sec. 2 of Regulation 2016/679, the correct notification should:

(a) describe the nature of the personal data breach in clear and plain language; (b) contain at least the information and measures referred to in Article 33 paragraph 3 lit. b), c) and d) of Regulation 2016/679, i.e. c) name and surname and contact details of the data protection officer or designation of another contact point from which more information can be obtained; d) description of the possible consequences of a personal data breach; ) 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.

It should be emphasized that the breach of confidentiality of data that occurred in the case in question, in connection with the breach of personal data protection consisting in sending an insurance policy to an unauthorized recipient, in particular data on PESEL numbers along with names and surnames, residential or correspondence addresses, telephone numbers, e-mail addresses and information about the subject of insurance (passenger car), the scope of insurance, payment, assignment, as well as additional provisions resulting from the contract, cause a high risk of violating the rights or freedoms of natural persons. As the Article 29 Working Party points out in the guidelines on reporting personal data breaches in accordance with Regulation 2016/679, hereinafter also referred to as "guidelines": people whose data has been breached. Examples of such damage include discrimination, identity theft or fraud, financial loss and damage to reputation. " There is no doubt that the examples of damage cited in the guidelines may occur in the present case. Another important factor for such an assessment is the possibility of easy identification of persons whose data was affected by the breach, based on the disclosed data. As a consequence, this means that there is a high risk of violating the rights and freedoms of persons covered by the violation in question, which in turn results in the obligation for the Company to report a violation of personal data protection to the supervisory body, in accordance with Art. 33 paragraph 1 of the Regulation 2016/679, which must contain the information specified in art. 33 paragraph 3 of Regulation 2016/679 and notification of these persons about the violation in accordance with art. 34 sec. 1 of the Regulation 2016/679, which must contain the information specified in art. 34 sec. 2 of Regulation 2016/679.

The above assessment is not affected by the fact of asking the wrong recipient to permanently delete the correspondence received. There is no certainty that before these activities the person did not make e.g. a photocopy or did not record the personal data contained in the document in any other way, e.g. by writing them down. Thus, the mere deletion of correspondence does not give any guarantee that the intentions of such a person will not change now or in the future, and the

possible consequences of using such categories of data may be significant for the persons whose data was affected by the breach. The same applies to a possible declaration of destruction of the correspondence received, because the Company cannot actually verify it. The WP29 guidelines state: “Whether a controller knows that personal data is in the hands of persons whose intentions are unknown or who may be malicious may be relevant to the level of potential risk. There may be a breach of data confidentiality consisting in an accidental disclosure of personal data to a third party, as defined in Art. 4 point 10, or to another recipient. This may be the case, for example, if personal data is inadvertently sent to the wrong department of the organization or to a vendor organization whose services are widely used. The administrator may request the recipient to return or securely destroy the data received. In both cases - due to the fact that the controller is in a permanent relationship with these entities and may know their procedures, their history and other relevant details concerning them - the recipient can be considered "trusted". In other words, the controller can trust the recipient enough to be able to reasonably expect that the party will not read or access the data sent by mistake, and that it will follow the instruction to send it back ”. In the present case, however, there are no grounds for recognizing an unauthorized recipient and treating it as a "trusted recipient". Moreover, the Article 29 Working Party clearly states in the guidelines that "in case of any doubts, the controller should report the breach, even if such caution could turn out to be excessive".

It is also irrelevant that in the present case, the breach of personal data protection occurred due to the fact that the Company's clients themselves provided the wrong e-mail address to which the policy was to be sent. The data has been made available to an unauthorized addressee, which means that there has been a security breach leading to unauthorized disclosure of personal data, and the scope of this data determines that there is a high risk of violating the rights and freedoms of natural persons. At the same time, it should be emphasized that the data controller allowing the possibility of using e-mail for communication with the client should be aware of the risks related to, for example, incorrect provision of the e-mail address by the client and in order to minimize them, take appropriate organizational and technical measures, such as verification of the address provided, or the encryption of documents sent in this way. As is clear from the notification of a breach of personal data protection (administrator reference [...]) submitted after the initiation of the administrative procedure, these measures did not function properly, since the data controller in point 9B of the above-mentioned In order to minimize the risk of a recurrence of the breach, he decided to conduct a conversation with the agent and train employees of the agency, which will take into account the need to encrypt electronic correspondence addressed to customers and the need to pay attention to the correctness of the

contact details provided by the customer.

Moreover, the infringement also involves, pursuant to Art. 35 sec. 1 of the Act of 11 September 2015 on insurance and reinsurance activities (Journal of Laws of 2020, item 895, as amended), in violation of insurance secrecy, which clearly raises the seriousness of the breach and justifies its stricter assessment.

