

THE CHAIRMAN OF PERSONAL DATA PROTECTION

Warsaw, on 05

January

2021

DECISION

DKE. 561/11/2020

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 2, art. 60, art. 101, art. 101a and art. 103 of the Act of May 10, 2018 on the Protection of Personal Data (Journal of Laws of 2019, item 1781) and Art. 57 sec. 1 lit. a), art. 83 sec. 1-2 and art. 83 sec. 6 in connection with Art. 58 sec. 2 lit. e) and lit. i) Regulation of the European Parliament and 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 (Journal of Laws UE L 119 of 04/05/2016, p. 1 and Journal of Laws UE L 127 of 23/05/2018, p. 1, as amended), after conducting administrative proceedings initiated ex officio for the imposition of an administrative fine on Ms MZ conducting business activity under the name of K., President of the Office Personal Data Protection, finding that Ms M. Z., who runs a business under the name of K., has failed to comply with the administrative decision of the President of the Personal Data Protection Office of [...] February 2020, (ref. [...]) imposes on Ms M. Z. running a business under the name of K. an administrative fine in the amount of PLN 85 588 (in words: eighty five thousand five hundred eighty eight zlotys).

JUSTIFICATION

The Office for Personal Data Protection received a notification of a personal data breach of [...] July 2019 submitted by MZ MZ running a business under the name K., (hereinafter also referred to as the "Entrepreneur"). unauthorized copying on [...] April 2019 of personal data of one hundred patients from the system ([A]) of the clinic by a former employee in order to use them for marketing their own services. At the same time, it indicated that the infringement concerned the following categories of patients 'personal data: PESEL number, first and last names, parents' names, date of birth, address of residence or stay and telephone number. The entrepreneur resigned from notifying data subjects about the breach of personal data protection, despite the fact that he assessed the risk of violating the rights and freedoms of natural persons as high. In connection with the above, the

President of the Personal Data Protection Office (hereinafter also referred to as the "President of the Personal Data Protection Office"), with a request of [...] August 2019 (reference number [...]), addressed to the Entrepreneur pursuant to Art. 52 sec. 1 of the Act of May 10, 2018 on the Protection of Personal Data (Journal of Laws of 2019, item 1781) and art. 34 sec. 4 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46 / EC (Journal UE L 119 of 04/05/2016, p. 1 and EU Official Journal L 127 of 23/05/2018, p. 2) (hereinafter referred to as "Regulation 2016/679"), called him to immediately notify persons, data subjects, about the breach of the protection of their personal data and providing these persons with recommendations to minimize the potential negative effects of the breach. In this speech, the President of the Personal Data Protection Office also indicated to the Entrepreneur exemplary risks related to this type of breach and exemplary recommendations as to the measures that persons affected by the breach may take to protect themselves against the negative effects of the breach.

Due to the Entrepreneur's lack of reaction to the request of [...] August 2019, the President of the Personal Data Protection Office initiated administrative proceedings for failure to notify data subjects about a breach of the protection of their personal data. By an administrative decision of [...] February 2020 (reference number [...]), the President of the Personal Data Protection Office ordered the Entrepreneur - pursuant to Art. 58 sec. 2 lit. e) Regulation 2016/679 - notification to data subjects - within three days from the date on which the decision becomes final - about a breach of personal data protection in order to provide them with the information required in accordance with art. 34 sec. 2 of the Regulation 2016/679, i.e. .:

- a) description of the nature of the personal data breach;
- b) name and contact details of the personal data protection officer or designation of another contact point from which more information can be obtained;
- c) a description of the possible consequences of a breach of personal data protection;
- (d) a description of the measures taken or proposed by the administrator to remedy the breach, including measures to minimize its possible effects.

The entrepreneur did not file a complaint against the above-mentioned administrative decision with the Provincial Administrative Court, therefore it became final and binding on [...] April 2020.

In order to check whether the obligations imposed by the above decision were performed by the Entrepreneur, the President of

the Personal Data Protection Office initiated the examination procedure with reference number [...].

