Warsaw, on 02

November

2022

Decision

DKN.5131.8.2022

Based on Article. 104 § l of the Act of June 14, 1960 Code of Administrative Procedure (Journal of Laws of 2022, item 2000) in connection with Art. 7, art. 60 and art. 102 sec. 1 item 1 i sec. 3 of the Act of May 10, 2018 on the protection of personal data (Journal of Laws of 2019, item 1781) and art. 57 sec. 1 lit. a) and h) and Art. 58 sec. 2 lit. i) in connection with 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, as well as art. 83 sec. 1–3, art. 83 sec. 4 lit. a) and art. 83 sec. 5 lit. a) 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 regulations on data protection) (Official Journal of the EU L 119 of 4/05/2016, p. 1, 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 conducting administrative proceedings initiated ex officio regarding the violation of the provisions on the protection of personal data by the Head of the Dobrzyniewo Duże Commune (Dobrzyniewo Duże, ul. Białostocka 25), the President of the Personal Data Protection Office,

stating the violation by the Head of the Dobrzyniewo Duze Commune 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 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 EU Official Journal L 119 of May 4, 2016, p. 1, EU Official Journal L 127 of May 23, 2018, p. 2 and EU Official Journal L 74 of March 4, 2021, p. 35 .), hereinafter referred to as: "Regulation 2016/679", consisting in the processing of personal data in a manner that does not ensure adequate security of personal data, including protection against unauthorized or unlawful processing, using appropriate technical or organizational measures by failing to implement appropriate technical measures and organizational, and consequently, the inability to demonstrate compliance with the principle of "integrity and confidentiality", which constitutes a violation of the principle of "accountability" expressed in Art. 5 sec. 2 of Regulation 2016/679, imposes on the Mayor of the Dobrzyniewo Duże Commune 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 8,000 (say: eight thousand zlotys).

Justification

The Head of the Commune of Dobrzyniewo Duże (Dobrzyniewo Duże, ul. Białostocka 25), hereinafter also referred to as: the Head of the Commune or the Administrator, [...] of February 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 personal data protection O. members, which took place on [...] February 2022. The breach of personal data protection consisted in breaking into the employee's apartment and stealing a laptop with a file containing personal data of O. members. breach of personal data protection, there has been a loss of confidentiality of personal data of the above-mentioned people. The commune head determined the scale of the infringement, which showed that the stolen computer contained 51 records with personal data in the following areas: name and surname, address of residence or residence and PESEL registration number. The reported breach has been registered under reference [...].

By letter of [...] February 2022, the supervisory authority asked the Mayor of the Commune, among others about:

Providing information whether the stolen computer was private or business, and if private, whether the Administrator's procedures allow the use of private computers for business purposes and how the Administrator determines how they are secured and verifies the implementation of these security measures.

Providing information whether the Administrator has carried out a risk analysis taking into account the threat in the form of theft of computer equipment used to process personal data.

Providing information whether the Dobrzyniewo Duze Commune Office has implemented instructions on the use, transport and storage of portable computers containing personal data.

In the reply given in the letter of [...] February 2022, the Commune Head explained the following:

The stolen computer was a work computer.

The administrator regularly conducts a risk analysis. The risk analysis prepared on [...] December 2021, in line [...], provides for "Data loss threat Theft / loss of equipment and media outside the organization", which refers to the threat in the form of theft of computer equipment used to process personal data.

Regulations for the use of portable computers have been developed at the Commune Office in Dobrzyniewo Duzy, constituting Annex No. [...] to the Policy [...]. at the Dobrzyniewo Duże Commune Office, introduced by order No. [...] of the Commune

Head of [...] May 2018 on the introduction of the Policy at the Dobrzyniewo Duże Commune Office.

In addition, attached to the above-mentioned In writing, the Vogt of the municipality provided a risk analysis for 2021, rules for the use of laptop computers and a calculator of the weight of the infringement.

At the same time, the Commune Head informed that the administrator of the IT systems of the Commune Office in Dobrzyniewo Duzy submitted a written statement on February [...], 2022 that all business laptops used by the Administrator have cryptographic protection in the form of encrypted hard drives.

Then, on [...] February 2021, the President of the UODO asked the Head of the Commune for further explanations, i.e.:

Presentation of a detailed description of the adopted methodology for creating passwords as a means of securing access to computers, including a stolen computer, e.g. by indicating the adopted password complexity conditions, hash functions used and possible other solutions and their parameters (e.g. the salt used and its length).

Providing information whether the administrator has a copy of personal data lost as a result of computer theft.

