Warsaw, on 09

May

2023

Decision

DKN.5131.44.2022

Based on Article. 104 § 1 of the Act of June 14, 1960 Code of Administrative Procedure (Journal of Laws of 2022, item 2000, as amended), art. 7 sec. 1 and art. 60, art. 102 sec. 1 item 1 i sec. 3 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. i), art. 83 sec. 1–3, art. 83 sec. 4 lit. a) in connection with art. 24 sec. 1, art. 25 sec. 1 and art. 32 sec. 1 and 2 art. and 83 sec. 5 lit. a) in connection with art. 5 sec. 1 lit. f) and art. 5 sec. 2 Regulation of the European Parliament and of the EU Council 2016/679 of April 27, 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 data protection regulations) (Official Journal EU L 119 of 4/05/2016, p. 1, Official Journal of the EU L 127 of 23/05/2018, p. 2 and Official Journal of the EU L 74 of 4/03/2021, p. 35), after carrying out administrative proceedings initiated ex officio regarding the violation of the provisions on the protection of personal data by the Mayor of the City and Commune of W. (W. City and Commune Office, ul. [...]), President of the Personal Data Protection Office,

finding a violation by the Mayor of the City and Commune of W. (W. City and Commune Office, ul. […]) of the provisions of art. 5 sec. 1 lit. f), art. 5 sec. 2, art. 24 sec. 1, art. 25 sec. 1 and art. 32 sec. 1 and 2 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46 / EC (general regulation on data protection) (Official Journal of the EU L 119 of 4/05/2016, p. 1, Official Journal of the EU L 127 of 23/05/2018, p. 2 and Journal of the EU L 74 of 4/03/2021, p. 35), hereinafter referred to as Regulation 2016/679, consisting in failure by the Mayor of the City and Municipality of W. to apply appropriate organizational measures to ensure a level of security corresponding to the risk of data processing, which resulted in unauthorized copying of personal data from a company computer to a portable storage medium by an employee of the City Hall and the Commune of W., imposes on the Mayor of the City and Commune of W. (W. City and Commune Office, ul. [...]) for violation of the provisions of Art. 5 sec. 1 lit. f), art. 5 sec. 2, art. 25 sec. 1 and art. 32 sec. 1 and 2

of Regulation 2016/679, an administrative fine of PLN 10,000 (say: ten thousand zlotys).

Justification

The Mayor of the City and Commune of W. (W. City and Commune Office, ul. [...]), also referred to as the Mayor or the Administrator, (...) on May 2022, notified the President of the Office for Personal Data Protection, hereinafter also referred to as the President of the Personal Data Protection Office, a breach of protection personal data, which took place (...) May 2022 (supplementary notification was made [...] May 2022).

The violation of personal data protection occurred as a result of the unauthorized execution of a copy of personal data from a company computer to a portable storage medium by an employee of the City and Commune Office in the following scope: surnames and first names, date of birth, bank account number, address of residence or residence, PESEL registration number , other (information on settlements of fees for rent, water, sewage, electricity, rental of premises).

In the notification of a personal data breach of (...) May 2022, the Administrator indicated that "(...) on [...] May 2022, a flash drive was brought to the City and Commune Office of W. on the recommendation of an employee on sick leave. We know from preliminary information that the carrier contains business documents containing personal data, such as: contracts with natural persons, rental contracts, invoices, settlements. The carrier was delivered by a third party who is not an employee of the Office. This person is also not authorized. We suspect that an employee on leave made an unauthorized and unauthorized copy of official documents to a private data carrier (…)".

In the supplementary notification of (...) May 2022, the Administrator indicated that "(...) on [...] May 2022, Mrs. K.B. as the Manager [...] reported to the Data Protection Inspector with information that there was probably a data protection breach. In the course of the initial conversation, it was established that [...] on May 2022, one of the former employees of the City and Commune Office of W. brought an unidentified flash drive on the instructions of the current employee on sick leave, Ms. D. Z. After verifying the contents of the medium, it was noticed that it contained files containing templates of contracts, contracts for entrusting the processing of personal data, contracts for the use of pitches, information on rents, data necessary to make calculations for electricity, water, sewage and rents, letters to residents of social and municipal housing, letters for granting premises and lists of premises. Most documents are only templates that do not contain personal data. The data contained in the documents are names and surnames, addresses, invoice amounts and occasionally [up to 10 people] - PESEL numbers and bank account numbers. The medium contains personal data of about 250 natural persons and companies. The exact

number of people is difficult to estimate due to the fact that many names in the documents are repeated, and more than about 2,100 files were analyzed on the medium itself (…) After the investigation, which lasted from […] May 2022. until [...] May 2022, the following was stated: On [...] May 2022, around 7 a.m., Mrs. D. Z. appeared in the office despite the fact that the Office was open on that day from 8 a.m. It was also established that she did not register her presence on the working time recorder, because on that day she was on sick leave. After analyzing the logs, the IT specialist determined that Mrs. D. Z. logged on to her computer at 6:58 and logged out at 7:32. Initially, the purpose of the visit was not known to the employees. On the same day, i.e. […] May 2022, around 8 am, Mrs. D. Z. sent the password to her work computer to one of her colleagues. Due to the large number of substantive errors committed by Mrs. D. Z. [not related to the protection of personal data] on [...] May 2022, it was decided that it would be necessary to review the documents on her computer. Unfortunately, most of the documents have not been found. At first, it was suspected that it was a system or server failure of the Office or the fact that documents were moved to another folder. In the course of the proceedings, however, it was established that the disappearance of the documents was caused by their downloading to an external medium and deleting them from the disk, which was confirmed by analyzing the logs and by recreating data from the flash drive, on which most of the sought documents were found. In the course of the proceedings, it was impossible to determine whether any unauthorized person had access to the data on the carrier. However, given the situation where a third party brings a medium containing data directly to the Office at the employee's request, it should be considered that such access was possible, which causes a high risk of violating the rights and freedoms of natural persons in connection with the processing of their personal data. In connection with the situation, it was clearly stated that the provisions on the protection of personal data had been violated. (…)".

In connection with the submitted explanations, the President of the UODO, acting pursuant to art. 58 sec. 1 lit. a) and e) of Regulation 2016/679, asked the Administrator, among others o: 1) providing the supervisory body with the procedure for the use of portable storage media, functioning in the City and Commune Office of W., 2) providing information whether the data was uploaded by the employee to a private or business medium, 3) providing information whether the administrator uses encryption ports or other tools preventing the transfer of data to an unauthorized storage medium, 4) provide information whether the administrator conducted staff training in the scope of the possibility of such personal data protection violations.

