THE CHAIRMAN OF PERSONAL DATA PROTECTION

Warsaw, on 06

June

2022

DECISION

DKN.5110.12.2021

DECISION

Based on Article. 104 § 1 and art. 105 § 1 of the Act of June 14, 1960, Code of Administrative Procedure (Journal of Laws of 2021, item 735, as amended), art. 7 sec. 1, 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), art. 57 sec. 1 lit. a) and lit. h), art. 58 sec. 2 lit. i), art. 83 sec. 1 and 2 and article. 83 sec. 4 lit. a) in connection with Art. 33 sec. 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), after conducting administrative proceedings initiated ex officio regarding the breach by Esselmann Technika Pojazdowa Sp. z o.o. Sp. k. with headquarters in Poznań at ul. Kartuska 60 (correspondence address: ul. ..., ... J.) provisions on the protection of personal data, President of the Office for Personal Data Protection,

1) finding a breach by Esselmann Technika Pojazdowa Sp. z o.o. Sp. k. with headquarters in Poznań at ul. Kartuska 60 provision of Art. 33 sec. 1 of the Regulation of the European Parliament and of the EU Council 2016/679 of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46 / EC (general regulation on data protection) (Journal of Laws UE L 119 of 4 May 2016, p. 1, as amended), hereinafter referred to as Regulation 2016/679, consisting in failure to notify the President of the Personal Data Protection Office of a breach of personal data protection without undue delay, no later than within 72 hours after finding a violation, it imposes on Esselmann Technika Pojazdowa Sp. z o.o. Sp. k. with headquarters in Poznań at ul. Kartuska 60, an administrative fine in the amount of PLN 15,994 (say: fifteen thousand nine hundred and ninety-four zlotys);

2) discontinues the proceedings as to the remainder.

Justification

The President of the Personal Data Protection Office, hereinafter also referred to as the "President of the Personal Data Protection Office", by letters of [...] March 2021 and [...] April 2021, was notified by the County Police Commander in J. about potential irregularities in Esselmann Technika Pojazdowa Sp. z o.o. Sp. k., hereinafter referred to as the "Company", regarding the processing of personal data of its employees. Doubts in this respect were related in particular to the processing of data in the personal files of employees, including the loss of documents relating to the employees of the Company. In addition, the Poviat Police Commander in J., acting under the authority of the District Prosecutor's Office in J., requested the President of the Personal Data Protection Office to inspect the Company's compliance with the provisions on the protection of personal data.

In connection with the above, by letters of [...] April 2021 (reference number: ...), of [...] June 2021 (reference number: ...) and [...] July 2021 (reference number: ...) President of the Personal Data Protection Office asked the Company to provide explanations in the matter, incl. to indicate:

1) what category of data was in the lost documents constituting part of the personal files of the Company's employees,

2) whether the lost documents constituting part of the personal files of the Company's employees were found, and if not, on what basis the Company concluded that the fact of their loss does not violate the rights or freedoms of data subjects, does not constitute a breach of the protection of personal data of its employees and does not requires notification of the violation to the President of the Personal Data Protection Office pursuant to Art. 33 sec. 1 of Regulation 2016/679,

3) whether the Company, as an employer, obtained from the person responsible for their loss explanations in this regard, and if so, what is their content, and under what circumstances the loss occurred or could have occurred (transfer or transport of files, sharing them, etc.).

In response to the above-mentioned letters, the Company sent letters to the President of the Personal Data Protection Office of [...] May 2021, [...] June 2021 and [...] August 2021, in which it indicated that in the period from [...] January to [...] in March 2020, P. M. (employed under an employment contract during this period) had access to the personal data of the Company's employees. Above the person, being the only person employed in the Company's office at the time of the incident, was instructed to complete, describe and attach documents to employees' personal files. P. M. collected documents for the files from the employees personally. According to the explanations of the Company, in the first week of March 2020, B. Z., a health

and safety inspector employed by (...), who provided services to the Company, stated that P. M. asked her for help in setting up personal files of the Company's employees. Moreover, B. Z. informed the Company that there was no employment certificate in the personal files of the employees. D. R. D. R. was asked by the Company to report the above-mentioned of the document, stated, however, that the document had already been handed over to P. M. P. M. then stated that she had provided the document to B. Z., who denied it.