In a letter of [...] May 2020, he called on the Entrepreneur to provide explanations and a list of persons to whom the information referred to in the decision order had been provided, as well as information on the manner of their transmission and evidence of their transmission (copies of ten sample notifications with confirmation posting them). In this letter, the Entrepreneur was also informed that the finding of non-compliance with the order imposed by the President of the Personal Data Protection Office may result in imposing an administrative fine on him, in accordance with Art. 83 sec. 6 of the Regulation 2016/679. In response to the above request, the Entrepreneur did not send the requested copies of the notifications, but only in a letter received by the Personal Data Protection Office on [...] May 2020, his attorney informed that the quotation "Unfortunately, despite our willingness, we were not able to do so. to create lists, because we do not know which patients' data was collected by the doctor referred to in the notification submitted by K. Currently, more than [...] people are treated in our facilities and it is impossible to notify everyone about the possibility of their personal data breaching".

On [...] June 2020, the President of the Personal Data Protection Office (UODO) sent the Entrepreneur a reminder referred to in Art. 15 § 1 of the Act of June 17, 1966 on enforcement proceedings in administration (Journal of Laws of 2020, item 1427, as amended), containing a call on the Entrepreneur to execute the decision order within 7 days and to document the execution of this the order by presenting evidence in the form of a list of persons who have been notified in connection with a breach of the protection of their personal data, containing information on how the notification was sent, as well as copies of ten selected letters together with confirmation of posting. On the same day, the representative of the Entrepreneur was also informed by phone about the obligation to execute the order of the decision of the President of the Personal Data Protection Office and to present evidence of its execution. In a letter received by the Office for Personal Data Protection on [...] June 2020, the Entrepreneur's attorney presented copies of ten notifications sent by registered mail on [...] June 2020, with the following text: "We would like to inform you that in 2019 there could have been for breach of your personal data (name, surname, telephone number) by one of our doctors (DB). At the same time, we would like to inform you that this person in our clinic is no longer working and that the investigation is pending against him. If you have any questions, please contact the GDPR administrator in our facility: M. K. [...] ". The submitted copies of the notifications did not contain all the information that the Entrepreneur was required to provide by the order of the President of the Personal Data Protection Office, i.e. they did not contain information on the description of the nature of the breach, description of the possible consequences of the breach and description of the

measures applied or proposed by the administrator to remedy the breach - including in order to minimize its possible effects.

Therefore, in a letter of [...] July 2020, the President of the Personal Data Protection Office called on the Entrepreneur to supplement the explanations and provide evidence documenting the implementation of the decision. In response to the repeated summons to provide explanations, the Entrepreneur's attorney explained by e-mail of [...] July 2020 that the quotation "(...) the points you mentioned in the summons were met:

b) If you have any questions, please contact the GDPR administrator in our facility:

M. K. [...]

c) It is impossible to explain this point, in my opinion it is enough to mention what data has been breached.

d) At the same time, we would like to inform you that this person in our clinic is no longer working and that the investigation is pending against him.

Accordingly, I believe that there is no basis for re-sending patient notifications. "

In the opinion of the President of UODO, the explanations submitted by the Entrepreneur's attorney and the evidence presented by him gave the basis for the conclusion that the Entrepreneur did not comply with the order of the administrative decision of the President of the Personal Data Protection Office of [...] February 2020, ref. [...].

In connection with the above, by a letter of [...] September 2020, the President of the Personal Data Protection Office initiated ex officio administrative proceedings with reference number DKE.561.11.2020. [...] on imposing an administrative fine on the Entrepreneur for failure to comply with an order issued by the supervisory authority pursuant to Art. 58 sec. 2 lit. e) in connection with Art. 34 sec. 1 and 2 of Regulation 2016/679. The above letter of the Entrepreneur was, inter alia, requested to present financial data in the form of a financial statement, and in the absence of such a statement, a statement on the turnover and financial result for 2019, in order to determine the basis for the administrative fine. In addition, the letter indicated that if the Entrepreneur presents evidence that the order of the said decision of the President of the Personal Data Protection Office was fully implemented, this circumstance may have a mitigating effect on the amount of the administrative fine imposed in this proceeding or may result in the withdrawal from its imposition.