In a situation where, as a result of a breach of personal data protection, there is a high risk of violation of the rights and freedoms of natural persons, the controller is obliged to implement all appropriate technical and organizational measures to immediately identify the breach of personal data protection and promptly inform the supervisory authority, and in cases of high risk violation of the rights and freedoms of data subjects as well. The controller should fulfill this obligation as soon as possible. Recital 85 of the preamble to Regulation 2016/679 explains: "In the absence of an adequate and prompt response, a breach of personal data protection may result in physical harm, property or non-material damage to natural persons, such as loss of control over own personal data or limitation of rights, discrimination, theft or falsification of identity, financial loss, unauthorized reversal of pseudonymisation, breach of reputation, breach of confidentiality of personal data protected by professional secrecy or any other significant economic or social damage. Therefore, as soon as it becomes aware of a breach of personal data protection, the controller should notify it to the supervisory authority without undue delay, if practicable, no later than 72 hours after the breach has been discovered, unless the controller can demonstrate in accordance with the accountability principle that it is unlikely to be, that the breach could result in a risk of violation of the rights or freedoms of natural persons. If the notification cannot be made within 72 hours, the notification should be accompanied by an explanation of the reasons for the delay and the information may be provided gradually without further undue delay. '

In turn, recital 86 of the preamble to Regulation 2016/679 explains: "The controller should inform the data subject without undue delay of the breach of personal data protection, if it may result in a high risk of violating the rights or freedoms of that person, so as to enable that person to take necessary preventive actions. Such information should include a description of the nature of the personal data breach and recommendations for the individual concerned to minimize the potential adverse effects. Information should be provided to data subjects as soon as reasonably possible, in close cooperation with the supervisory authority, respecting instructions provided by that authority or other relevant authorities such as law enforcement authorities. (...) ".

Therefore, when deciding to notify the supervisory authority and data subjects of the breach, only after the initiation of

administrative proceedings (despite the fact that the information about the event was sent to it on [...] May 2020 by an unauthorized recipient), it practically deprived them of the person, provided without undue delay, reliable information about the violation and the possibility of counteracting potential damage. Meanwhile, the role of notifying people about a breach of their personal data is primarily to provide data subjects - quick and transparent information about the breach of personal data protection, along with a description of the possible consequences of the breach of personal data protection and the measures they can take to minimize its possible negative effects.

Consequently, it should be stated that the Company notified a personal data breach to the supervisory body after the deadline specified in Art. 33 paragraph 1 of Regulation 2016/679 and did not notify data subjects without undue delay of a breach of their data protection, in accordance with art. 34 sec. 1 of the Regulation 2016/679, which means the Company's breach of these provisions.

Pursuant to Art. 58 sec. 2 lit. i) of Regulation 2016/679, each supervisory authority has the power to apply, in addition to or instead of other remedial measures provided for in Art. 58 sec. 2 of Regulation 2016/679, an administrative fine under Art. 83 of the Regulation 2016/679, depending on the circumstances of the specific case. The President of the Personal Data Protection Office states that in the case under consideration there are premises justifying the imposition of an administrative fine on the Company pursuant to Art. 83 sec. 4 lit. a) of Regulation 2016/679 stating, inter alia, that the breach of the administrator's obligations referred to in art. 33 and 34 of Regulation 2016/679 is subject to an administrative fine of up to EUR 10,000,000, and in the case of an enterprise - up to 2% of its total annual worldwide turnover from the previous financial year, with the higher amount being applicable.

Pursuant to art. 83 sec. 2 of Regulation 2016/679, administrative fines shall be imposed, depending on the circumstances of each individual case, in addition to or instead of the measures referred to in Art. 58 sec. 2 lit. a) - h) and lit. j) Regulation 2016/679. When deciding to impose an administrative fine on the Company, the President of the Personal Data Protection Office - pursuant to Art. 83 sec. 2 lit. a) - k) of Regulation 2016/679 - took into account the following circumstances of the case, which necessitate the application of this type of sanction in the present case and which had an aggravating effect on the amount of the fine imposed:

a) The nature and gravity of the infringement (Article 83 (2) (a) of Regulation 2016/679).

The infringement found in the present case is of considerable gravity and serious nature as it is likely to cause pecuniary or

non-pecuniary damage to the data breached persons and the likelihood of its occurrence is high.

Duration of the infringement (Article 83 (2) (a) of Regulation 2016/679).

The President of the Personal Data Protection Office recognizes the long duration of the infringement as an aggravating circumstance. From the Company becoming aware of a breach of personal data protection ([...] May 2020) to the fulfillment of its obligations referred to in Art. 33 and 34 of Regulation 2016/679, five months have lapsed, during which the risk of violating the rights or freedoms of persons affected by the violation could be realized, and which could not be prevented by these people due to the Company's failure to comply with the obligation to notify them about the violation.

b) Intentional nature of the infringement (Article 83 (2) (b) of Regulation 2016/679).