As explained by the Company, the incident in question was not reported to the President of the Personal Data Protection Office due to the lack of risk of violating the rights or freedoms of the data subject. D. R. did not make any claims to the Company for this reason. Moreover, as indicated by the Company, P. M. is a long-term friend of D. R. and this fact, in the opinion of the Company, contributed to the fact that he did not make any claims against the Company for breach of the protection of his personal data.

Then, in a letter of [...] September 2021 (ref. No .: ...), the President of the Personal Data Protection Office again asked the Company for clarification, and in particular, to indicate whether the lost document (work certificate) constituting part of the personal files of the Company's employee, D. R. , was found, and if so, in what circumstances, place and time from finding it lost.

In response, the Company, in a letter of [...] September 2021, addressed to the President of the Personal Data Protection Office, stated that D. R.'s employment certificate was personally handed over to P. M., who never handed it over to the Company or returned it to D. R. According to the Company's statement, the document was not found.

In another letter of [...] October 2021 (ref. No .: ...), the President of the Personal Data Protection Office asked the Company to indicate whether the employee was notified of a breach of personal data protection, in accordance with art. 34 sec. 1 and sec. 2 of Regulation 2016/679, and if so, how.

Referring to the above-mentioned of the letter of the President of the Personal Data Protection Office, the Company, in a letter of [...] November 2021, explained that D. R. had been informed about the infringement pursuant to Art. 34 sec. 1 and 2 of Regulation 2016/679, immediately after its finding. The company did not provide other evidence in support of the above statement, e.g. in the form of the content of the information addressed to D.R., proof of delivery of information, etc.

In connection with the above arrangements, in a letter of [...] December 2021 (ref. No .: ...), the President of the Personal Data Protection Office (UODO) sent to the Company a notice of the initiation of administrative proceedings regarding the failure to

notify the personal data breach to the President of the Personal Data Protection Office in accordance with Art. 33 sec. 1 of Regulation 2016/679 and the lack of notification of a personal data breach of the affected person, in accordance with art. 34 sec. 1 and 2 of Regulation 2016/679. The company, after receiving the notification of the initiation of the procedure, did not provide additional explanations on the matter.

Having read the entirety of the evidence collected in the case, the President of UODO considered the following:

When assessing whether a breach of personal data protection results in a risk of violation of the rights or freedoms of natural persons, one should take into account, inter alia, the content of recitals 75 and 85 of Regulation 2016/679. Moreover, the Article 29 Working Party in the Guidelines on the reporting of personal data breaches in accordance with Regulation 2016/679 (WP250rev.01), hereinafter referred to as the guidelines [1], indicated that the controller, when assessing the risk to individuals resulting from the breach, should take into account the specific circumstances violations, including the severity of the potential impact and the likelihood of its occurrence, and recommended that the assessment should take into account the criteria indicated in these guidelines during the assessment. In the above-mentioned The guidelines also clarify that when assessing the risks that may arise from a breach, the controller should collectively consider the importance of the potential impact on the rights and freedoms of individuals and the likelihood of their occurrence. Of course, the risk increases when the consequences of a breach are more severe and also when the likelihood of their occurrence increases. In case of any doubts, the controller should report the violation, even if such caution could turn out to be excessive.

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

Art. 33 sec. 1 and 3 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 - 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.

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

In the case in question, there was a breach of personal data protection, consisting in the loss by the Company of a document in the form of an employee's work certificate. The above fact was confirmed by the Company in explanations addressed to the President of the Personal Data Protection Office, inter alia, in the letters of [...] June 2021 and [...] August 2021, the Company also indicated in them that it had not reported the violation in question to the President of the Personal Data Protection Office, because in its opinion it did not involve a risk of violating the rights or freedoms of the person whose data they concern, and moreover, the employee whose employment certificate was lost did not make any claims against the Company in this respect. The company also stated that it had notified the employee of the loss of the employment certificate containing his personal data, in accordance with the regulations.