In response to the letter informing about the initiation of proceedings to impose an administrative fine, the representative of the Entrepreneur, by e-mail of [...] September 2020, undertook to send the quotation "re-notification for patients affected by the violation". In addition, on [...] September 2020, the representative of the Entrepreneur contacted the Office for Personal Data

Protection by phone, asking for a list of previously submitted (by letter of [...] June 2020) of ten notifications to the case with reference number [...]. It was informed that in connection with the proceedings currently pending against the Entrepreneur (reference number DKE.561.11.2020. [...]) concerning the imposition of an administrative fine for non-compliance with the order issued by the President of the Personal Data Protection Office by decision no. [...], is obliged to provide a complete notification of the data subject about the breach of personal data protection and a list of all persons affected by the breach together with confirmation of sending notifications, in order to document the obligation resulting from the decision order. On the occasion of this telephone conversation, an official memo was prepared on [...] September 2020. On [...] September 2020, the Entrepreneur's attorney sent a sample notification to the Office for Personal Data Protection by e-mail, in order to agree its content with the Office and then send it to persons affected by a breach of personal data protection. In connection with the above e-mail, containing a sample notification of a breach of personal data protection, an employee of the Personal Data Protection Office contacted the Entrepreneur's attorney also by e-mail (on [...] September 2020), and then by phone (on [...] October 2020 year) to clarify that the notification is incomplete. The Representative of the Entrepreneur was informed that the notification should indicate the full scope of personal data disclosed as a result of the breach (in line with the notification of [...] July 2019), and should contain a description of the possible consequences of the breach of personal data protection and remedial steps taken by the administrator. Moreover, the representative of the Entrepreneur was instructed that examples of possible consequences and remedial steps were indicated to the Entrepreneur in the content of the decision of [...] February 2020, ref. [...]. During the telephone conversation, the Entrepreneur's attorney undertook to send evidence of the execution of the order contained in the decision by the end of October 2020. In a letter received by the Personal Data Protection Office on [...] November 2020, the Entrepreneur's attorney stated that the quotation: "I inform you that, in accordance with the request sent by the Department of Penalties and Enforcement of the Office for Personal Data Protection, we notified a total of 37 people (victims) . Ultimately, that many people resulted from the analysis of logs and information carried out by our IT department that Mr. D (...) B (...) saw. At the same time, I would like to inform you that these are all victims of this case. "

Thirty-seven items were indicated in the list of persons to whom the Entrepreneur sent notifications about the violation of their personal data attached to the letter, with two items from the list repeated. In addition, the letter was enclosed with: a copy issued by Poczta Polska S.A. for the benefit of the Entrepreneur a VAT invoice No. [...] of [...] October 2020 documenting the purchase of thirty-seven postage stamps with a value of PLN 3.30 each, a copy of the declaration of [...] October 2020, with

the following text: "We confirm the sending of letters by Mr. MK ordinary in the amount of 37 pieces ", with an illegible signature and a stamp that reads" W. [...] * AN * "and a copy of the unaddressed sample notice. In response to the above letter, on [...] November 2020, the President of the Personal Data Protection Office (UODO) sent a request to the Entrepreneur to supplement the evidence, indicating that the submitted explanations and evidence are incomplete and do not provide grounds for stating that the Entrepreneur had materially notified the data subjects, in accordance with the order of the administrative decision of the President of the Personal Data Protection Office of [...] February 2020, file ref. [...]. The entrepreneur was requested to complete the evidence of the execution of the decision order, i.e. to send the correct list of persons to whom the notifications were sent, and copies of all addressed notifications together with the confirmation of sending registered mail or return acknowledgments of receipt - within 7 days from the date of delivery of this letter. In response, the representative of the Entrepreneur in a letter received by the Personal Data Protection Office on [...] December 2020, informed that the quotation "there is no obligation to send registered letters and it is enough to send them by regular mail and confirm their shipment. I carried out this order and confirmed it with an invoice and a written certificate from the postal worker. Moreover, he pointed out that the quotation "the number of notifications is correct - patients' repeats are not accidental, they are the result of the fact that they had been to the appointment twice".