In response to the above summons from the supervisory authority, the Administrator, in a letter of (...) May 2022, explained that the Mayor could not unequivocally state whether the data was copied by the employee to a private or business medium,

because "(...) the employee was not caught < by the hand> during data downloading. However, assuming that the data were returned on the same medium on which they were ripped, it should be assumed that it was a private medium (…)". The administrator also explained that until the date of the breach in question, he did not use port encryption and other tools preventing the transfer of data to an unauthorized medium. At the same time, he stated that he had started implementing the blockade of USB ports on all business computers and that he was in the process of searching for an appropriate system that would prevent unauthorized copies of documents located on local drives of workstations and on network drives. In response to the question whether the Administrator conducted staff training in the scope of the possibility of such personal data protection violations, the Mayor indicated that when hiring new people, he always provides them with documentation on the protection of personal data, enriched with training in the form of self-education, legal provisions, examples of violations of the provisions in the processing of personal data, or instructions on how to proceed in the event of a violation of personal data processing. The administrator explained that on the day of starting work, each employee receives an authorization to process personal data, under which he declares that "(...) he has read the provisions on the protection of personal data and <GDPR documentation> introduced at the administrator's office (...)" and at the same time undertakes to comply with the above regulations and documentation as well as appropriate protection and data processing, along with maintaining secrecy and confidentiality. In addition, the Mayor stated that "(...) training for employees was organized in 2018 in three rounds [on [...] October, [...] October and [...] December]. Attendance at the training was confirmed by the employees' signatures (…)".

The administrator also attached the "Procedure (...)" to the explanations.

Then, the President of the UODO, in a letter of (...) May 2022, asked, among others, o: 1) providing information whether the person guilty of the infringement participated in the training, if so, requested an attendance list together with the training plan, 2) an indication of the reasons why the administrator conducted training for its employees only in 2018, 3) providing a photocopy of the statement of the employee guilty of the infringement that he has read the provisions on the protection of personal data and the "GDPR documentation" together with an indication whether the above-mentioned the statement also includes the procedure for the use of portable storage media, 4) providing explanations whether the controller has carried out a risk analysis for the processing of personal data covered by the breach, both before and after its occurrence.

In response to the above letter of the President of UODO, in the letter of (...) September 2022, the administrator indicated that he did not have a written confirmation that the person guilty of the infringement participated in the training in 2018. The mayor

stated that he found the attendance list from the training organized in 2018, noting that according to with knowledge, not all employees participating in the training signed the list (the person guilty of the infringement did not sign either).

The administrator indicated that he conducted training in the form of a video-conference at his headquarters in 2018. At the same time, he stated that "(...) later, the administrator did not take action to organize another training, because a training in the form of guided self-education was prepared for employees. Employees were also familiarized in 2020 with the amended <GDPR documents>, including the instructions on how to proceed in the event of a breach. The employees signed declarations that they had read these documents. During the inspection of the current work of employees in the field of personal data protection, no significant deficiencies were found, and if they were detected, ongoing talks were held with employees in order to issue instructions for correcting them. However, these conversations were not recorded. Therefore, bearing in mind the above, the administrator did not conduct another training for employees (…)". The mayor further explained that he had not conducted a risk analysis for the processing of data affected by the breach before it occurred. After the breach occurred, a general risk analysis and impact assessment for the processing of data covered by the breach were carried out.

The explanations also indicate that the implementation of the procedure for the use of portable storage media in the City and Commune Office of Warsaw took place (...) in May 2022.

To the explanations of (...) September 2022, the Administrator attached a photocopy of the employee's statement on having read the data protection provisions and the "GDPR documentation", indicating that "(...) this statement [included in the authorization] does not, however, contain a statement covering the procedure regarding the use storage media. This procedure was introduced later and, despite familiarizing employees with it, the administrator did not collect written statements about familiarizing themselves with the procedure (...)".

In connection with the submitted explanations, on (...) September 2022, the President of the UODO instituted ex officio administrative proceedings regarding the possibility of the Mayor, as the data controller, violating the obligations arising from the provisions of Art. 5 sec. 1 lit. f), art. 5 sec. 2, art. 24 sec. 1, art. 25 sec. 1 and art. 32 sec. 1 and 2 of Regulation 2016/679, in connection with a breach of personal data protection, reported to the President of the UODO on (...) May 2022 and registered under number (...).

In response to the initiation of administrative proceedings, in a letter of (...) September 2022, the administrator indicated that "(...) referring to the proceedings conducted so far, the Mayor of the City and Commune of W. as the data controller wishes to

demonstrate that throughout the entire period of the proceedings he showed good will and willingness to cooperate in the infringement with the President of the Data Protection Office (...) Regardless of the information provided so far regarding the measures taken to eliminate similar irregularities in the future, the administrator has taken additional steps to train all authorized persons on the premises of the City Hall and Communes W. Training will take place on two dates in October (...) Therefore, the administrator wishes to express its readiness to continue active participation in the ongoing proceedings, express its remorse and at the same time ask that the President of the Data Protection Office take into account mitigating circumstances when issuing decisions in the proceedings in question (...)".

On (...) January 2023, the Mayor sent the document "Evaluation (...)", which was introduced by the Administrator on (...) June 2022.

The supervisory authority assessed the evidence in terms of examining its credibility and evidential value. The President of the UODO considered all the evidence submitted by the Administrator to be credible. The above is supported by the fact that the individual explanations provided by the Mayor are logical, consistent and correlate with the entirety of the evidence.

In this factual state, after reviewing all the evidence collected in the case, the President of the Office for Personal Data Protection considered the following: Pursuant to Art. 34 of the Act of May 10, 2018 on the Protection of Personal Data (Journal of Laws of 2019, item 1781) - hereinafter referred to as: the Act of May 10, 2018, the President of the UODO is the competent authority on data protection and the supervisory authority within the meaning of Regulation 2016/679. Pursuant to Art. 57 sec. 1 lit. (a) and (h) of Regulation 2016/679, without prejudice to other tasks defined under that Regulation, each supervisory authority in its territory monitors and enforces the application of this Regulation and conducts proceedings for infringements of this Regulation, including on the basis of information received from another supervisory authority or other public authority.

Article 5 of Regulation 2016/679 formulates the rules regarding the processing of personal data that must be respected by all administrators, i.e. entities that individually or jointly with others determine the purposes and methods of personal data processing. In accordance with art. 5 sec. 1 lit. f) of Regulation 2016/679, personal data must be processed in a manner that ensures adequate security of personal data, including protection against unauthorized or unlawful processing and accidental loss, destruction or damage, using appropriate technical or organizational measures ("confidentiality and "). Pursuant to Art. 5 sec. 2 of Regulation 2016/679, the administrator is responsible for compliance with the provisions of para. 1 and must be able to demonstrate compliance with them ("accountability"). Specification of the confidentiality principle referred to in art. 5 sec. 1

lit. f) of Regulation 2016/679, are further provisions of this legal act. In accordance with art. 24 sec. 1 of the Regulation 2016/679, taking into account the nature, scope, context and purposes of processing as well as the risk of violating the rights or freedoms of natural persons with different probabilities and severity, the administrator implements appropriate technical and organizational measures so that the processing takes place in accordance with this regulation and to be able to demonstrate it . These measures are reviewed and updated if necessary.