Taking a stance on the above, it should be pointed out that pursuant to § 2 sec. 1 of the Regulation of the Minister of Family, Labor and Social Policy of 30 December 2016 on the employment certificate (Journal of Laws of 2018, item 1289, as

amended), the employment certificate includes information necessary to determine rights under the employment relationship and rights from social insurance regarding:

1) the period or periods of employment,

2) the employee's working time during the employment relationship,

3) the type of work or positions held or functions performed,

4) the procedure and legal basis for termination or the legal basis for the termination of the employment relationship, and in the event of termination of the employment contract with notice - the party to the employment relationship who made the notice,

5) the period for which the employee is entitled to compensation in connection with the shortening of the notice period for the employment contract pursuant to art. 361 § 1 of the Act of June 26, 1974 - the Labor Code, hereinafter referred to as the "Labor Code",

6) annual leave due to the employee in the calendar year in which the employment relationship ended and used for that year,

7) unpaid leave used and the legal basis for granting it,

8) used paternity leave,

9) used parental leave and the legal basis for granting it,

10) used childcare leave and the legal basis for granting it,

11) the period in which the employee has benefited from the protection of the employment relationship referred to in art. 1868 § 1 point 2 of the Labor Code,

12) release from work provided for in art. 188 of the Labor Code, used in the calendar year in which the employment relationship ended,

13) the number of days for which the employee has received remuneration, in accordance with art. 92 of the Labor Code, in the calendar year in which the employment relationship ended,

14) the period of active military service or its alternative forms,

15) the period of performing work in special conditions or of a special nature;

16) used additional leave or other entitlement or benefit provided for by the provisions of the labor law,

17) non-contributory periods, falling in the employment period to which the employment certificate relates, taken into account when determining the right to a retirement pension or disability pension,

18) attachment of remuneration for work in accordance with the provisions on enforcement proceedings,

19) receivables from the employment relationship recognized and unpaid by the employer until the date of termination of this relationship due to lack of financial resources,

20) information on the amount and components of remuneration and qualifications obtained - at the request of the employee.

Above the information included in the content of the employment certificate constitutes personal data, especially as they appear together with the name and surname, employer and information about the date of birth of the data subject. Some of these data are particularly relevant to the rights or freedoms of the data subject. In particular, such data should be considered information on the procedure and legal basis for termination or legal basis for termination of the employment relationship, and in the event of termination of the employment contract with notice - the party to the employment relationship that gave notice and on the seizure of remuneration for work in accordance with the provisions on enforcement proceedings . This information, due to its nature, in the event of disclosure to unauthorized persons, may constitute the cause of violation of the freedoms or rights of the data subject. The above data may directly or indirectly reveal information about the personal life of the data subject, about his legal problems and financial status (e.g. information about the seizure of remuneration for enforcement proceedings), etc.

In this situation, the recognition by the Company that the incident did not constitute a breach of personal data protection had no factual or legal grounds. The circumstances of the data protection breach, as significant, should be taken into account by the Company when assessing whether it occurred, what was its scale and whether it was potentially associated with a risk of violating the rights or freedoms of data subjects, and whether the risk is high . Meanwhile, as is clear from the explanations provided, the Company did not do so, groundlessly considering that the breach was not associated with the risk of breaching the above-mentioned rights or freedoms in general, despite the fact that the lost document has not yet been found.