The company made a conscious decision not to initially notify the President of the Personal Data Protection Office and data subjects about the breach, despite receiving information about the event from an unauthorized recipient and the letters of the President of the Personal Data Protection Office (UODO) addressed to it indicating the possibility of a high risk of violation of rights or freedoms in this case. the persons concerned by the violation. It should be emphasized here that in the past - in the case of infringements similar or similar to the discussed - the Company reported them to the President of the Personal Data Protection Office, so it was aware that it should also fulfill this obligation this time.

c) The degree of responsibility of the administrator, taking into account technical and organizational measures implemented by him pursuant to art. 25 and 32 (Article 83 (2) (d) of Regulation 2016/679).

The breach found was related to the lack of implementation or incorrect implementation by the Company of organizational and technical measures ensuring data security, i.e. verification of e-mail addresses provided by customers or encryption of files containing personal data sent in electronic messages.

d) The degree of cooperation with the supervisory authority in order to remove the breach and mitigate its possible negative effects (Article 83 (2) (f) of Regulation 2016/679).

In the present case, the President of the Personal Data Protection Office found the cooperation with him on the part of the Company unsatisfactory. This assessment concerns the reaction of the Company to the letters of the President of the Personal Data Protection Office indicating the possibility of a high risk of violating the rights or freedoms of the persons affected by the violation in this case. Correct, in the opinion of the President of the Personal Data Protection Office (UODO), the actions (notification of the infringement to the President of the Personal Data Protection Office and notification of the persons affected

by the infringement) were initiated by the Company only as a result of the formal initiation of administrative proceedings by the President of the Personal Data Protection Office in the case.

e) 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 special categories of personal data referred to in art. 9 of Regulation 2016/679, however, their wide scope (names and surnames, addresses of residence or correspondence, PESEL numbers, telephone numbers, e-mail addresses and information on the subject of insurance - a passenger car, scope of insurance, payments, assignment, as well as additional provisions resulting from from the contract), is associated with a high risk of violating the rights and freedoms of natural persons.

f) How the supervisory authority learned about the breach (Article 83 (2) (h) of Regulation 2016/679).

The President of the Personal Data Protection Office (UODO) was not informed about the breach of the protection of personal data being the subject of this case, i.e. disclosure of personal data processed by the Company as the data controller to an unauthorized person, in accordance with the procedure specified in Art. 33 of the Regulation 2016/679. The fact that there is no information about a breach of data protection from the controller obliged to provide such information to the President of the Personal Data Protection Office should be considered as incriminating this controller.

When determining the amount of the administrative fine, the President of the Personal Data Protection Office also took into account the mitigating circumstances affecting the final penalty, i.e .:

a) Number of injured data subjects (Article 83 (2) (a) of Regulation 2016/679).

In the present case, it was established that the breach concerned only the personal data of two persons. Such a number of persons affected by the infringement, especially in view of the fact that the Company - due to the scale and scope of its activities - processes the personal data of a very large number of clients (insured persons and policyholders), should be considered small, which undoubtedly constitutes a mitigating circumstance in the present case. .

b) Actions taken by the controller or processor to minimize the damage suffered by data subjects (Article 83 (2) (c) of Regulation 2016/679).

Even before reporting the violation, the company turned to the wrong recipient with a request to permanently delete the correspondence received. Such activity of the Company deserves recognition and approval, however, it is by no means tantamount to the guarantee of the actual removal of personal data by an unauthorized person and does not exclude possible

negative consequences of their use for data subjects.

The sanctions applied by the President of the Office in the present case, in the form of an administrative fine, as well as its amount, had no influence on other sanctions indicated in Art. 83 sec. 2 of Regulation 2016/679, the circumstances:

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

b) compliance with previously applied measures in the same case, referred to in Art. 58 sec. 2 of Regulation 2016/679 (Article 83 (2) (i) of Regulation 2016/679);

(c) adherence to approved codes of conduct pursuant to Art. 40 of the Regulation 2016/679 or approved certification mechanisms pursuant to Art. 42 of Regulation 2016/679 (Article 83 (2) (j) of Regulation 2016/679);

(d) financial gains or losses avoided, directly or indirectly, from the infringement (Article 83 (2) (k)).

In the opinion of the President of the Personal Data Protection Office, the applied administrative fine under the established circumstances of this case performs the functions referred to in Art. 83 sec. 1 of Regulation 2016/679, i.e. it is effective, proportionate and dissuasive in this individual case.