In connection with the information provided in the letter of [...] February 2022 that "all company laptops used by the administrator have cryptographic protection in the form of encrypted hard drives", an indication of what function/program the disk of the stolen computer was encrypted with.

In the letter of [...] February 2022, which is a response to the above letter of the supervisory body, the commune head explained that:

Computers used by the administrator, including a stolen computer, have defined rules that force periodic changes of the password and password complexity. System […].

It has a copy of personal data lost as a result of computer theft.

The statement referred to in the letter of [...] February 2022 concerned the current state as at the date of submitting the statement. The hard drive of the stolen computer was not encrypted.

In connection with the submitted explanations, on February [...], 2022, the President of the UODO initiated administrative proceedings regarding the possible violation by the Commune Head, as the data controller, of the obligations under 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 the breach of the protection of personal data of O. members (sign. letter [...]).

In response to the initiation of administrative proceedings, in letters of February [...], March 2022 and August 2022, the Head of

the Commune provided information that he had implemented encryption of hard drives of portable computers used by the Administrator to process personal data and, that […] March 2022 a stolen laptop was found. The computer hardware was destroyed, but the computer disk was not damaged. The analysis of the Windows system logs showed that the computer's operating system had not been started since the day of the theft (no information about logging into the system).

Then, on [...] September 2022, the President of the UODO asked the Head of the Commune for further explanations, i.e. to indicate:

The reasons why the security measure in the form of hard disk encryption was not applied to the stolen computer.

Since when a stolen computer containing personal data subject to protection was released to an employee for use outside the workplace.

In the letter of [...] September 2022, which is a response to the above-mentioned letter of the supervisory body, the commune head explained that:

"Since the risk analysis was carried out, ASI successively encrypted the hard drives of portable computers used by the Administrator. However, the turn of the calendar year is associated with carrying out a number of works to prepare the office for the new calendar year (purchase and implementation of equipment, configuration of accounting programs and an electronic document circulation system). The computer owned by the employee was to be encrypted as soon as possible, but unfortunately it was stolen earlier. Currently, the stolen computer is with the Administrator. In connection with the ongoing explanatory proceedings, the drive is not encrypted and the equipment has been secured. Currently, all portable computers used by the Administrator are encrypted.

The computer was handed over to the employee [...] October 2011."

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:

In accordance with 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 the art, 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 importance 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 assessing 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 adequate, 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. Taking into account, in particular, the scope of personal data processed by the Mayor of the Commune using a stolen computer, 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 configuration of the operating systems used by regular testing, measuring and assessing the effectiveness of technical and organizational measures to ensure security 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.

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.

In the facts of the case in question, the risk concerned the threat of theft of company computer equipment from the private apartment of an employee of the Dobrzyniewo Duże Commune Office. As established, the the computer was protected against unauthorized access only with a password. In view of the above, it should be pointed out that with regard to portable computers taken outside the Administrator's organization, 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 the above-mentioned the provisions of Regulation 2016/679, is obliged to apply additional safeguards in the form of, for example, encryption of computer hard drives. These additional safeguards should be determined as a result of a risk analysis, after proper identification of threats to personal data processed using portable computers used outside the administrator's organization. According to the risk analysis presented by the Mayor of the Commune carried out [...] December 2021, the Administrator was aware of the risks associated with the loss of computer equipment taken outside his organization, because in the line [...] of the analysis he provided "Data loss risk Theft / loss of equipment and media outside the organization". Moreover, the Commune Head assessed this risk as unacceptable and specified, as part of the risk management method, the safeguards to be implemented in order to reduce it. Among the listed safeguards to reduce the level of risk, the commune head indicated, among others: "encryption of laptops (A, B)", but did not use them, at least on the computer that was stolen from the employee's private apartment and on which the personal data of O members were located. As he explained in the letter of [...] February 2022 ., "The stolen computer's disk was not encrypted." Therefore, the Commune Head, despite the correct identification in the risk analysis carried out in 2021 of threats to personal data processed using computers taken outside his organization, correct determination of the risk level for the above. data and defining the method of dealing with the risk by indicating the safeguards to be applied to reduce this risk, did not take any action to actually eliminate this risk or reduce it to an acceptable level. The effect of the Administrator's inaction in this regard was the materialization of the identified threat in the form of the theft of a company computer with personal data, on which appropriate security measures were not applied to