Therefore, it should be emphasized once again that in the case at hand, due to the failure to find the document, it is not important whether an unauthorized entity, e.g. a potential finder, actually came into possession and became familiar with the personal data contained in the lost work certificate of the Company's employee, but the fact that there was such a risk and, consequently, potentially there was also a risk of violation of the rights or freedoms of the data subject. It should be emphasized that the possible consequences of the event that took place do not have to materialize - in the content of Art. 33 sec. 1 of Regulation 2016/679 indicates 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 (unless it is unlikely that the breach would result in a risk of breach of rights or freedom of natural persons). Therefore, the circumstances raised by the Company that D. R. does not pursue claims against the Company for the loss of the employment certificate is irrelevant to the fact that the Company, as the administrator, is obliged to report the breach of personal data protection to the President of the Personal Data Protection Office, in accordance with Art. 33 sec. 1 of Regulation 2016/679. It is also irrelevant that the work certificate of D. R. was handed over by him personally to P. M., who, as the Company indicated in its explanations, did not then hand it over to the Company or returned it to D. R. It should be remembered that the handing over of the employment certificate to P. M. was tantamount to it to the Company, because Mr. M., as an employee of the Company, acted on its behalf and at its request, and was also a person authorized by the Company to process personal data of employees.

It should be emphasized that the breach of personal data protection that occurred in connection with the loss of the employment certificate of an employee of the Company poses a risk of violating rights or freedoms. As the Article 29 Working Party points out in the guidelines, “This risk exists where a breach could lead to physical or material or non-material damage to the data subjects of the breach. 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 case of a person whose personal data constituted the content of the lost employment certificate. Another important factor for such an assessment is the possibility of easy identification of the person whose data was affected by the breach, based on the disclosed data, especially in their local environment, which is a relatively small poviat town (J.).

Thus, it should be emphasized again that in the present case, it is not important whether an unauthorized person actually acquainted himself with the personal data of the person whose data is on the lost work certificate, but that there was a risk of such an event (i.e. the unauthorized person had the opportunity to become familiar with the data), which in turn means, due to the scope of data contained in the lost certificate, that there is a risk of violating the rights or freedoms of the data subject. In a similar case, the Provincial Administrative Court in Warsaw, in the judgment of September 22, 2021, file ref. II SA / Wa 791/21 stated that "(...) in the case at hand, it is not important whether an unauthorized recipient actually came into possession and became acquainted with the personal data of other persons, but that there was such a risk, and consequently also potentially there is a risk of violating the rights or freedoms of data subjects ”. Further, the Court also emphasizes that “the possible

consequences of an event that has occurred do not have to materialize. In the wording of Art. 33 sec. 1 of Regulation 2016/679 indicates 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, unless it is unlikely that the breach would result in a risk of violating the rights or freedoms natural persons. Therefore, the fact raised by the Administrator that the quotation: "no information has been received by the University that could have an impact on the change of the risk level or requiring taking other technical and organizational measures extending the catalog of actions taken" remains irrelevant for determining the Administrator's obligation to report the data breach in question personal data to the President of the Personal Data Protection Office, in accordance with the above provision ".

The Provincial Administrative Court in Warsaw made a similar opinion in the judgment of January 21, 2022 (file reference: II SA / Wa 1353/21), indicating that "(...) the possible consequences of the event of a personal data breach do not have to materialize - as in Art. . 33 sec. 1 GDPR, 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. The circumstance raised by the Company that the breach did not result in the occurrence of physical or damage to natural persons is irrelevant for the determination of the Company's obligation to notify the President of the Personal Data Protection Office of the breach of personal data protection, in accordance with the above-mentioned recipe ".

As already mentioned, in the case at hand, there is a risk that the content of the employment certificate and the personal data contained therein could be viewed by unauthorized persons in an unspecified number due to the inability to precisely define the circumstances, and in particular where the employment certificate was lost. As a consequence, this means that there is a risk of violation of the rights or freedoms of the data subject, which in turn results in the emergence of the Company, as the administrator, which should be emphasized again, an obligation to notify the breach of personal data protection to the supervisory authority, pursuant to Art. 33 sec. 1 of the Regulation 2016/679, which must contain the information specified in Art. 33 sec. 3 of this regulation.

