THE CHAIRMAN OF PERSONAL DATA PROTECTION

Warsaw, on 30

June

2021

DECISION

DKN.5131.11.2020

Based on Article. 104 § 1 of the Act of June 14, 1960, Code of Administrative Procedure (Journal of Laws of 2021, item 735), art. 7 sec. 1 and art. 60, art. 101, art. 101a paragraph. 2 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 lit. i), art. 83 sec. 1-2 and art. 83 sec. 4 lit. a) in connection with Art. 33 paragraph 1 and art. 34 sec. 1, 2 and 4 of Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46 / EC (general regulation on data protection) (Journal of Laws UE L 119 of 04/05/2016, p. 1, Official Journal of the European Union L 127 of 23/05/2018, p. 2 and EU Official Journal L 74 of 04/03/2021, p. 35), hereinafter referred to as "Regulation 2016/679", after conducting an ex officio administrative procedure for failure to notify the personal data breach to the President of the Personal Data Protection Office and no notification of the breach of personal data protection of the persons affected by the breach by the Promotion Foundation Mediacji i Edukacji Prawnej Lex Nostra with its registered office in Warsaw at ul. Sienna 45 lok. 5, the President of the Personal Data Protection Office,

1) finding a breach by the Lex Nostra Foundation for the Promotion of Mediation and Legal Education with its seat in Warsaw at ul. Sienna 45 lok. 5 of Art. 33 paragraph 1 of Regulation 2016/679, consisting in not reporting to the President of the Personal Data Protection Office the breach of personal data protection without undue delay, no later than 72 hours after the breach has been found, and the provision of Art. 34 sec. 1 of Regulation 2016/679, consisting in not notifying about a breach of personal data protection, without undue delay of data subjects, is imposed on the Foundation for the Promotion of Mediation and Legal Education Lex Nostra with its registered office in Warsaw at ul. Sienna 45 lok. 5 an administrative fine in the amount of PLN 13,644 (say: thirteen thousand six hundred and forty four zlotys).

2) orders the Lex Nostra Foundation for the Promotion of Mediation and Legal Education with its seat in Warsaw at ul. Sienna

45 lok. 5, notification of data subjects about the personal data breach that occurred on [...] January 2020, in order to provide them with the information required in accordance with Art. 34 sec. 2 of Regulation 2016/679, i.e. a) description of the nature of the personal data breach; b) name and contact details of the data protection officer or designation of another contact point from which more information can be obtained; c) description of the possible consequences of the data breach d) description of the measures taken or proposed by the administrator to remedy the breach - including measures to minimize its possible negative effects, within 3 days from the date of notification of this decision,

Justification

Foundation for the Promotion of Mediation and Legal Education LEX NOSTRA with headquarters in Warsaw, ul. Sienna 45 lok. 5 (hereinafter referred to as the "Foundation"), is a public benefit organization whose statutory objectives include, among others: providing legal aid as well as legal and psychological advice, assistance to victims of crime and their families, activities to protect the rights of victims by public institutions, public health care system and entities operating in the insurance industry, as well as promoting mediation in the broadly understood legal and economic transactions and social life. The Foundation carries out its statutory goals by providing natural persons with free legal assistance and by directing interventions on their behalf and in their interest to the relevant bodies and public institutions. In this regard, the Foundation processes the personal data of people to whom it provides such assistance.

The Office for Personal Data Protection, hereinafter also referred to as "UODO", on [...] October 2020 received a "notification of suspected violation of the principles of compliance with the provisions on the protection of personal data" by the LEX NOSTRA Foundation for the Promotion of Mediation and Legal Education with its seat in Warsaw, ul. Sienna 45 lok. 5 (hereinafter: the Foundation), consisting in the quotation: "(...) loss of personal data of many people, which took place on [...] January 2020, as a result of the theft of files containing the personal data of the beneficiaries (...)" in Mazowieckie a field office in [...]. As is clear from the notification, the theft was the subject of the quotation: "(...) criminal proceedings conducted by the District Prosecutor's Office in [...], reference number [...], however, the analysis of the submitted decision to discontinue the investigation shows that it was only conducted in the context of an attempt to commit an offense under Art. 279 of the Penal Code, and not the loss of documents containing personal data. ". Therefore, there was a concern as to whether the Foundation properly secured the documents against their loss and administered the personal data contained therein in accordance with the requirements of Regulation 2016/679. The supervisory authority was informed by letter no. [...] of [...] October 2020

(presentation date: [...] October 2020) by the Ministry of Justice, which is the body supervising the Foundation.