Pursuant to art. 25 sec. 1 of Regulation 2016/679, taking into account the state of technical knowledge, the cost of implementation and the nature, scope, context and purposes of processing as well as the risk of violating the rights or freedoms of natural persons with different probabilities and severity resulting from processing, the controller - both when determining the processing methods and during the processing itself - implements appropriate technical and organizational measures, such as pseudonymization, designed to effectively implement the principles of data protection, such as data minimization, and to provide the processing with the necessary safeguards to meet the requirements of this regulation and protect the rights of persons whose data applies.

From the content of art. 32 sec. 1 of Regulation 2016/679 shows that the administrator is obliged to apply technical and organizational measures corresponding to the risk of violating the rights and freedoms of natural persons with different probability of occurrence and severity of the threat. The provision specifies that when deciding on technical and organizational measures, the state of technical knowledge, the cost of implementation, the nature, scope, context and purposes of processing as well as the risk of violating the rights or freedoms of natural persons with different probability and severity should be taken into account. The quoted provision shows that the determination of appropriate technical and organizational measures is a two-stage process. First of all, it is important to determine the level of risk associated with the processing of personal data, taking into account the criteria indicated in art. 32 sec. 1 of Regulation 2016/679, and then it should be determined what technical and organizational measures will be appropriate to ensure a level of security corresponding to this risk. These arrangements, where applicable, should include measures such as pseudonymisation and encryption of personal data, the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services, the ability to quickly restore the availability and access to personal data in the event of a physical incident or technical and regularly testing, measuring and evaluating the effectiveness of technical and organizational measures to ensure the security of processing. Pursuant to art. 32 sec. 2 of Regulation 2016/679, when assessing whether the level of security is appropriate, the

administrator takes into account, in particular, the risk associated with processing, in particular resulting from accidental or unlawful destruction, loss, modification, unauthorized disclosure or unauthorized access to personal data sent, stored or otherwise processed.

As indicated by art. 24 sec. 1 of Regulation 2016/679, the nature, scope, context and purposes of processing as well as the risk of violating the rights or freedoms of natural persons with different probabilities and severity are factors that the controller is obliged to take into account in the process of building a data protection system, also in particular from the point of view of other obligations indicated in art. 25 sec. 1, art. 32 sec. 1 or Art. 32 sec. 2 of Regulation 2016/679. The indicated provisions specify the confidentiality principle specified in art. 5 sec. 1 lit. f) of Regulation 2016/679, and compliance with this principle is necessary for the proper implementation of the accountability principle resulting from art. 5 sec. 2 of Regulation 2016/679.

One of the legal grounds for the protection of personal data introduced by Regulation 2016/679 is the obligation to ensure the security of processed data, specified, inter alia, in art. 32 sec. 1 of Regulation 2016/679. This provision introduces a risk-based approach, while indicating the criteria based on which the controller should select appropriate technical and organizational measures to ensure a level of security corresponding to this risk. In addition to the risk of violating the rights or freedoms of natural persons, the state of technical knowledge, the cost of implementation and the nature, scope, context and purposes of processing should therefore be taken into account.

For the proper performance of the obligations arising from the above-mentioned provisions of Regulation 2016/679, the administrator should first conduct a risk analysis and, based on it, determine and implement adequate security measures in the processing of personal data.

If the Administrator has provided for the possibility of using portable storage media (e.g. USB memory), the analysis in question should indicate possible risks resulting from the possibility of their incorrect use, which could result in unauthorized copying of data saved on a company computer to a portable storage medium by an employee. Consequently, the analysis in question should provide for appropriate security measures to minimize the risk of a personal data breach.

In the realities of this case, it should be pointed out that the Administrator, allowing the possibility of using portable storage media (e.g. USB memory), in particular if these media are privately owned, based on a properly conducted risk analysis, should identify threats to the processed personal data using this type of computer hardware, and then define and implement appropriate technical and organizational measures to ensure the security of this data, as well as regularly check the

effectiveness of these measures, in accordance with the requirements of art. 32 sec. 1 and 2 of Regulation 2016/679.

It should also be pointed out that the obligation to implement appropriate technical and organizational measures in order to provide the processing with the necessary safeguards due to the adopted method of processing personal data results, among others, from straight from art. 25 sec. 1 of Regulation 2016/679. This provision requires the data controller to take data protection into account, in particular in the design phase, which means that the Mayor, giving the possibility to use portable storage media (e.g. USB sticks), should already at this stage specify (and implement) effective security measures.

It should be pointed out that Regulation 2016/679 introduced an approach in which risk management is the foundation of activities related to the protection of personal data. Risk management is a continuous process that forces the data controller not only to ensure compliance with the provisions of Regulation 2016/679 through a one-time implementation of organizational and technical security measures, but also to ensure continuous monitoring of the level of threats and ensure accountability in terms of the level and adequacy of the introduced security measures. In view of the above, it becomes necessary to be able to prove to the supervisory authority that the solutions introduced to ensure the security of personal data are adequate to the level of risk, as well as take into account the nature of the organization and the mechanisms used for processing personal data. Therefore, the administrator is to independently conduct a detailed analysis of the data processing processes carried out and perform a risk assessment, and then apply measures and procedures that will be adequate to the assessed risk. The consequence of this approach is the need to independently select security measures based on a threat analysis. It should be emphasized that the administrators are not provided with specific security measures and procedures.

In the context of the above, it should be pointed out that the risk analysis carried out by the data controller should be documented and justified on the basis of, first of all, the determination of the facts existing at the time of its implementation. In particular, the characteristics of the ongoing processes, assets, vulnerabilities, threats and existing safeguards as part of the ongoing personal data processing processes should be taken into account. Also, during this process, the scope and nature of personal data processed in the course of activities carried out by the data controller cannot be omitted, because depending on the scope and nature of the disclosed data, the potential negative consequences for a natural person in the event of a breach of the protection of their personal data will depend.

The term asset is used to indicate anything that is of value to the data controller. Certain assets will be of a higher value than others, and they should also be assessed and secured from this perspective. The interconnections of existing assets are also

very important, e.g. the confidentiality of assets (personal data) will depend on the type and method of processing this data. Determining the value of assets is necessary to assess the effects of a possible incident (breach of personal data protection). It is obvious that a wide range of personal data or the processing of personal data referred to in art. 9 or art. 10 of Regulation 2016/679, may cause (in the event of a personal data breach) far-reaching negative consequences for the data subjects, so they should be assessed as high-value assets, and thus the degree of their protection should be adequately tall.