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

Pursuant to Art. 57 sec. 1 of the Regulation 2016/679, without prejudice to other tasks specified under this regulation, each supervisory authority on its territory (including the President of the Personal Data Protection Office on the territory of the Republic of Poland), inter alia, monitors and enforces the application of the Regulation (Article 57 (1) (a)).) and conducts proceedings on its application (Article 57 (1) (h)). The instruments for the implementation of the tasks referred to in Art. 57 sec. 1 of the Regulation 2016/679, there are remedial powers granted to supervisory authorities (including the President of the Personal Data Protection Office) pursuant to art. 58 sec. 2 of Regulation 2016/679, including, in particular, the right to order the controller to notify the data subject of a breach of personal data protection (Article 58 (2) (e)), as well as the right to apply, in addition to or instead of other measures, referred to in Art. 58 sec. 2 of Regulation 2016/679, an administrative fine pursuant to Art. 83 of this regulation (Article 58 (2) (i)).

Pursuant to Art. 83 sec. 6 of Regulation 2016/679, failure to comply with the order issued by the supervisory authority pursuant

to art. 58 sec. 2 is subject to an administrative fine of up to EUR 20,000,000, and for a company - up to 4% of its total annual worldwide turnover from the previous financial year, whichever is higher.

Referring the above-mentioned provisions of Regulation 2016/679 to the facts established in the case, and the facts described above, it should be stated that the Entrepreneur did not comply (or - in accordance with the terminology used by the EU legislator in Article 83 (6) of Regulation 2016/679) - "Does not comply") with the order of the administrative decision of the President of the Personal Data Protection Office of [...] February 2020, file ref. [...].

A legally valid administrative decision of the President of the Personal Data Protection Office of [...] February 2020, file ref. [...], the Entrepreneur was obliged to notify the data subjects - within three days from the date on which the decision becomes final - about the breach of their personal data that took place on [...] April 2019, in order to provide information required in accordance with Art. 34 sec. 2 of the Regulation 2016/679, i.e.

- a) description of the nature of the personal data breach;
- b) name and contact details of the personal data protection officer or designation of another contact point from which more information can be obtained;
- c) a description of the possible consequences of a breach of personal data protection;
- (d) a description of the measures taken or proposed by the administrator to remedy the breach, including measures to minimize its possible effects.

The President of the Personal Data Protection Office indicated in the administrative decision in question that the proper fulfillment of the obligation specified in Art. 34 of Regulation 2016/679 is to provide data subjects - quickly and transparently - with information about a breach of the protection of their personal data, together with a description of the possible consequences of the breach of personal data protection and the measures that they can take to minimize its possible negative effects. In the justification of the decision, the President of the Personal Data Protection Office also stressed that the breach of confidentiality of data in the form of a PESEL number along with names and surnames, parents' names, date of birth, address of residence or stay and a telephone number causes a high risk to the rights and freedoms of data subjects and requires notifying these persons about the violation in order to inform them, inter alia, about the possible negative effects of the violation and the actions (measures) they can take to protect against the negative effects of the violation. The President of the Personal Data Protection Office concluded that by acting in accordance with the law and showing care for the interests of data subjects,

the controller (Entrepreneur) should therefore, without undue delay, provide data subjects with the best possible protection of personal data.

In the opinion of the President of UODO, the Entrepreneur has not proved - neither during the procedure to verify the implementation of the decision of the President of UODO (reference number [...]), or in the course of this procedure concerning the imposition of an administrative fine on the Entrepreneur (reference number DKE.561.11.2020. [...] - execution of the order of the administrative decision addressed to him of [...] February 2020, file ref. [...]).