In connection with the above, on [...] November 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, asked the Foundation to indicate whether, due to the loss of personal data of many persons as a result of the theft of files containing personal data of the beneficiaries, the breach was reported to the supervisory authority, and in the case of a negative answer, asked to send the analysis of the breach in question, as well as information on whether a data protection officer has been appointed, and if so, whether the controller has consulted the data protection officer, the possibility of reporting the breach to the supervisory authority.

In the letter, the President of the Personal Data Protection Office called the Foundation to submit explanations within 7 days of receiving the letter.

In response to the above, the Foundation in a letter of [...] November 2020 stated that it did not notify the supervisory authority of the breach and that it did not have a data protection officer appointed in its organization. In addition, the Foundation indicated that the analysis of the infringement had assessed its seriousness at a low level. On its basis, the Foundation concluded that there was no breach resulting in the need to notify the President of the Personal Data Protection Office.

In connection with the above-mentioned in a letter, due to the risk assessment of violation of the rights and freedoms of data subjects contained therein, the President of the Personal Data Protection Office in a letter of [...] November 2020 called the Foundation to indicate the number of persons affected by the violation of personal data protection and the categories of personal data included in the lost documentation with their specification. He also called for clarification whether special categories of personal data referred to in art. 9 sec. 1 of Regulation 2016/679, as well as personal data related to convictions and violations of the law, as referred to in art. 10 of Regulation 2016/679, as well as how the stolen documentation containing personal data was secured against unauthorized persons and whether the lost documentation was restored and when, and if not, why and what is the planned date of its recovery.

In response of [...] December 2020, the Foundation informed that the violation concerned 96 people, the lost documentation contained the following categories of citation data: "(...) name, surname, correspondence address, telephone number and probably PESEL identification number, nevertheless only 3-4 people whose personal data has been lost have Polish citizenship, and the remaining people do not have Polish citizenship, and thus do not have a PESEL number ", special

categories of personal data were not processed, and the premises where the documentation was located had proper security in the form of: double entry to the premises with certified locks, rooms in the premises have lockable doors (except the secretariat), monitoring and alarm operated by a professional security company are installed, there are strongboxes and lockable cabinets in the premises. Regarding the reconstruction of the lost documentation, the Foundation stated that the quotation: "(...) due to the fact that the cases were closed, the lost documentation could not be restored."

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 [...] December 2020, the President of the Personal Data Protection Office initiated administrative proceedings against the Foundation (letter reference: [...]) and called for additional information on where exactly the files with personal data were located, whether in the event of failure to secure the documentation in accordance with the rules adopted in the organization, the persons responsible for the violation were identified, whether a security policy was developed and implemented, and if so, how the administrator monitors compliance with these rules by employees, whether on the day of the theft of documents containing personal data, the security measures were operational / operational, used for their intended purpose (entrance doors and other rooms locked), activated (monitoring, alarm), what regulations regulate the period storage l or lack thereof, personal files of persons who benefited from the Foundation's help, possibly what were the criteria for the storage period of personal data set by the administrator, what citizenship were held by people who did not have a PESEL identification number, whose data was lost and a request was made to send an analysis of the violation taking into account all criteria taken into account by the controller in the final assessment of the violation of the rights and freedoms of natural persons.