Determining the existing or applied safeguards is necessary, among other things, in order not to duplicate them. It is also essential to check the effectiveness of these safeguards, because the existence of an untested security, firstly, may eliminate its value, and secondly, it may give a false sense of security and may result in the omission (non-detection) of a critical vulnerability, which, if used, will cause very negative effects, including, in particular, lead to a breach of personal data protection.

Vulnerability is commonly referred to as a weakness or a security gap that, when used by a given threat, may interfere with the functioning and may also lead to incidents or breaches of personal data protection. Identifying threats consists in determining what threats and from what direction (reason) may appear.

The method of conducting a risk analysis is, for example, defining the risk level as the product of the probability and consequences of a given incident. Typically, a risk matrix is used, which allows you to visualize risk levels, presenting risk levels for which the organization defines appropriate actions.

In order for the risk analysis to be carried out properly, threats that may occur in the data processing processes should be defined for each of the assets.

Taking into account, in particular, the scope of personal data processed by the Mayor contained in documents copied to a portable data carrier, in order to properly fulfill the obligations imposed on the above the provisions of Regulation 2016/679, the Administrator was obliged to take actions to ensure an appropriate level of data protection by implementing appropriate technical and organizational measures, as well as actions aimed at optimal security and configuration of the resources, tools and devices (including computer hardware) used by regular testing, measuring and evaluating the effectiveness of technical and organizational measures to ensure the security of data processing in the form of security tests in the field of IT infrastructure and applications. The nature and type of these activities should result from the risk analysis carried out, in which vulnerabilities related to the resources used and the resulting threats should be identified, and then adequate security

measures should be defined. However, according to the collected evidence, the administrator did not conduct a risk analysis for the processing of data covered by the breach before the occurrence of the personal data breach in question. As pointed out by the Provincial Administrative Court in Warsaw in the judgment of May 13, 2021, file ref. II SA/Wa 2129/20, "The data controller should therefore carry out a risk analysis and assess what threats it is dealing with."

It should be emphasized that risk management (conducting a risk analysis and, on this basis, implementing appropriate safeguards) is one of the basic elements of the personal data protection system and, as also indicated by the above-mentioned judgment of the Provincial Administrative Court in Warsaw, is a continuous process. Therefore, both the adequacy and effectiveness of the security measures applied should be periodically verified, in accordance with the requirement provided for in Art. 32 sec. 1 lit. d) Regulation 2016/679. The data controller should therefore regularly test, measure and evaluate the effectiveness of technical and organizational measures to ensure the security of processing.

New risks or threats may also materialize or be revealed spontaneously, in a way that is completely independent of the administrator, and this is a fact that should also be taken into account both when building a personal data protection system and during its implementation. This, in turn, defines the need to conduct regular verification of the entire personal data protection system, both in terms of adequacy and effectiveness of the implemented organizational and technical solutions.

It should also be emphasized that the study of the probability of a given event should not be based solely on the frequency of occurrence of events in a given organization, because the fact that a given event did not occur in the past does not mean that it cannot occur in the future.

In this context, it should be noted that the Provincial Administrative Court in Warsaw, in its judgment of August 26, 2020, file ref. II SA/Wa 2826/19, raised that "(...) activities of a technical and organizational nature are the responsibility of the personal data administrator, but they cannot be selected in a completely free and voluntary manner, without taking into account the degree of risk and the nature of the protected personal data. "

In the case in question - due to the failure to carry out a risk analysis for personal data processing operations prior to the occurrence of a personal data protection breach in connection with the use by employees of the City and Commune Office of W. of computer equipment enabling the connection of portable data carriers (in particular USB memory sticks), including private portable media which would take into account the risks associated with unauthorized copying of files containing personal data by an employee from a company computer to this type of data carrier - the Administrator did not monitor both the

adequacy and effectiveness of the security measures applied, contrary not only to the obligations arising from art. 24 sec. 1, art. 25 sec. 1 and art. 32 sec. 1 and 2 of Regulation 2016/679, but also the accountability principle referred to in Art. 5 sec. 2 of Regulation 2016/679.

The jurisprudence indicates that "(...) Regulation 2016/679 does not, however, prejudge how the administrator should fulfill the obligations arising from the principle of accountability contained in Art. 5 sec. 2 the above-mentioned of the regulation, however, indicates the need to account for compliance with the regulations, report on their implementation and provide evidence of proper performance of duties. The accountability principle obliges controllers to demonstrate that they have taken all measures to ensure compliance with the obligation to protect personal data. In the light of the above principles, it is the administrator, not the supervisory authority dealing with the protection of personal data, who is responsible for developing, updating and maintaining all procedures and documents related to the protection of personal data, as well as for creating evidence that proves the compliance of processing with the provisions (...)" (judgment of the Provincial Administrative Court in Warsaw of February 1, 2022, reference number II SA/Wa 2106/21, LEX No. 3392761). The above is confirmed by the decision of the Provincial Administrative Court in Warsaw of February 10, 2021, ref. II SA/Wa 2378/20: "The accountability principle is therefore based on the controller's legal responsibility for the proper fulfillment of duties and imposes on him the obligation to demonstrate, both to the supervisory authority and to the data subject, evidence of compliance with all data processing principles." The issue of the principle of accountability is similarly interpreted by the Provincial Administrative Court in Warsaw in the judgment of August 26, 2020, file ref. II SA/Wa 2826/19: "Taking into account all the standards of Regulation 2016/679, it should be emphasized that the administrator has considerable freedom in terms of the security measures used, but at the same time is responsible for violating the provisions on the protection of personal data. The principle of accountability directly implies that it is the data controller who should demonstrate, and thus prove, that he complies with the provisions set out in Art. 5 sec. 1 of Regulation 2016/679."

To sum up, it should be pointed out again that the circumstances of the case show that the Mayor, prior to the occurrence of a personal data breach, did not assess the risk of a possible violation of the confidentiality of personal data (Article 5(1)(f) of Regulation 2016/679), resulting from from the risks related to allowing the use of portable data carriers by employees of the City Hall and the Commune of Warsaw, including threats related to the unauthorized making of copies of files from a company computer to this type of data carrier. As a consequence, the Mayor also failed to comply with the accountability principle in this

regard (Article 5(2) of Regulation 2016/679). It should be emphasized that carrying out a risk analysis before allowing the use of portable data carriers by employees of the City Hall and the Municipality of W., and then monitoring the adopted security procedures, would minimize the risk of the breach in question and would satisfy the accountability obligation imposed on the Administrator.