protect this data, which resulted in a violation of their confidentiality. As indicated by the Provincial Administrative Court in Warsaw in the justification of the judgment of August 26, 2020, file ref. II SA/Wa 2826/19, "This provision [art. 32 of Regulation 2016/679] does not require the data controller to implement any technical and organizational measures that are to constitute personal data protection measures, but requires the implementation of adequate measures. Such adequacy should be assessed in terms of the manner and purpose for which personal data are processed, but the risk associated with the processing of such personal data should also be taken into account, which risk may be of different levels.", as well as "The adopted measures are to be effective, in specific cases, some measures will have to be low-risk mitigation measures, others must be high-risk mitigation measures, but it is important that all measures (and each one separately) are adequate and proportionate to the degree of risk." The indicated Court made a similar statement in the judgment of September 3, 2020, file ref. II SA/Wa 2559/19, stating that "The consequence of such an orientation is the resignation from the list of security requirements imposed by the legislator in favor of self-selection of security measures based on threat analysis. The administrators are not provided with specific security measures and procedures. The administrator is to independently conduct a detailed analysis of the conducted data processing processes and perform a risk assessment, and then apply measures and procedures that will be adequate to the assessed risk." Moreover, the lack of implementation of the above-mentioned of the security measure constitutes the Administrator's failure to comply with its own security rules, i.e. the "Regulations [...]", constituting Annex No. [...] to the Policy [...] in the Dobrzyniewo Duże Commune Office, introduced by order No. [...] of the Commune Head of [...] of May 2018 on the introduction of the Policy [...] in the Commune Office of Dobrzyniewo Duże. In point [...] above. In the case of storing personal data or the Employer's secret on a portable computer, the User is obliged to store them on an encrypted disk, secured at least (...). It should be emphasized that the indicated documentation was introduced by the Administrator on [...] May 2018, so already at the time of application of Regulation 2016/679 he was aware of the need to apply this type of measure to ensure the security of personal data processed using portable computer equipment. However, its implementation took place only after the breach of personal data protection in question occurred, because according to the submitted statement, from [...] February 2022 "all company laptops used by the administrator have cryptographic protection in the form of encrypted hard drives". The above was also pointed out by the Provincial Administrative Court in Warsaw, which in its judgment of January 19, 2021, file ref. II SA/Wa 702/20, argued that "(...) the data controller should properly protect personal data against their accidental loss using appropriate technical and organizational measures. Personal data should be

processed in a manner that ensures their appropriate security and appropriate confidentiality, including protection against unauthorized access to them and the equipment used for their processing and against unauthorized use of these data and equipment (recital 39 of Regulation 2016/679)" .

Explaining the reasons for the lack of ensuring an adequate level of security for personal data processed on the stolen computer, the commune head in a letter of September 2022 indicated "a number of works preparing the office for the new calendar year", after which he intended to encrypt the hard drive of the computer in question. For obvious reasons, the above circumstance cannot be an excuse for breaching the provisions on the protection of personal data. In addition, bearing in mind that the works indicated by the Administrator are not extraordinary duties (purchase and implementation of equipment, configuration of accounting programs and the electronic document circulation system), and encrypting the computer's hard drive does not require excessive forces and resources, this is an expression of disregard for the provisions on the protection personal data in favor of other autonomous obligations.

Therefore, the findings made do not give grounds to conclude that the technical measures used by the Head of the Commune to ensure the security of personal data were adequate to the state of technical knowledge, implementation costs and the nature, scope, context and purposes of processing, which consequently did not ensure effective implementation of the principles of protection data, including ensuring the confidentiality of data processed on company laptops taken outside the Administrator's organization.

Only after the violation, the Commune Head took action to avoid similar events in the future by encrypting the hard drives of portable computers owned by the Administrator. In connection with the above, it should be noted that if the Head of the Commune had complied with the results of his own risk analysis and the method of dealing with risk specified therein, and with the provisions of the "Regulations [...]", the personal data protection could not have been violated and the loss of confidentiality of data of members of O. This assessment is not changed by the fact that a stolen mobile device was found on [...] March 2022 and the fact that, according to the explanations of the Mayor of the Commune, "Analysis of system C logs showed that the computer's operating system had not been started since the day of the theft (no information about logging into the system)". At the moment when the personal data protection breach was found, the risk of violating the rights or freedoms of natural persons was high, due in particular to the scope of personal data processed using a stolen laptop and the lack of implementation of adequate security measures on it to ensure the protection of this data.

In the absence of the data controller's use of adequate technical measures to minimize the risk of violating the security of data processed using a laptop taken outside the Administrator's organization, it should be concluded that the commune head did not ensure 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. As indicated by the Provincial Administrative Court in Warsaw in the judgment of August 26, 2020, file ref. II SA/Wa 2826/19 "(...) 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." 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 Office for Personal Data Protection, 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 Head of the Commune.

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).