After the initiation of administrative proceedings in this case, together with a request for additional information, in a letter of [...] January 2021, the Foundation explained that the documents containing personal data were in the premises locked with an approved lock, monitored, with an alarm turned on, which was supervised by a professional security company, some of the folders were hidden in lockers and in a safe, and some of the folders were not hidden due to the quotation: "(...) that these were documents on which the current affairs were being worked on by the Foundation (...) ", After the incident, the administrator conducted disciplinary interviews with employees, has a developed and implemented security policy, quotation:" The administrator and the employer supervise employees with regard to their compliance with employee obligations, including compliance with the security policy. After the implementation of the safety procedure, training was organized to familiarize

employees with the practical aspects of applying the above-mentioned policy, and refresher training was also planned. The Foundation uses, inter alia, the principle of two pairs of eyes - internal control outgoing correspondence, which serves to verify the external transfer of personal data to an entity not authorized to receive them, the principle of loss of access to personal data for former employees, the principle of random checks - verification of data collection by the employee, in terms of validity, period and amount of data. It should be noted that employees are aware that acting against the regulations will be sanctioned; " able to verify it, the monitoring was started and functioning properly, the alarm system, due to technical problems related to the remote control for its activation, probably not armed, we explain that after theft with burglary, technical problems with the remote control for arming the alarm system were verified with the security agency and eliminated ", quotation:" the criteria for storing data have been standardized in the Register of Processing Activities ("RCP"), it contains an entry that the data will be stored for a period resulting from legal provisions, e.g. in relation to the archiving of tax documents, the period of storage Personal Data is 5 years from the end of the calendar year o, on which the tax payment deadline related to the contract has expired; in relation to the archiving of paper documents related to providing assistance, the time of their storage determines the time of the Foundation's assistance (the criterion is therefore the end of providing assistance in an individual case, most often it is the construction of letters - requests for payment, lawsuits) or withdrawal of consent to processing . The Foundation explained that the data storage period is limited to the minimum, and it is determined by the fulfillment of the goal of ending legal / psychological assistance; ", quoted:" The Foundation is not able to precisely determine the citizenship of people without a PESEL number, whose data has been lost, however, they will be persons from […], […], […], […] and […]; ". A copy of the infringement analysis was attached to the letter of […] January 2021. The Foundation assessed the seriousness of a personal data breach according to the Personal Data Breach Severity Calculator, taking into account the recommendations contained in the publication of the European Union Agency for Network and Information Security (ENISA). The assessment of the severity, according to the Personal Data Protection Breach Severity Calculator, allowed the controller to determine the level of severity of the data protection breach for data subjects as low and to accept no obligation to report the breach to the supervisory authority and notify persons about the breach of data protection.

Until the date of this decision, the Foundation has not recovered the personal data lost as a result of the infringement being the subject of these proceedings.

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

following:

Pursuant to Art. 4 point 12 of Regulation 2016/679, a breach of personal data protection means a breach of security leading to accidental or unlawful destruction, loss, modification, unauthorized disclosure or unauthorized access to personal data transmitted, stored or otherwise processed.

Article 33 of Regulation 2016/679 provides 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 - notify 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 (section 1). 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 (paragraph 3).

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

1) describe the nature of the personal data breach in clear and simple language;

2) contain at least the information and measures referred to in Art. 33 paragraph 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 breach of personal data protection; 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.

The content of the above-mentioned provisions of Regulation 2016/679 shows that in the event of a breach of personal data protection on the part of the data controller, an obligation arises to report it to the President of the Personal Data Protection

Office, if the breach involves a risk of violating the rights or freedoms of natural persons - regardless of the level of this risk. On the other hand, in a situation where the breach of personal data protection causes a high risk of violation of the rights or freedoms of natural persons, the data controller is obliged to notify these persons about the breach of their data protection.

There is no doubt that the event consisting in "(...) loss of personal data of many people, which took place on [...] January 2020, as a result of the theft of files containing the personal data of the beneficiaries (...)" due to the scope of data contained in in the lost documentation, it constitutes a breach of data confidentiality due to the possibility of becoming acquainted with the above-mentioned data by an unauthorized person (s) and a breach of data availability due to the fact that "(...) the lost documentation was not recoverable". Consequently, it should be considered that there was a breach of security leading to accidental loss and unauthorized access to personal data processed by the Foundation, and therefore a breach of personal data protection.