As already indicated above, in the facts of the case in question, the risk concerned the threat of unauthorized use of a portable data carrier by an employee of the City and Commune Office of W. (most likely this carrier was owned by the employee). In the course of the proceedings, the Administrator did not prove that the company computers used by the employees of the City Hall and Municipality of Warsaw were protected against the possibility of unauthorized copying of files containing personal data using portable storage media, such as a USB stick. Before the breach, the Mayor did not use port protection and other tools preventing the transfer of data to an unauthorized data carrier. As a consequence, the Administrator is unable to definitively determine whether the data from the company computer located at his headquarters were copied to a portable data carrier that was his property, or whether this carrier was the property of an employee. However, in the letter of (...) May 2022, the Administrator himself admits that "(...) assuming that the data were returned on the same medium to which they were downloaded, it should be assumed that it was a private medium (...)". In the light of the above, it would be of secondary importance to introduce encryption of business portable storage media, since business computers located at the Administrator's headquarters were not protected against the possibility of copying data from them to an unauthorized portable data carrier (in this case, most likely owned by an employee of the City and Commune Office of W. ). In addition, it should be noted that the "Procedure (...)", which regulates the use of portable data carriers, was adopted only after the breach of personal data protection in question occurred.

It should be pointed out again that with regard to portable storage media used by employees of the City and Commune Office of Warsaw, due to the associated risks, in order to counteract the potential effects of a breach and prevent the loss of confidentiality of personal data on such a device, the administrator , pursuant to art. 24 sec. 1, art. 25 sec. 1 and art. 32 1 and 2 of Regulation 2016/679, is obliged to use effective safeguards that, in the case of e.g. copying documents from work computers to a portable data carrier, will prevent unauthorized persons from accessing personal data processed by the Administrator. As shown above, the Mayor did not introduce such effective safeguards against the occurrence of a breach.

Due to the fact that the Administrator did not carry out a risk analysis before the personal data protection breach occurred, the

Mayor is unable to demonstrate whether the adopted solutions actually ensured adequate security in the case of personal data processing in connection with the use of portable media by employees of the City Hall and Municipality of Warsaw data. The selection of these measures should take place as a result of a properly conducted risk analysis for personal data processing operations, which, however, the Administrator did not do before the personal data protection breach occurred. It should also be noted that the Mayor - due to the nature of the solutions he has adopted - is objectively unable to verify and, consequently, also demonstrate whether the employee used portable data carriers in a way that guaranteed the lawful processing of personal data.

As it results from the collected evidence, the Administrator has conducted trainings covering issues related to the protection of personal data, however, he is unable to prove that the person responsible for the violation of personal data protection participated in these trainings. Therefore, it should be emphasized that also in this case the Administrator did not comply with the accountability principle, as he is unable to prove that the employee (whose activity led to the violation) was properly trained in the application of the provisions governing the protection of personal data. Properly conducted trainings allow the trainees to properly understand the principles of personal data processing specified by the Administrator, and consequently contribute to reducing the risk of violations in this area. It should also be pointed out that conducting training in the field of personal data protection, in order to be considered an adequate security measure, must be carried out in a cyclical manner, which will ensure constant reminder and, consequently, consolidation of the principles of personal data processing covered by the training. In addition, all persons authorized to process personal data must participate in such training, and the training itself must cover all issues related to the processing of personal data within the agreed training topic. Omitting any of these elements will result in the training not fulfilling its role, because some people will not be trained at all or the training participants will not receive full knowledge in a given area. The consequence of the above may be a violation of the protection of personal data, as in the case being the subject of these proceedings. Moreover, the lack of training in the manner described above means that this security measure in practice does not reduce the risk of personal data breaches, which undoubtedly contributes to the weakening of the level of personal data protection and determines the need to recognize a violation of the provisions of Regulation 2016/679 relating to administrator's obligations in the field of data security. It should also be remembered that training will not replace technical solutions. It should also be pointed out that before the personal data protection breach occurred, training in the field of personal data protection was conducted only in 2018. Referring to the considerations made above, it should be pointed out

that the issues related to the protection of personal data are constantly changing (e.g. new types of threats will appear having a significant impact on the possibility of a breach of personal data protection, the legal order regulating issues related to generally understood security in the data processing process is also changing, etc.). What's more, the administrator regularly conducts training in the subject matter in question, which allows him to check the knowledge of employees in this area. The above gives the basis for the statement that, firstly, the employees employed at the City and Commune Office of Warsaw did not have updated knowledge on the protection of personal data, secondly, the Administrator did not know whether the employees were properly trained in the discussed area and had the knowledge to them to process their data in a way that ensures their appropriate security.

The result of the Administrator's inaction in this regard, as indicated above, was the materialization of a threat in the form of making an unauthorized copy of documents containing personal data from a computer located at the Administrator's headquarters to a portable data carrier (USB stick), over which the Administrator had no control, which resulted in a violation of the confidentiality of personal data processed by the Mayor.

It should be noted here that only after finding a personal data breach, the Mayor took adequate actions to avoid a future breach of personal data protection, the possibility of which is related to the use of portable data carriers. First of all, it should be pointed out that after the event, the Administrator conducted a risk analysis taking into account the process of processing personal data using, among others, portable storage media, which indicates that "(...) confidentiality threats include: (...) - unauthorized transfer of information containing personal data to another medium, - loss of a medium containing personal data, (...) - unauthorized removal of personal data contained on electronic medium (…)".

The analysis in question also indicates threats in the field of accountability. The administrator indicates that these threats include: "(...) lack of control over files created as part of the processing of data subject to a breach in the scope of their copying, saving and deletion, (...)".

The risk analysis, which was carried out after finding a breach of personal data protection, is proof that the Administrator correctly recognized the consequences of the lack of appropriate safeguards for the processing of personal data in the situation where the use of portable storage media was allowed. In the analysis in question, the administrator indicated the conclusions drawn: "(...) the above the analysis carried out for the data covered by the breach and all possible threats gave a full picture of what to pay special attention to in the unit, what additional security measures to apply and allows for the creation

of a well-functioning security policy [data protection regulations] of the existing IT system in which personal data is processed. In addition, it also facilitates the creation of appropriate documentation (…)".

The mayor also indicated that he had taken a number of actions to introduce appropriate safeguards in the process of processing personal data in order to increase the level of security. According to the submitted "Schedule (...) of (...) May 2022 at the City and Commune Office of W.", the Administrator, among others planned to introduce measures preventing the making of unauthorized copies of documents located on network drives and local workstations. A network access blockade has also been introduced. At the same time, the Administrator indicated that "(...) after analyzing the use of storage media in the departments of the City Hall and the Commune of Warsaw, it was decided that introducing a measure in the form of blocking ports is impossible due to the frequent use of external media for authorization and customer service (...)" . In addition, the Administrator (...) of May 2022 introduced the "Procedure (...)". According to this document "(...) Each carrier used in the ICT environment of the City and Commune of Warsaw, excluding CDs and DVDs, should have a unique inventory number allowing it to be associated with an individual user or a role played in a given ICT system (...) Subject to sec. 3 and 4, in the ICT environment of the City and Commune Office of W. it is possible to use only carriers owned by the employer (...) In justified cases, the mayor may consent to the use of other carriers than those specified in sec. 1, in particular for the purposes of photographic, training or test documentation (…) In the event of a need for a one-time data transfer from a carrier other than specified in sec. 2 and 3 to the ICT environment of the City and Commune Office of W., the user is obliged to ask an IT specialist to check this medium with updated anti-virus software and perform data transfer (...) In the ICT environment of the City and Commune of Warsaw, it is forbidden to use media owned by users, and in particular performing activities consisting in copying, copying files, mounting, disassembling devices, uploading, downloading software and data in order to transfer or copy information from the employer's ICT equipment to media owned by users (...)".