At the outset, it should be emphasized that, in accordance with art. 5 sec. 2 of Regulation 2016/679, with the accountability principle, the controller is responsible for compliance with the provisions of para. 1 of this provision (including - in accordance with the so-called principle of legality - for the processing of personal data "in accordance with the law") and must be able to demonstrate compliance with them. In the present case, the President of the Personal Data Protection Office (UODO) legally validated by an administrative decision of [...] February 2020, ref. [...] that the Entrepreneur is processing personal data unlawfully, and specifically in accordance with the provisions of art. 34 sec. 1 and 2 of Regulation 2016/679 ordering the administrator - in the event of a breach of personal data protection that may cause a high risk of violation of the rights or freedoms of natural persons - immediately notify the data subjects of this breach (in the form and content specified in section 2) . The application of the accountability principle in this case means that the Entrepreneur is obliged - in particular in the proceedings before the President of the Personal Data Protection Office - to prove the execution of the decision order, which would be equivalent to restoring the processing of personal data by him to the lawful state. Such implications of the accountability principle are confirmed by the doctrine of the personal data protection law, according to which "The statement that the controller should be able to demonstrate compliance with the rules may be read as imposing the burden of proof on the controller with regard to compliance with data processing rules. In the event of a dispute with the data subject or with the supervisory authority, the controller should be able to provide evidence that it complies with the Principles. Such evidence may include, in particular, documents relating to data processing and protection. " (P. Fajgielski [in:] Commentary to Regulation 2016/679 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 Data Protection Regulation) [in :] General Data Protection Regulation Act on Personal Data Protection Comment, Warsaw 2018, Article 5.

<https://sip.lex.pl/#/commentary/587773149/570589/fajgielski-pawel-kom-comment-do-rozporzadzenia>

-no-2016-679-on-protection-of-natural-persons-in ...? cm = URELATIONS).

In the present case - in the opinion of the President of the Personal Data Protection Office - the Entrepreneur did not provide evidence of the fulfillment of the obligation referred to in Art. 34 sec. 1 and 2 of Regulation 2016/679.

Firstly, the Entrepreneur proved (by presenting a copy of the postal mailing book) that on [...] June 2020, notifications of a personal data breach were sent to ten people. In view of the content of these notifications - unquestionably not meeting the requirements of Art. 34 sec. 2 of Regulation 2016/679 - and a small number of them in relation to the number of one hundred persons whose data was violated (or the number of thirty-seven persons indicated by the Entrepreneur - after checking - in the letter received to the Personal Data Protection Office on [...] November 2020), this action can in no way be considered as the execution of the order of the decision of the President of the Personal Data Protection Office.

Secondly, the documents presented by the Entrepreneur as evidence of sending notifications to thirty-seven persons on [...] or [...] October 2020 do not clearly indicate that such notifications were actually addressed to the persons whose data was violated. This is evidenced by the following circumstances:

- a) The VAT invoice No. [...] of [...] October 2020 documents only the purchase of thirty-seven postage stamps and not the performance of the postal service (delivery by post).
- b) There is no certainty that the statement "We confirm posting 37 letters by Mr. M. K." comes from the postal operator (there is no indication of the operator's company or any other indication). Moreover, this declaration is unverifiable and therefore unreliable - due to the illegible signature it is impossible to identify the person making the declaration.
- c) Even if the above statement was confirmed by the fact that the Entrepreneur sent thirty-seven ordinary letters (which, as indicated above, is not the case), it is certainly not possible (even taking into account the invoice documenting the purchase of postage stamps) that they were the notifications referred to in the decision order that they contained content consistent with the example (unaddressed) notification presented by the Entrepreneur, and ultimately - that they were addressed to persons affected by the infringement (listed in the list prepared by the Entrepreneur).