We deal with the risk of violating the rights or freedoms of natural persons when the violation may result in physical, material or non-material damage to the natural persons whose data has been violated. It should be emphasized that the possible consequences of the event that occurred do not have to materialize - in the content of Art. 33 paragraph 1 of Regulation 2016/679, it was indicated that the mere occurrence of a breach of personal data protection, which involves the risk of violating the rights or freedoms of natural persons, implies an obligation to notify the breach to the competent supervisory authority. It is similar in the case of Art. 34 sec. 1 of Regulation 2016/679 - for the obligation to notify the data subject about the violation, it is sufficient that the violation may result in a high risk of violating the rights or freedoms of these persons.

The values that Regulation 2016/679 places particular emphasis on in the field of risk assessment are therefore the rights or freedoms of data subjects and these values should be first of all taken into account when assessing the risk related to the processing of personal data. Pursuant to recital 2 of the preamble to Regulation 2016/679, the principles and provisions on the protection of natural persons with regard to the processing of their personal data may not - irrespective of their citizenship or place of residence - violate their fundamental rights and freedoms, in particular the right to the protection of personal data. . This right is a fundamental right guaranteed by Art. 8 of the Charter of Fundamental Rights and must be respected in the conduct of any data processing operation without exception. When talking about the risk of violating the rights and freedoms of natural persons under Regulation 2016/679, it is necessary to take into account: 1) the probability of a specific infringement event, and 2) the seriousness of the event, i.e. the amount of damage that this event may cause to a person the data subject.

On the other hand, recital 76 of Regulation 2016/679 indicates that the probability and severity of the risk of violation of the rights or freedoms of the data subject should be determined by reference to the nature, scope, context and purposes of data processing. Risks should be assessed on the basis of an objective and factual analysis that determines whether there is a risk or a high risk to data processing operations. It is not without significance for the assessment of the situation that the Foundation is not able to accurately indicate the categories of personal data contained in the lost documentation, which may have contributed to its incorrect assessment of the risk of breach, quotation: "(...) categories of personal data in the lost documentation include name, surname, correspondence address, telephone number and probably PESEL number, but only 3-4 people whose personal data has been lost have Polish citizenship, and the remaining people do not have Polish citizenship, and thus do not have a PESEL number; ". At the same time, it does not appear from the collected evidence that the Foundation undertook any actions to verify the actual scope of personal data contained in the stolen documentation and whether the PESEL number really concerned only 3-4 people. The lack of such verification increases the level of risk of violating the rights or freedoms of these persons. As a result of its conduct, it could turn out that the scope of personal data accessed by an unauthorized person (or persons) is wider than indicated by the Foundation, if only due to the fact that in connection with providing legal / psychological assistance, the Foundation could obtain data necessary for the proper provision of such assistance, other than those mentioned in the explanations provided by it.

In this context, it should be emphasized that the risk analysis presented by the Foundation, constituting an appendix to its explanations, is in fact a printout from the calculator of the seriousness of personal data breaches made available on the website of one of the entities providing support services in the field of personal data protection. The President of the Personal Data Protection Office (UODO) does not assess the correctness of the indicated calculator operation here, but underlines that it is possible to obtain any result with the help of calculators, depending on the data entered for the calculations. In addition, the above-mentioned printouts contain a reservation that "each breach or suspected breach of personal data protection should be analyzed individually, in particular with regard to the obligations set out in Art. 33 and 34 of the GDPR, therefore this calculator can only be used as an additional resource and cannot be used as an independent basis for decision-making by any entity or person that uses the calculator on their own responsibility ". Moreover, these documents do not bear the date of production, nor do they contain a description of the detailed criteria which the Foundation followed when making its assessment with the help of the indicated calculator. The printout presented by the Foundation, in line with the supplier's

reservation contained therein, may therefore only be of an auxiliary nature and may not constitute the basis for assessing the risk of violating the rights or freedoms of natural persons.