It should also be noted that the Mayor took additional steps to train all authorized persons at the City Hall and Municipality of W. To sum up, it should be pointed out that the Administrator, after the occurrence of a personal data breach, took a number of actions to adapt personal data processing operations to the provisions of the Regulation 2016/679 in order to ensure adequate security of personal data being processed, including in the process of processing personal data in connection with the use of portable storage media (e.g. USB memory) in this process. Taking these actions, due to the fact that it took place after the breach of personal data protection, does not, however, relieve him of responsibility for the violation of the provisions of

Regulation 2016/679 indicated in this decision.

In the absence of the Administrator's use of adequate technical measures to minimize the risk of breaching the security of data processed using portable data carriers (e.g. USB memory), in particular if this carrier was owned by an employee, it should be stated that before the personal data breach occurred, the Mayor did not ensured an appropriate level of protection of data processed using them. This determines the Administrator's failure to implement appropriate technical measures during the processing of personal data, so that the processing is carried out in accordance with Regulation 2016/679 and in order to provide the processing with the necessary safeguards, which he was obliged to do in accordance with art. 24 sec. 1 and 25 sec. 1 of Regulation 2016/679, as well as the failure to use technical measures to ensure a level of security corresponding to the risk of violating the rights or freedoms of natural persons by ensuring the ability to continuously ensure confidentiality, integrity, availability and resilience of systems and processing services, which is required by the data controller in art. 32 sec. 1 lit. b) of Regulation 2016/679, and taking into account the risk associated with the processing of personal data referred to in art. 32 sec. 2 of Regulation 2016/679, and consequently also of a violation of the confidentiality principle expressed in art. 5 sec. 1 lit. f) Regulation 2016/679, the above-mentioned the rules are detailed. The consequence of the Administrator's violation of the confidentiality principle is the violation of the accountability principle referred to in art. 5 sec. 2 of Regulation 2016/679.

Based on Article. 58 sec. 2 lit. i) of Regulation 2016/679, each supervisory authority has the power to apply, in addition to or instead of other corrective measures provided for in art. 58 sec. 2 lit. a) - h) and point. j) of this Regulation, an administrative fine under Art. 83 of Regulation 2016/679, depending on the circumstances of a particular case. Taking into account the findings of fact, the President of the Personal Data Protection Office, using the powers vested in him specified in the above-mentioned provision of Regulation 2016/679, stated that in the case under consideration there were premises justifying the imposition of an administrative fine on the Mayor of the City and Municipality of W.

In accordance with art. 83 sec. 4 lit. a) of Regulation 2016/679, violation of the provisions on the obligations of the administrator and the processing entity referred to in art. 8, 11, 25-39 as well as 42 and 43 are subject in accordance with sec. 2, 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 applicable.

In accordance with art. 83 sec. 5 lit. a) of Regulation 2016/679, violation of the provisions on the basic principles of processing, including the conditions of consent, referred to in art. 5, 6, 7 and 9 are subject to, in accordance with sec. 2, an administrative

fine of up to EUR 20,000,000, and in the case of an enterprise - up to 4% of its total annual worldwide turnover from the previous financial year, with the higher amount applicable.

Article 83 sec. 3 of Regulation 2016/679, on the other hand, provides that if the controller or processor intentionally or unintentionally violates several provisions of this regulation as part of the same or related processing operations, the total amount of the administrative fine does not exceed the amount of the penalty for the most serious infringement.

In the present case, the administrative fine against the Mayor was imposed for violation of Art. 25 sec. 1 and art. 32 sec. 1 and 2 of Regulation 2016/679 on the basis of the above-mentioned art. 83 sec. 4 lit. a) of Regulation 2016/679, while for violation of Art. 5 sec. 1 lit. f) and art. 5 sec. 2 of Regulation 2016/679 - pursuant to art. 83 sec. 5 lit. (a) of this Regulation. At the same time, the penalty imposed on the Mayor jointly for violating all the above provisions - pursuant to the provision of Art. 83 sec. 3 of Regulation 2016/679 - does not exceed the amount of the fine for the most serious violation found in this case, i.e. violation of Art. 5 sec. 1 lit. f) and art. 5 sec. 2 of Regulation 2016/679, which, pursuant to Art. 83 sec. 5 lit. a) of Regulation 2016/679 is subject to an administrative fine of up to EUR 20,000,000, and in the case of an enterprise - up to 4% of its total annual worldwide turnover from the previous financial year.

When deciding to impose an administrative fine, the President of the UODO - pursuant to Art. 83 sec. 2 lit. a) - k) of Regulation 2016/679 - took into account the following circumstances of the case, which make it necessary to apply this type of sanction in this case and have an aggravating effect on the amount of the imposed administrative fine:

1. The nature, gravity and duration of the infringement, taking into account the nature, scope or purpose of the given processing, the number of data subjects affected and the extent of the damage suffered by them (Article 83(2)(a) of Regulation 2016/679). in this case, a violation of the provisions on the protection of personal data, which resulted in the possibility of obtaining unauthorized access to the data processed by the Mayor by an unauthorized person or persons, and consequently the possibility of obtaining personal data of persons that were contained in documents (related to the performance of public administration tasks) copied unjustifiably by an employee to a portable storage medium, is of considerable importance and serious nature, as it poses a high risk of negative legal consequences for an exactly undetermined, potentially large number of people (the Administrator indicated that the breach concerns about 250 people), whose data could be accessed by a person or unauthorized persons. The Mayor's violation of the obligations to apply measures to protect the processed data against disclosure to unauthorized persons entails not only the potential, but also the real possibility of using these data by third parties

without the knowledge and against the will of the data subjects, contrary to the provisions of Regulation 2016/679 e.g. in order to establish legal relations or incur liabilities on behalf of the persons whose data was obtained. At this point, it needs to be emphasized that the Mayor, as the executive body of the local government (municipality), is obliged to apply higher standards, in particular with regard to the security of the processed data.

The long duration of the infringement of the provisions of Regulation 2016/679 should also be emphasized, as it should be assumed that the infringement began on May 25, 2018, i.e. on the date of application of Regulation 2016/679, and ended (…) in May 2022. Although the unauthorized use of a portable storage medium by an employee of the City and Commune Office of Warsaw took place (...) in May 2022, which showed the lack of adequate security measures, the Administrator was obliged to adapt the data processing processes to the the requirements of Regulation 2016/679.