For the above assessment, it does not affect whether the content of the employment certificate has in fact been read by unauthorized persons, how many, etc. a person whose duties, as part of employment in the Company, included establishing and keeping personal files of its employees. For the actions of this person, the Company is fully liable under applicable law, as for its own actions. In the above-mentioned the issue was raised by the Provincial Administrative Court in Warsaw in its

judgment of February 15, 2022 (file reference number II SA / Wa 3309/21), which ruled that "(...) the President of the Court as an administrator is responsible for any irregularities found in the data processing process . The fact that the President of the Court transferred the obligation to secure the carrier to the probation officer, did not verify whether the probation officer had secured it in any way, and did not carry out a test in terms of the effectiveness of this protection, deserves a negative assessment. In this state of affairs, the negligence of the President of the Court should be considered gross. ". 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".

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 personal data breach, 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 75 of the preamble to Regulation 2016/679 indicates, inter alia: "The risk of violating the rights or freedoms of persons, with different probability and severity of threats, may result from the processing of personal data that may lead to physical or property or non-material damage, in particular : where the processing may result in discrimination, identity theft or identity fraud, financial loss, damage to reputation, breach of the confidentiality of personal data protected by professional secrecy, unauthorized reversal of pseudonymisation or any other significant economic or social harm; where data subjects may be deprived of their rights and freedoms or the ability to exercise control over their personal data […] ".

When applying the provisions of Regulation 2016/679, it should be borne in mind that their purpose (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 with regard to 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.

The above reasoning is confirmed by the judgment of the Provincial Administrative Court in Warsaw of September 22, 2021 (file reference number II SA / Wa 791/21), in which the Court, when deciding on the imposition of an administrative fine in connection with the violation of the provisions on the protection of personal data, referred to the above-mentioned the above issue, additionally pointing out that "When assessing whether there are risks of violating human rights or freedoms, the administrator should take into account all possible damage and harm that may result from a given event for natural persons (such as: S. Jandt [in:] DS.-GVO ..., edited by J. Kuhling, B. Buchner, p. 617; Y. Reif [in:] DS.- GVO ..., edited by P. Gola, p. 496). They may in particular consist in losing control over your own personal data, negative image consequences, the possibility of another person concluding contracts using the personal data of another natural person, financial losses or, finally, negative social perception, which may be a consequence of making some personal data public. For the risk to occur, it is not necessary for the final loss or harm resulting from a given breach of personal data protection (as above, p. 616) ".

Consequently, it should be stated that the Company, despite the risk of violating the rights or freedoms of a natural person, did not notify the supervisory authority of a breach of personal data protection consisting in the loss of a document containing personal data of its employee (work certificate) and thus failed to comply with the obligation under Art. 33 sec. 1 of the Regulation 2016/679, which means the Company's breach of this provision.

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 of Regulation 2016/679, is subject to an administrative fine of up to EUR 10,000,000, and in the case of an enterprise - up to 2% of its total annual global turnover from the previous financial year, with the higher amount 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) Duration of the infringement (Article 83 (2) (a) of Regulation 2016/679);

The President of the Personal Data Protection Office considers the relatively long duration of the infringement to be an aggravating circumstance. At least a dozen or so months have elapsed from the Company becoming aware of the breach of personal data protection to the date of this decision, during which the risk of violating the rights or freedoms of the person affected by the breach could have materialized.

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

The company made a conscious decision not to notify the President of the Personal Data Protection Office (UODO), despite the letters of the President of the Personal Data Protection Office (UODO) addressed to it, indicating a possible risk of violating the rights or freedoms of the persons affected by the infringement. The Company's obligation under Art. 33 sec. 1 of the Regulation 2016/679, was not implemented by it.

c) 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 Company's reaction to the letters of the President of the Personal Data Protection Office indicating the possibility of a risk of violating the rights or freedoms of persons affected by the violation and the existence of an obligation to report the violation to the supervisory authority. Correct, in the opinion of the President of the Personal Data Protection Office (UODO), the action (notification of the infringement to the President of the Personal Data Protection Office) was not taken by the Company also after the initiation of administrative proceedings by the President of the Personal Data Protection Office.