It should be emphasized that the breach of data confidentiality that occurred in the case in question, in connection with the breach of personal data protection consisting in the following: "(...) loss of personal data of many people, which took place on [...] January 2020, the result of the theft of files containing the beneficiaries' personal data (...) ", in particular data on PESEL registration numbers together with names and surnames, correspondence addresses, telephone numbers, causes 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 violation of the rights and freedoms of persons affected by the violation in question, which in turn results in the Foundation's obligation 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.

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 not to notify the supervisory authority and the data subjects of the breach, the Foundation practically deprived these persons of the possibility of counteracting potential damage. By notifying the data subject without undue delay, the controller enables the person to take the necessary preventive measures to protect the rights or freedoms against the negative effects of the breach. Art. 34 sec. 1 and 2 of Regulation 2016/679 is intended not only to ensure the most effective protection of the fundamental rights or freedoms of data subjects, but also to implement the principle of transparency, which results from Art. 5 sec. 1 lit. a) of Regulation 2016/679 (cf. Chomiczewski Witold (in :) GDPR. General Data Protection Regulation. Comment. ed. E. Bielak - Jomaa, D. Lubasz, Warsaw 2018). Proper fulfillment of the obligation specified in art. 34 of Regulation 2016/679 is to provide data subjects with quick and transparent information about a breach of the protection of their personal data, together with a description of the possible consequences of the breach of personal data protection and the measures that they can take to minimize its possible negative effects. Acting in accordance with the law and showing concern for the interests of data subjects, the controller should, without undue delay, provide data subjects with the best possible protection of personal data. To achieve this goal, it is necessary to at least indicate the information listed in Art. 34 sec. 2 of Regulation 2016/679, from which the administrator did not fulfill.

As a rule, the controller should notify the data subjects individually about the breach of personal data protection. However, if

the Foundation does not have copies of the stolen documents, it is not able to reproduce them or does not process these data using the IT system, and thus is not able to identify the data subjects, then pursuant to Art. 34 sec. 3 lit. c) of Regulation 2016/679 should notify these persons by issuing a public announcement or applying a similar measure in order to inform data subjects of the breach in an equally effective manner.

Therefore, when deciding not to notify the supervisory authority and the data subjects of the breach, the administrator in practice deprived these persons of reliable information about the breach and the possibility of counteracting potential damage, provided without undue delay.

When applying the provisions of Regulation 2016/679, it should be borne in mind that the purpose of this regulation (expressed in Article 1 (2)) is to protect the fundamental rights and freedoms of natural persons, in particular their right to the protection of personal data, and that the protection of natural persons in connection with the processing of personal data is one of the fundamental rights (first sentence of Recital 1). In case of any doubts, e.g. as to the performance of obligations by administrators - not only in a situation where there has been a breach of personal data protection, but also when developing technical and organizational security measures to prevent them - these values should be taken into account in the first place.

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

Pursuant to Art. 34 sec. 4 of Regulation 2016/679, if the controller has not yet notified the data subject about the breach of personal data protection, the supervisory authority - taking into account the probability that this breach of personal data protection will result in a high risk - may request it or may state that 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 it follows that each supervisory authority has the right to remedy the need for the controller to notify the data subject about a breach of data protection.

Pursuant to Art. 58 sec. 2 lit. i) of Regulation 2016/679, each supervisory authority has the power to apply, in addition to or instead of other remedial measures provided for in Art. 58 sec. 2 of Regulation 2016/679, an administrative fine under Art. 83 of the Regulation 2016/679, depending on the circumstances of the specific case. The President of the Personal Data Protection Office states that in the case under consideration there are circumstances justifying the imposition of an

administrative fine on the Foundation 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 Foundation, 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 significant and serious nature, as it may cause material or non-material damage to the data subjects of the breach, and the probability of their occurrence is high. The high risk of negative consequences for people whose data has been lost by the Foundation, and thus the seriousness of the breach, is confirmed by the circumstances of the event taking place on [...] January 2020, in particular that it was not an accidental event, but a deliberate act of a person or third parties (unknown to the Foundation, the President of the Personal Data Protection Office, or the law enforcement agencies conducting the theft proceedings) acting in a criminal manner and which should be assumed - due to this method of operation - bad will as the motive for this action.