In the present case, there is no evidence that persons whose data was accessed by an unauthorized person or persons suffered material damage. Nevertheless, the mere breach of confidentiality of their data constitutes non-pecuniary damage (harm) to them; natural persons whose data was obtained in an unauthorized manner may at least feel fear of losing control over their personal data, identity theft or identity fraud, discrimination, or finally financial loss. In addition, public notice to individuals does not guarantee that the information has reached every person it should reach. Thus, a situation could have arisen in which persons affected by the breach, having no knowledge of the breach, could not take action to ensure at least a minimum sense of security by increasing caution in using their own personal data.

2. Unintentional nature of the breach (Article 83(2)(b) of Regulation 2016/679). The controller was aware that if personal data processing was allowed with the use of computer equipment enabling the connection of portable data carriers (in particular USB memory sticks), including private portable data carriers, should process personal data in such a way as to ensure their appropriate security, including protection against unauthorized or unlawful processing, using appropriate technical and organizational measures, and thus in such a way as to ensure compliance with the principle " integrity and confidentiality" expressed in art. 5 sec. 1 lit. f) Regulation 2016/679. The mayor, due to the scope of the Office's activities, was aware of the frequent use of portable data carriers for authorization and customer service. It should therefore provide for the possibility of breaching the protection of personal data through the unauthorized use of this type of data carrier. Despite the adopted practice of using portable data carriers, the Administrator did not conduct a risk analysis in the scope covered by the breach. Only after the personal data protection breach occurred, the Mayor took specific technical and organizational steps, such as

conducting a risk analysis, introducing the "Procedure (...)" and measures preventing the making of unauthorized copies of documents located on network drives and local workstations. The Administrator's activities showed awareness of the lack of ensuring an adequate level of security of personal data processed using portable data carriers (e.g. USB memory), in particular when this carrier is not owned by the Administrator. In the case in question, the Mayor could have foreseen that the adopted solutions would not ensure an adequate level of personal data security, which would constitute a violation of the provisions on the protection of personal data. Thus, he unintentionally violated the provisions on the protection of personal data - art. 5 sec. 1 li. f) Regulation 2016/679 in connection with joke. 24 sec. 1, 25 sec. 1, 32 sec. 1 and 2 of Regulation 2016/679 and, consequently, also art. 5 sec. 2 of Regulation 2016/679.

Taking into account the findings in the case being the subject of this decision, it should be stated that the Administrator has committed negligence resulting in a breach of data confidentiality. Thus, this is an important circumstance affecting the amount of the administrative penalty.

3. Categories of personal data affected by the breach (Article 83(2)(g) of Regulation 2016/679). The personal data on the portable storage medium did not belong to the special categories of personal data referred to in Art. 9 of Regulation 2016/679, however, their scope, i.e. surnames and first names, date of birth, bank account number, address of residence or stay, PESEL registration number, other (information on settlements of fees for rent, water, sewage, electricity, rental of premises ) is associated with a high risk of violating the rights or freedoms of natural persons affected by the violation. It should be emphasized that, in particular, unauthorized disclosure of such categories of data as the PESEL registration number together with the name and surname that uniquely identify a natural person may have a real and negative impact on the protection of the rights or freedoms of that person. As indicated by the Provincial Administrative Court in Warsaw in the judgment of July 1, 2022, file ref. act II SA/Wa 4143.21 "In the event of a breach of such data as name, surname and PESEL number, identity theft or falsification is possible, resulting in negative consequences for the data subjects." It should be pointed out that the PESEL registration number, i.e. an eleven-digit numeric symbol, uniquely identifying a natural person, containing, among others, date of birth and gender designation, and thus closely related to the private sphere of a natural person and also subject, as a national identification number, to exceptional protection under Art. 87 of Regulation 2016/679, is data of a special nature and requires such special protection.

When determining the amount of the administrative fine, the President of the UODO took into account, as a mitigating

circumstance, having an impact on reducing the amount of the fine imposed, the good cooperation of the Administrator with the supervisory authority undertaken and carried out in order to remove the infringement and mitigate its possible negative effects [art. 83 sec. 2 lit. f) Regulation 2016/679]. It should be pointed out here that, apart from the proper fulfillment of the Mayor's procedural obligations during the administrative proceedings, which ended with the issuance of this decision, the Mayor fully implemented the recommendations of the President of the UODO regarding supplementing the notification of data subjects about the breach. The mayor also took specific and quick actions, which resulted in removing the possibility of recurrence of the violation. In particular, the Administrator removed the susceptibility to a violation of the protection of personal data being processed by introducing the recording of portable memory. In addition, the Mayor introduced a ban on the use of private portable storage media by employees of the City and Municipality of Warsaw, in particular a ban on copying, copying files, assembling, disassembling devices, uploading, downloading software and data in order to transfer or copy information from the employer's ICT equipment to carriers owned by users.

The fact that the President of the Personal Data Protection Office applied sanctions in the form of an administrative fine to the Mayor in this case, as well as its amount, was not affected by other ones indicated in art. 83 sec. 2 of Regulation 2016/679 circumstances, that is:

1. Actions taken to minimize the damage suffered by data subjects (Article 83(2)(c) of Regulation 2016/679). In this case, no damage was found on the part of the person affected by the breach, therefore The administrator was not obliged to take any action to minimize them.

2. 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). In the Guidelines of the Data Protection Working Party of Article 29 adopted on October 3, 2017 on the application and determination of administrative fines for the purposes of Regulation No. 2016/679 indicated that - considering this premise - "the supervisory authority must answer the question to what extent the controller <did everything that could be expected>, given the nature, purposes or scope of processing and in the light of the obligations imposed on it by ordinance".

The President of the UODO stated in this case that the Mayor violated the provisions of art. 25 sec. 1, art. 32 sec. 1 and 2 of Regulation 2016/679. In his opinion, the administrator bears a high degree of responsibility for failure to implement appropriate technical and organizational measures that would prevent a breach of personal data protection. It is obvious that in the