d) The manner in which the supervisory authority became aware of the breach (Article 83 (2) (h) of Regulation 2016/679);

The President of the Personal Data Protection Office was not informed about the breach of the protection of personal data

being the subject of this case, i.e. the loss by the Company of the employment certificate of one of its employees, the President of the Personal Data Protection Office was not informed in accordance with the procedure specified in Art. 33 of the Regulation 2016/679, only as a result of explanatory activities carried out by the President of the Personal Data Protection Office in the Company as a result of a notification of possible irregularities and a request for inspection activities addressed to the President of the Personal Data Protection Office by the Poviat Police Commander in J. on the order of the District Prosecutor's Office in J. Circumstances of the lack of information on breach of data protection originating from the administrator obliged to provide such information to the President of the Personal Data Protection Office, i.e. the Company, should be considered as incriminating this administrator.

The following circumstances were considered to be attenuating circumstances in the present case:

a) the number of injured data subjects and the extent of the damage suffered by them (Article 83 (2) (a) of Regulation 2016/679) - the infringement in this case concerned only one person, and it was not found that the the data concerned, it suffered any damage due to the lack of claims against the Company;

b) no previous infringements committed by the administrator have been identified (Article 83 (2) (e) of Regulation 2016/679).

The fact that the President of the Personal Data Protection Office (UODO) applied in the present case of the sanction in the form of an administrative fine, as well as its amount, was not influenced by other sanctions indicated in Art. 83 sec. 2 of Regulation 2016/679, the circumstances:

a) the nature and gravity of the breach, taking into account the nature, scope and purpose of the processing (Article 83 (2) (a) of Regulation 2016/679) - the breach found in this case is not of significant and serious nature - the risk of violating the rights or freedoms of a person, data subject is not high;

b) actions taken by the controller to minimize the damage suffered by the data subject (Article 83 (2) (c) of Regulation 2016/679) - in the present case, no harm was found to the person affected by the infringement, in connection with what the Company was not obliged to take any actions to minimize them;

c) the degree of responsibility of the controller, taking into account technical and organizational measures implemented by him pursuant to Art. 25 and 32 (Article 83 (2) (d) of Regulation 2016/679) - breach of the provisions of Regulation 2016/679, assessed in this proceeding (failure to notify the President of the Personal Data Protection Office of the breach of personal data protection), is not related to the technical measures applied by the controller and organizational;

d) the categories of personal data concerned by the breach (Article 83 (2) (g) of Regulation 2016/679) - no breach of data protection belonging to specific categories of personal data referred to in Art. 9 sec. 1 of the Regulation 2016/679, and the breach of which could constitute a circumstance having an impact on the penalty imposed by this decision;

e) 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 President of the Personal Data Protection Office has not previously applied the measures referred to in the aforementioned provision;

(f) 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) - the administrator does not apply approved codes of conduct or approved certification mechanisms;

g) financial benefits or losses avoided directly or indirectly as a result of the infringement (Article 83 (2) (k) of Regulation 2016/679) - it was not found that the controller would obtain any benefits or avoid financial losses due to the infringement.

In the opinion of the President of the Personal Data Protection Office, the applied administrative fine 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, as the controller, will fulfill its obligations in the field of personal data protection in the future, in particular in the scope of reporting the breach of personal data protection to the President of the Personal Data Protection Office. 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 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 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, which is closest after that date.

Bearing in mind the above, the President of the Personal Data Protection Office, pursuant to art. 83 sec. 4 lit. a) in connection with Art. 103 of the Act of May 10, 2018 on the Protection of Personal Data, for the violation described in the operative part of this decision, imposed on the Company - using the average EUR exchange rate of January 28, 2022 (EUR 1 = PLN 4.5697) - an administrative fine in the amount of PLN 15,994 (equivalent to EUR 3,500).