Summarizing the above, it should be stated that there are no grounds to believe that the Entrepreneur has complied with his obligation under Art. 34 (1) and (2) of Regulation 2016/679, the obligation to notify data subjects about a breach of the protection of their personal data, which was the subject of the notification of [...] July 2019, and thus executed the order of the administrative decision of the President of the Personal Data Protection Office of [...] February 2020, file ref. [...]. The status of

non-compliance with the order issued by the President of the Personal Data Protection Office is current as at the date of this decision.

It should be noted here that the breach of the provisions of Regulation 2016/679 being the subject of this proceeding, i.e. non-compliance with the order issued by the President of the Personal Data Protection Office, lasts from [...] March 2020, i.e. from the day following the expiry of the the deadline set in the decision for its execution. It should be emphasized, however, that the state of violation of the provisions of Regulation 2016/679, which was to be removed by the decision order (the state of not informing about the violation of the persons affected by this violation) is much longer; has been running since at least [...] July 2019, when the Entrepreneur reported a breach of personal data protection, so he undoubtedly already had knowledge of it.

The entrepreneur, despite the correct delivery of the decision of the President of the Personal Data Protection Office (UODO), made no attempt to execute the order. He took any action only as a result of the intervention of the President of the Personal Data Protection Office. However, these actions were slow and - as shown above - ineffective, which increased the risk of additional damages on the part of those affected by the infringement. Pursuant to recital 86 of Regulation 2016/679 "Information should be provided to data subjects as soon as reasonably possible, in close cooperation with the supervisory authority, respecting the instructions provided by this authority or other relevant authorities, such as law enforcement authorities. . For example, the need to minimize the imminent risk of harm will require the immediate notification of data subjects, while the implementation of appropriate measures against the same or similar data breaches may justify subsequent notification. '

It should be emphasized that both in the course of the procedure verifying the implementation of the decision of the President of the Personal Data Protection Office (reference number [...]) and in the course of this procedure concerning the imposition of an administrative fine on the Entrepreneur (reference number DKE.561.11.2020. [...]), the employee The Personal Data Protection Office (UODO) provided the Entrepreneur with a number of instructions regarding the execution of the order, in particular regarding the correct formulation of notifications and the form of their transmission to interested persons, as well as the method of documenting these activities before the President of the Personal Data Protection Office, responsible for the enforcement of the orders he issued. In the opinion of the President of the Personal Data Protection Office, the Entrepreneur's failure to comply with these guidelines, or even ignoring them, proves his gross disregard for the obligations related to the

protection of personal data.

Taking into account the above considerations, the President of the Personal Data Protection Office states that in the present case there are premises justifying the imposition on the Entrepreneur - pursuant to Art. 83 sec. 6 of Regulation 2016/679 - an administrative fine in connection with non-compliance with an order issued pursuant to Art. 58 sec. 2 lit. e) Regulation 2016/679. Pursuant to art. 83 sec. 2 of Regulation 2016/679, administrative fines are imposed depending on the circumstances of each individual case. It refers in each case to a number of circumstances listed in points a) to k) of the above-mentioned provision. When deciding to impose an administrative fine on the Entrepreneur and determining its amount, the President of the Personal Data Protection Office (UODO) took into account the following circumstances aggravating the assessment of the infringement:

a) The nature, gravity and duration of the breach, taking into account the nature, scope or purpose of the processing (Article 83 (2) (a) of Regulation 2016/679)

A breach subject to an administrative fine in these proceedings (failure to comply with the order issued by the President of the Personal Data Protection Office pursuant to Article 58 (2) of Regulation 2016/679) violates the system aimed at protecting one of the fundamental rights of a natural person, which is the right to the protection of personal data. or, more broadly, to protect its privacy. An important element of this system, the framework of which is set out in Regulation 2016/679, are supervisory authorities with tasks related to the protection and enforcement of the rights of natural persons in this respect. In order to fulfill these tasks, supervisory authorities have been endowed with a number of corrective powers, including the power to order the controller to notify the data subject of a data breach (Article 58 (2) (e)). Disregard by the Entrepreneur of the order issued against him by the President of the Personal Data Protection Office, which in fact specifies the obligation provided for in the provisions of Regulation 2016/679, means in fact disregarding the provisions on the protection of personal data and the role of the President of the Personal Data Protection Office in the data protection system specified in the provisions of Regulation 2016/679. Such conduct of an Entrepreneur who is an entity professionally and on a large scale processing personal data of patients (including health data, i.e. data subject to special protection under Article 9 of Regulation 2016/679) should be considered of great importance and particularly reprehensible. The significance of the infringement is additionally increased by the fact that the infringement by the Entrepreneur was not a one-off and incidental event; the procedure of the Entrepreneur subject to assessment in these proceedings is of a continuous and long-term nature. It runs from [...] March 2020, that is from