considered context of the nature, purpose and scope of personal data processing, the Administrator did not "did everything that could be expected of him"; thus did not comply with the provisions of Art. 25 and 32 of Regulation 2016/679 obligations.
In the present case, however, this circumstance determines the essence of the infringement itself; it is not merely a factor mitigating or aggravating its assessment. For this reason, the lack of appropriate technical and organizational measures referred to in Art. 25 and art. 32 of Regulation 2016/679, cannot be considered by the President of the UODO in this case as a circumstance that may additionally affect the stricter assessment of the infringement and the amount of the administrative fine imposed on the Mayor.
3. Any relevant previous violations by the controller or processor (Article 83(2)(e) of Regulation 2016/679). The President of the UODO has not found any previous violations of the provisions on the protection of personal data by the Administrator, therefore there are no grounds for treating this circumstance as aggravating. It is the duty of each administrator to comply with the law (including the protection of personal data), so the lack of previous violations cannot be a mitigating circumstance when imposing sanctions.
4. The manner in which the supervisory authority found out about the breach (Article 83(2)(h) of Regulation 2016/679). The President of the UODO found the breach as a result of reporting a breach of personal data protection made by the Administrator. When making this notification, the administrator only fulfilled the legal obligation imposed on him, there are no grounds to consider that this circumstance is a mitigating circumstance. In accordance with the Guidelines on the application and determination of administrative fines for the purposes of Regulation No. 2016/679 Wp. 253 "The supervisory authority may become aware of a breach as a result of proceedings, complaints, articles in the press, anonymous tips or notification by the data controller. Pursuant to the regulation, the controller is obliged to notify the supervisory authority of a breach of personal data protection. The mere fulfillment of this obligation by the controller cannot be interpreted as a mitigating factor.'
5. Compliance with the measures previously applied in the same case referred to in Art. 58 sec. 2 of Regulation 2016/679 (Article 83(2)(i) of Regulation 2016/679). Before issuing this decision, the President of the UODO did not apply any measures listed in art. 58 sec. 2 of Regulation 2016/679, therefore the controller was not required to take any actions related to their application, and which actions, subject to the assessment of the President of the UODO, could have an aggravating or mitigating impact on the assessment of the infringement found.
6. Application of approved codes of conduct under Art. 40 of Regulation 2016/679 or approved certification mechanisms under

Art. 42 of Regulation 2016/679 (Article 83(2)(j) of Regulation 2016/679). The mayor does not apply approved codes of conduct or approved certification mechanisms referred to in the provisions of Regulation 2016/679. However, their adoption, implementation and application is not - as stipulated in the provisions of Regulation 2016/679 - mandatory for controllers and processors in this connection, and therefore the circumstance of their non-application cannot be considered to the disadvantage of the Administrator in this case. In favor of the Administrator, however, the circumstance of adopting and using such instruments as measures guaranteeing a higher than standard level of protection of personal data being processed could be taken into account.

7. Financial benefits achieved directly or indirectly in connection with the infringement or losses avoided (Article 83(2)(k) of Regulation 2016/679). precipitate. Therefore, there are no grounds for treating this circumstance as incriminating the controller. The finding of measurable financial benefits resulting from the violation of the provisions of Regulation 2016/679 should be assessed definitely negatively. On the other hand, failure by the administrator to achieve such benefits, as a natural state, independent of the infringement and its effects, is a circumstance that, by nature, cannot be a mitigating factor for the Administrator. This is confirmed by the wording of Art. 83 sec. 2 lit. k) of Regulation 2016/679, which requires the supervisory authority to pay due attention to the benefits "achieved" - occurred on the part of the entity committing the infringement.

8. Other aggravating or mitigating factors (Article 83(2)(k) of Regulation 2016/679). The President of the UODO, examining the case comprehensively, did not notice any circumstances other than those described above that could affect the assessment of the infringement and the amount of the adjudicated administrative fine.

Taking into account all the circumstances discussed above, the President of the Office for Personal Data Protection decided that the imposition of an administrative fine on the Mayor is necessary and justified by the weight, nature and scope of the infringements alleged against the Mayor. It should be stated that the application of any other remedy provided for in Art. 58 sec. 2 of Regulation 2016/679, in particular, limiting oneself to a reminder (Article 58(2)(b)) would not be proportionate to the identified irregularities in the processing of personal data and would not guarantee that the Administrator will not commit further negligence in the future.

Referring to the amount of the administrative fine imposed on the Mayor, it should be noted that in the circumstances of this case - i.e. in view of finding a violation of several provisions of Regulation 2016/679, i.e. the principle of data confidentiality, expressed in art. 5 sec. 1 lit. f) of Regulation 2016/679, and reflected in the form of obligations set out in Art. 25 sec. 1, art. 32

sec. 1, art. 32 sec. 2 of Regulation 2016/679, and consequently also Art. 5 sec. 2 of Regulation 2016/679 (rules of accountability) and the fact that the Mayor is the authority of the public finance sector unit - Art. 102 of May 10, 2018 on the protection of personal data (Journal of Laws of 2019, item 1781), which limits the amount (up to PLN 100,000) of an administrative fine that may be imposed on a public finance sector entity.

In the opinion of the President of the UODO, the applied administrative fine meets the functions referred to in art. 83 sec. 1 of Regulation 2016/679, i.e. it will be effective, proportionate and dissuasive in this individual case.

In the opinion of the President of the UODO, the penalty imposed on the Mayor will be effective, because it will lead to a state in which the Mayor will apply such technical and organizational measures that will ensure a level of security for the processed data corresponding to the risk of violating the rights and freedoms of data subjects and the severity of the threats accompanying the processing of these personal data. The effectiveness of the penalty is therefore equivalent to a guarantee that the Mayor, from the moment of completion of these proceedings, will approach the requirements of the provisions on the protection of personal data with the utmost care.

The applied administrative fine is also proportional to the infringement found, in particular its weight, effect, the circle of affected natural persons and the high risk of negative consequences that they may suffer in connection with the infringement.

According to the President of the UODO, the administrative fine imposed on the Mayor will not constitute an excessive burden for him. The amount of the fine has been set at such a level that, on the one hand, it constitutes an adequate reaction of the supervisory authority to the degree of violation of the Administrator's obligations, but on the other hand, it does not cause a situation where the necessity to pay it will have negative consequences, in the form of a significant deterioration of the Administrator's financial situation . According to the President of UODO, the Mayor should and is able to bear the consequences of his negligence in the field of data protection, hence the imposition of a fine of PLN 10,000 (ten thousand zlotys) is fully justified.

In the opinion of the President of the UODO, the administrative fine will fulfill a repressive function in these specific circumstances, as it will be a response to the Mayor's violation of the provisions of Regulation 2016/679, but also a preventive one, as it will contribute to preventing future violations of the Administrator's obligations under the provisions on the protection personal data.

In the opinion of the President of the UODO, the fine imposed in the circumstances of this case meets the conditions referred

to in Art. 83 sec. 1 of Regulation 2016/679 due to the importance of the violations found in the context of the basic requirements and principles of Regulation 2016/679 - in particular the principle of confidentiality expressed in art. 5 sec. 1 lit. f) Regulation 2016/679.

The purpose of the imposed penalty is to ensure compliance by the Mayor with the provisions of Regulation 2016/679 in the future.

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

Print article

Metadata

Provider:

Inspection and Infringement Department

Produced information:

John Nowak

2023-05-09

Entered the information:

Wioletta Golanska

2023-06-06 09:34:49

Recently modified:

Edith Magziar

2023-06-15 10:20:51