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 breach by the Company as the administrator of the provisions of Regulation 2016/679. It will also fulfill a preventive function, because, in the opinion of the President of the Personal Data Protection Office, it will indicate to the Company and other data controllers that it is wrong to disregard the obligations of administrators related to the occurrence of a breach of personal data protection, and aimed at preventing it from being negative and often severe for the persons affected by the breach. , the effects, as well as the elimination of these effects or at least limitation.

In connection with the above, it should be noted that the fine in the amount of PLN 15,994 (say: fifteen thousand nine hundred and ninety-four zlotys) meets, in the established circumstances of this case, the conditions referred to in Art. 83 sec. 1 of Regulation 2016/679, due to the type and seriousness of the breach found in the context of the basic objective of Regulation 2016/679 - protection of fundamental rights and freedoms of natural persons, in particular the right to the protection of personal data.

Referring to the amount of the administrative fine imposed on the Company, the President of the Office for Personal Data Protection decided that it is proportional to both the seriousness of the breach found in this case and the financial situation of the Company and will not constitute an excessive burden for it. The submitted profit and loss account shows that the revenues from the Company's operations in the period November 28, 2019 - December 31, 2020 amounted to approximately PLN 2,500,000 (two million five hundred thousand zlotys), therefore the amount imposed in this case administrative fine constitutes approx. 0.64% of the turnover achieved by the Company in the period for which the Company presented financial data, i.e. in the period of approx. 13 months (from full December 2019 to full December 2020). At the same time, it is worth emphasizing that the amount of the imposed fine (PLN 15,994) is only about 0.04% of the maximum amount of the fine that the President of the Personal Data Protection Office could - applying, in accordance with Art. 83 sec. 4 of Regulation 2016/679, the maximum threshold of EUR 10,000,000 (according to the average EUR exchange rate of January 28, 2022 - PLN 45,697,000) - to be imposed on the Company for the breach of the provisions of Regulation 2016/679 found in this case.

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 Company's obligations as an administrator, but 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 employment or a significant decrease in the Company's turnover.

As regards the Company's failure to notify about a breach of personal data protection, the data subject is a breach of Art. 34

sec. 1 and 2 of Regulation 2016/67, which violation was also covered by the scope of this proceeding, the President of the Personal Data Protection Office (UODO) concluded, on the basis of the collected evidence, that there was no high risk of violation of the rights or freedoms of the above-mentioned persons, mainly due to the scope of data covered by the infringement, provided for in the employment certificate. This scope has been defined in § 2 sec. 1 of the Regulation of the Minister of Family, Labor and Social Policy of 30 December 2016 on the employment certificate (Journal of Laws 2018, item 1289, as amended), but does not include data such as PESEL number, identity documents, data included in art. 9 sec. 1 of Regulation 2016/679 to special categories of personal data or other data the nature of which determines the existence of a high risk of violation of the rights or freedoms of the data subject. In turn, the occurrence of a high risk of violation of the rights or freedoms of a natural person is a necessary condition for the obligation to notify the data subject about the violation, pursuant to Art. 34 sec. 1 of Regulation 2016/679. Due to the above, due to the fact that in the case in question there is no high risk of violation of the rights or freedoms of the data subject and the related obligation to notify this person about the violation, the proceedings in the part concerning the above-mentioned the issue has become redundant. Pursuant to Art. 105 § 1 of the Code of Administrative Procedure, when the proceedings for any reason have become redundant in whole or in part, the public administration authority issues a decision to discontinue the proceedings, respectively, in whole or in part. The premise for the discontinuation of the proceedings, pursuant to Art. 105 § 1 of the Code of Administrative Procedure, the proceeding is groundless "for any reason", i.e. for any reason that results in the lack of one of the elements of the material legal relationship with respect to its subjective or objective party (judgment of the Supreme Administrative Court of 21 January 1999, ref. SA / Sz1029/97).

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). The 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 aid may be granted upon application of a party submitted before 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 Office for Personal Data Protection 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 10 May 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.

[1] https://www.uodo.gov.pl/pl/10/12.

2022-06-06