the day following the expiry of the time limit set in the decision for the execution of the order contained in the decision, to the present day. Such a long duration of the violation (extending the violation of the provision of Article 34 of Regulation 2016/679, the removal of which was to be served by the order of the decision, which undoubtedly increases the risk of negative consequences for the persons affected by the violation) is contrary to the ratio legis of the provision of Art. 34 of Regulation 2016/679, assuming that in order to minimize the risk of damage to persons affected by the infringement, the notification of the breach of their personal data should be made as soon as possible - "without undue delay" (Article 34 (1) of Regulation 2016/679). The importance of the violation of this obligation by the administrator was emphasized, inter alia, in WP 253 of the Art. 29 Working Party of 3 October 2017 on the application and determination of administrative fines for the purposes of Regulation 2016/679 (<https://uodo.gov.pl/pl/10/13>), according to which "A controller / processor who has been negligent in not fulfilling the obligation to notify or at least not communicating all the details of the breach as a result of an incorrect assessment of the extent of the breach may, according to the supervisory authority, merit a more severe sanction - in other words, it is unlikely that such breach will be breached. considered minor. "

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

The Article 29 Working Party in the guidelines on the application and setting of administrative fines for the purposes of Regulation 2016/679 adopted on 3 October 2017, referring to the intentional or unintentional nature of the breach, indicated that, in principle, "intention" includes both knowledge and intentional action due to the characteristics of a prohibited act, while "inadvertent" means no intention to cause an infringement, despite the controller or processor's failure to fulfill the legally required duty of care. Intentional violations are more serious than unintentional violations and, consequently, more often involve the imposition of an administrative fine. In the course of the proceedings, the entrepreneur ignored the Office's recommendations as to the correct performance of his obligation, which indicates a deliberate non-compliance with the order. It should be emphasized that at no stage of the proceedings the Entrepreneur did not provide complete evidence of the execution of the order of the above-mentioned decisions.

c) Unsatisfactory level of cooperation with the supervisory authority to remove the breach and mitigate its possible negative effects (Article 83 (2) (f) of Regulation 2016/679)

When assessing the cooperation of the Entrepreneur with the President of the Personal Data Protection Office in the course of the entire case initiated by his notification of a breach of personal data protection on [...] July 2019, it should be stated that

even before the breach occurs, that is before the date of [...] March 2020 (the date of expiry of the deadline for the execution of the order of the decision of the President of the Personal Data Protection Office of February 26, 2020, ref. [...]) and the very decision of the President of the Personal Data Protection Office of [...] February 2020. Despite the correct delivery of both documents to the Entrepreneur, he did not take any actions to execute them. Only after the President of the Personal Data Protection Office (UODO) initiated the procedure to verify the implementation of the decision (reference number [...]), as well as during the course of this proceeding concerning the imposition of an administrative fine on him (reference number DKE.561.11.2020. [...]), the Entrepreneur made correspondence with the President of the Personal Data Protection Office and took certain steps to execute the order. However, as demonstrated above, these efforts have been slow and ineffective; have not ended - despite the appropriate instructions provided to the representative of the Entrepreneur by an employee of the Personal Data Protection Office in writing, by e-mail and by phone - with the Entrepreneur's performance of the obligation referred to in art. 34 of the Regulation 2016/679, and proving this fact to the President of the Personal Data Protection Office. The other conditions for the assessment of an administrative fine specified in Art. 83 sec. 2 of the Regulation 2016/679 did not affect (aggravating or mitigating) the assessment of the infringement made by the President of the Personal Data Protection Office (including: the degree of the controller's responsibility taking into account the implemented technical and organizational measures, any relevant prior infringements by the controller, categories of personal data affected by the infringement) , the manner in which the supervisory authority learned about the breach, compliance with the measures applied in the same case, referred to in Article 58 (2) of Regulation 2016/679, the use of approved codes of conduct or approved certification mechanisms, achieved in relation to the breach, financial benefits or avoided losses).