b) Duration of the violation (Article 83 (2) (a) of Regulation 2016/679). Duration of the violation of the provision of Article 34 sec. 1 of the Regulation 2016/679 is, in the opinion of the President of the Personal Data Protection Office, very long. Fifteen months have passed since the Foundation received information about a breach of personal data protection ([...] January 2020) until now (the breach has not been removed), during which the risk of violating the rights or freedoms of persons affected by the breach could be realized, and why these could not be prevented due to the failure by the Foundation to notify them of the infringement. The President of the Personal Data Protection Office also considers the duration of the violation of Art. 33 paragraph 1 of Regulation 2016/679, although the Foundation - in response to three calls to it and twelve months after receiving information about a breach of personal data protection - provided the President of the Personal Data Protection

Office with exhaustive information on the content of the notification referred to in Art. 33 paragraph 3 of Regulation 2016/679, therefore the President of the Personal Data Protection Office states that the breach of Art. 33 paragraph 1 has been removed.

c) Number of data subjects affected (Article 83 (2) (a) of Regulation 2016/679) In the present case, it was established that the infringement concerned the personal data of many persons - due to the theft of files containing the personal data of the beneficiaries - i.e. 96 people who have benefited from legal assistance at the Foundation.

d) Intentional nature of the breach (Article 83 (2) (b) of Regulation 2016/679). The Foundation made a conscious decision not to notify the President of the Personal Data Protection Office and the data subjects about the breach, despite learning about the loss of personal data of many persons as a result of the theft of files containing personal data, disregarding the letters of the President of the Personal Data Protection Office (UODO) addressed to it, indicating the obligations incumbent on the administrator under the above-mentioned Art. 33 paragraph 1 and 3 and article. 34 sec. 1 and 2 of Regulation 2016/679.

e) 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 the present case, the President of the Personal Data Protection Office found the Foundation's cooperation with him unsatisfactory. This assessment concerns the Foundation's response to the letters of the President of the Personal Data Protection Office pointing to the administrator's obligations under Art. 33 and art. 34 of the Regulation 2016/679. As indicated above (with reference to the premiss of Art. 83 (2) (a) - "Duration of the infringement"), the state of breach of Art. 34 sec. 1 was removed, but obtaining from the Foundation information corresponding to the minimum scope of notification specified in Art. 33 paragraph 3 of Regulation 2016/679 required several letters to be sent to it informing about the administrator's obligations and requesting explanations, and at a later stage of the procedure - to supplement and specify the information already provided to the President of the Personal Data Protection Office. On the other hand, in the scope of fulfilling the obligation to notify the data subjects of the breach (i.e. removing the state of violation of the provision of Article 34 (1) of Regulation 2016/679), no actions have been taken by the Foundation so far, despite the formal initiation of administrative proceedings by the President of the Personal Data Protection Office. regarding.

When determining the amount of the administrative fine, the President of the Personal Data Protection Office had no grounds to take into account any mitigating circumstances that could have an impact on the final penalty.