It should be emphasized that the penalty will be effective if its imposition leads to the fact that the Company, which processes personal data professionally and on a mass scale, will in the future fulfill its obligations in the field of personal data protection, in particular with regard to reporting a breach of personal data protection. To the President of the Personal Data Protection Office and to notify about a breach of personal data protection of persons affected by the breach. The application of an administrative fine in this case is also necessary considering the fact that the Company ignored the fact that we are dealing with a breach of data protection both when an event occurs as a result of deliberate action and when it is caused by inadvertent action.

In the opinion of the President of the Personal Data Protection Office, the administrative fine will fulfill a repressive function, as it will be a response to the Company's breach of the provisions of Regulation 2016/679. It will also fulfill a preventive function; in the opinion of the President of the Personal Data Protection Office, he will indicate to both the Company and other data administrators that the disrespect of the controllers' obligations related to the occurrence of a breach of personal data protection, and aimed at preventing its negative and often painful consequences for the persons affected by the breach, as well as removing these effects or at least a limitation.

Pursuant to art. 103 of the Act of May 10, 2018 on the Protection of Personal Data (Journal of Laws of 2019, item 1781), the equivalent of the amounts expressed in euro, referred to in Art. 83 of the Regulation 2016/679, are calculated in PLN according to the average EUR exchange rate announced by the National Bank of Poland in the exchange rate table on January 28 of each year, and if the National Bank of Poland does not announce the average EUR exchange rate on January 28 in a given year - according to the average euro exchange rate announced in the table of exchange rates of the National Bank of Poland that is closest to that date.

In connection with the above, it should be noted that a fine in the amount of PLN 85 588 (in words: eighty five thousand five hundred eighty eight zlotys), which is the equivalent of EUR 20,000 (average EUR exchange rate from January 28, 2020 - PLN 4.2794), meets the conditions referred to in Art. 83 sec. 1 of Regulation 2016/679 due to the seriousness of the breach found in the context of the basic objective of Regulation 2016/679 - the protection of fundamental rights and freedoms of natural persons, in particular the right to the protection of personal data. Referring to the amount of the administrative fine imposed on the Company, the President of the Office for Personal Data Protection decided that it is proportional to the financial situation of the Company and will not constitute a burden for it.

The amount of the fine has been set at such a level that, on the one hand, it constitutes an adequate reaction of the supervisory body to the degree of violation of the administrator's obligations, on the other hand, it does not result in a situation in which the necessity to pay a financial penalty will entail negative consequences, in the form of a significant reduction in employment or a significant decrease in the Company's turnover. According to the President of the Personal Data Protection Office, the Company should and is able to bear the consequences of its negligence in the field of data protection, as evidenced by, for example, the Company's financial statements for the period from [...] January 2019 to [...] December 2019, sent to the Personal Data Protection Office in on [...] October 2020

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

The decision is final. The party has the right to lodge a complaint against the decision with the Provincial Administrative Court in Warsaw, within 30 days from the date of its delivery, via the President of the Office for Personal Data Protection (address: ul. Stawki 2, 00-193 Warsaw). A proportional fee should be filed against the complaint, in accordance with Art. 231 in connection with Art. 233 of the Act of August 30, 2002, Law on proceedings before administrative courts (Journal of Laws of 2019, item 2325, as amended). A party (natural person, legal person, other organizational unit without legal personality) has

the right to apply for the right to assistance, which includes exemption from court costs and the appointment of an attorney, legal advisor, tax advisor or patent attorney. The right to assistance may be granted at the request of a party submitted prior to the initiation of the proceedings or in the course of the proceedings. The application is free of court fees.

Pursuant to Art. 105 paragraph. 1 of the Act of May 10, 2018 on the Protection of Personal Data (Journal of Laws of 2019, item 1781), the administrative fine must be paid within 14 days from the date of expiry of the deadline for lodging a complaint to the Provincial Administrative Court, or from on the day the ruling of the administrative court becomes legally binding, to the bank account of the Personal Data Protection Office at NBP O / O Warsaw no. 28 1010 1010 0028 8622 3100 0000. Moreover, pursuant to Art. 105 paragraph. 2 above of the Act, the President of the Personal Data Protection Office may, at the justified request of the punished entity, postpone the date of payment of the administrative fine or divide it into installments. In the event of postponing the payment of the administrative fine or dividing it into installments, the President of the Personal Data Protection Office shall charge interest on the unpaid amount on an annual basis, using a reduced rate of default interest, announced pursuant to Art. 56d of the Act of August 29, 1997 - Tax Ordinance (Journal of Laws of 2020, item 1325, as amended), from the day following the date of submitting the application.

Pursuant to Art. 74 of the Act of May 10, 2018 on the Protection of Personal Data (Journal of Laws of 2019, item 1781), the submission of a complaint by a party to the administrative court suspends the execution of the decision on the administrative fine.

2020-12-16