Pursuant to the wording of art. 83 sec. 1 of Regulation 2016/679, the administrative fine imposed by the supervisory authority should be effective, proportionate and dissuasive in each individual case. In the opinion of the President of the Personal Data Protection Office, the penalty imposed on the Entrepreneur in these proceedings meets these criteria. The severity of the penalty will discipline the Entrepreneur to comply with the orders of the decision and to properly cooperate with the President of the Personal Data Protection Office in any other future proceedings with the Entrepreneur's participation. The penalty imposed by this decision is - in the opinion of the President of the Personal Data Protection Office - proportional to the seriousness and blameworthy nature of the violation found. Moreover, this penalty will have a deterrent function; it will be a clear signal for both the Entrepreneur and other addressees of the decision of the President of the Personal Data Protection

Office that failure to comply with the order issued by him constitutes a separate (independent of the violation, the removal of which was the basis of the order) violation, and this violation of considerable importance. As such, it will therefore be subject to financial sanctions. It should be pointed out here that, in the opinion of the President of the Personal Data Protection Office, imposing an administrative fine on the Entrepreneur is a measure that will ensure compliance with the order issued against him by a decision of [...] February 2020, ref. [...].

In view of the failure by the Entrepreneur to present the financial data requested by the President of the Personal Data Protection Office for 2019, when determining the amount of the administrative fine in this case, the estimated size of the Entrepreneur's enterprise as well as the specificity, scope and scale of its activity were taken into account. In the course of the proceedings, it was found that the Entrepreneur conducts business activity on a large scale in the service sector that undoubtedly generates large revenues and profits, i.e. in health care. The information presented on the Entrepreneur's website ([...]) shows that he runs at least three medical facilities: D., K. and K. The large scale of the Entrepreneur's activity was confirmed by the Entrepreneur's representative himself in a letter that was received by the Office for Personal Data Protection on [...] May 2020, in which he said: "Currently, more than [...] people are treated in our facilities." In view of the above, it should be stated that the administrative fine imposed in this decision will not be associated with excessive detriment to the business conducted by the Entrepreneur.

Pursuant to the wording of Art. 103 of the Act of 10 May 2018 on the Protection of Personal Data (Journal of Laws of 2019, item 1781), the equivalent of the amounts expressed in euro, referred to in Art. 83 of Regulation 2016/679, are calculated in PLN at the average EUR exchange rate announced by the National Bank of Poland in the exchange rate table as of January 28 of each year, and if the National Bank of Poland does not announce the average EUR exchange rate on January 28 in a given year - according to the average euro exchange rate announced in the table of exchange rates of the National Bank of Poland that is closest to that date. In the present case, the applicable rate is PLN 4.2794 for EUR 1 in force on January 28, 2020. The administrative fine imposed in this decision in the amount of PLN 85 588 is therefore the equivalent of EUR 20,000. Considering the above, the President of the Personal Data Protection Office adjudicated as in the conclusion of this decision. 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 Personal Data Protection Office (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). 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.

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 the date 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 of the above-mentioned Act, the President of the Personal Data Protection Office may, at a justified request of the punished entity, postpone the 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 UODO shall charge interest on the unpaid amount on an annual basis, using a reduced rate of interest for late payment, announced pursuant to Art. 56d of the Act of August 29, 1997 - Tax Ordinance (Journal of Laws of 2019, item 900, as amended), from the day following the date of submitting the application.

2021-01-25