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) 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 assessed in this proceeding (failure to notify the President of the Personal Data Protection Office of the breach of personal data protection and failure to notify about the breach of personal data protection of the data subjects) is not related to the by the administrator of technical and organizational measures; b) relevant previous violations of the provisions of Regulation 2016/679 by the Foundation (Article 83 (2) (e) of Regulation 2016/679) - no relevant previous violations of Regulation 2016/679 were found by the Foundation; c) compliance with previously applied measures in the same case, referred to in Art. 58 sec. 2 of Regulation 2016/679 (Article 83 (2) (i) of Regulation 2016/679) - in this case, the measures referred to in art. 58 sec. 2 of Regulation 2016/679; d) application of approved codes of conduct pursuant to Art. 40 of the Regulation 2016/679 or approved certification mechanisms pursuant to Art. 42 of Regulation 2016/679 (Article 83 (2) (j) of Regulation 2016/679) - the Foundation does not apply approved codes of conduct or approved certification mechanisms referred to in the provisions of Regulation 2016/679; e) achieved directly or indirectly in connection with financial benefits or avoided losses (Article 83 (2) (k)) - as at the date of this decision, the President of the Personal Data Protection Office did not find that by committing a breach of the penalty, the Foundation obtained any financial benefits or avoided any financial losses; f) categories of personal data concerned by the infringement (Article 83 (2) (g) of Regulation 2016/679) - personal data lost as a result of theft of files do not belong to special categories of personal data referred to in art. 9 of Regulation 2016/679, however, the combination of several types of personal data (name, surname, correspondence address, telephone number and possibly the PESEL registration number) is associated with a high risk of violating the rights or freedoms of natural persons. on the violation (Article 83 (2) (h) of Regulation 2016/679) - On the violation of the protection of personal data being the subject of this case, that is: "(...) loss of personal data of many people, which took place on [...] January 2020, as a result of the theft of files containing personal data of the beneficiaries (...) ", processed by the Foundation acting as the administrator of these data, the President of the Personal Data Protection Office was not informed in accordance with the procedure laid down in Art. 33 of the Regulation 2016/679. The notification on this matter was submitted to the President of the Personal Data Protection Office by the Minister of Justice who supervises the activities of the Foundation within his competences.

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 Foundation, 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 necessary, also taking into account the fact that the Foundation 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 Foundation's violation 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 Foundation and other data administrators the reprehensibility of disregarding the obligations of administrators related to the occurrence of a breach of personal data protection, and aimed at preventing its negative and often painful consequences for the persons affected by the breach, as well as removing these effects or at least limiting them.

Pursuant to art. 103 of the Act of May 10, 2018 on the Protection of Personal Data (Journal of Laws of 2019, item 1781), hereinafter referred to as "u.o.d.o.", 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 13,644 (in words: thirteen thousand six hundred and forty-four zlotys), which is the equivalent of EUR 3,000 (average EUR exchange rate from January 28, 2021 - PLN 4.5479), meets in the established circumstances of the case, 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 Foundation, the President of the Personal Data Protection

Office decided that it is proportional to the financial situation of the Foundation 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 breach of the administrator's obligations, and on the other hand, it does not result in a situation in which the necessity to pay a financial penalty will entail negative consequences necessitating a significant reduction of positive from the point of view of view of the social interest of the Foundation's activities. According to the President of the Personal Data Protection Office, the Foundation should and is able to bear the consequences of its negligence in the field of data protection, as evidenced by, for example, the Foundation's financial statements sent to the Personal Data Protection Office on [...] April 2021 for the periods from [...] January 2018 . until [...] December 2018, according to which its revenues from statutory activities amounted to approx. PLN 1 million, and from [...] January 2019 to [...] December 2019, according to which its operating revenues of the Articles of Association amounted to approx. PLN 2.07 million. The financial data presented by the Foundation for the years 2018-2019 (indicating a high dynamics of revenue growth, and thus the development of the Foundation's activities) allow us to assume that in 2020, i.e. in the previous financial year, the Foundation's revenues (mostly based on funds from public sources, therefore stable sources) were not lower than PLN 2 million. Adopting, pursuant to Art. 101a paragraph. 2 uodo, this is the value of the Foundation's revenues as the basis for the size of the administrative fine, the President of the Personal Data Protection Office states that the fine of PLN 13,644 will not constitute an excessive burden for the Foundation, while being an effective and proportional measure and a preventive measure for the future - both towards the Foundation and and other entities with obligations specified in art. 33 paragraph. 1 and art. 34 sec. 1 of Regulation 2016/679.

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

2021-07-19