After conducting administrative proceedings, the President of the UODO found a violation of the basic processing principles set out in Art. 5 sec. 1 lit. f) and Art. 5 sec. 2 of Regulation 2016/679, the category of which, according to their nature, was defined in Art. 83 sec. 5 of Regulation 2016/679. In view of the above, the nature of the violation of the provisions on the protection of personal data is serious, classified into the category of provisions whose violation is subject to the highest possible administrative fine - up to EUR 20,000,000.

Also, the number of injured people is not small, as it covered 51 people, and the duration of the infringement, i.e. from May 25, 2018 (date of application of Regulation 2016/679) to February […], 2022 (date of the administrator's statement that " all company laptops used by the administrator have cryptographic protection in the form of encrypted hard drives") of the provisions on the protection of personal data, in which the administrator did not ensure that the processing was carried out in a way that ensures adequate security of personal data, including protection against unauthorized or unlawful processing, by appropriate technical or organizational means, was significant.

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

The commune head was aware of how he should process personal data on laptop computers issued to employees to ensure their adequate security, including protection against unauthorized or unlawful processing, using appropriate technical and organizational measures, and thus how to comply with the principle " integrity and confidentiality" expressed in art. 5 sec. 1 li. f) Regulation 2016/679. At the same time, it did not apply the security measures it specified in the risk analysis, i.e. hard drive encryption, and did not comply with the rules specified by it, ordering the use of this security measure, set out in the "Regulations [...]". The administrator's actions showed awareness of the lack of ensuring an adequate level of security for personal data processed on a portable computer. The justification for the lack of encryption of the hard drive of the stolen computer was a number of other obligations to be performed, not related to the protection of personal data. However, adequate protection of the computer was to take place after the fulfillment of these obligations. In view of the above, the Commune Head could have foreseen that during this period he would not ensure an adequate level of security of personal data processed on the computer, 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 in the form of 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 Commune Administrator committed negligence resulting in a breach of data confidentiality. Thus, this is an important circumstance affecting the amount of the administrative penalty.

3. The degree of responsibility of the administrator, taking into account the technical and organizational measures implemented by him pursuant to art. 25 and 32 (Article 83(2)(d) of Regulation 2016/679) - The administrator, based on the factors listed in Art. 25 sec. 1 and 32 sec. 1 of Regulation 2016/679 conducted an analysis and determined the risk of a threat in the form of computer theft and determined an appropriate technical security measure in the form of computer hard drive encryption. In addition, he developed a procedure ("Regulations […]"), which precisely required the encryption of computer hard drives. However, the facts of the case show that the hard drive of the stolen computer was not encrypted. The above constitutes the lack of implementation of technical and organizational measures pursuant to art. 25 and 32 of Regulation 2016/679, and thus the lack of ensuring an appropriate level of security.

4. Categories of personal data affected by the breach (Article 83(2)(g) of Regulation 2016/679) - The personal data on the stolen computer did not belong to the special categories of personal data referred to in Art. 9 of Regulation 2016/679, however, their scope, i.e. name and surname, address of residence or residence and PESEL number, 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, ref. no. 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."

When determining the amount of the administrative fine imposed on the Administrator, the President of the UODO took into account the following premises as mitigating circumstances:

1. Actions taken to minimize the damage suffered by data subjects (Article 83(2)(c) of Regulation 2016/679) - Immediately after the disclosure of the personal data protection breach, the Head of the Commune informed the Police about the theft. On March

[...], 2022, the stolen computer was found, and the analysis of system C logs carried out by the Administrator showed no information about logging into the system, which, in the opinion of the Administrator, proves that the computer's operating system has not been started since the theft. Thus, on the basis of the indicated circumstances, there are also no grounds to believe that the data subjects have suffered any damage as a result of this breach.

2. Any relevant previous violations by the controller or processor (Article 83(2)(e) of Regulation 2016/679) - no relevant previous violations of Regulation 2016/679 by the Commune Head were found.

3. The degree of cooperation with the supervisory authority to remove the infringement and mitigate its possible negative effects (Article 83(2)(f) of Regulation 2016/679) - In the course of the proceedings, the Head of the Commune sent explanations and gave clear, specific answers within the prescribed period.

4. Any other aggravating or mitigating factors applicable to the circumstances of the case, achieved directly or indirectly in connection with the infringement, financial benefits or losses avoided (Article 83(2)(k) of Regulation 2016/679) -

The President of the UODO did not state in the course of these proceedings that by committing an infringement punishable by the Commune Head, he achieved any financial benefits or avoided any financial losses. Even though the administrator violated Art. 32 sec. 1 of Regulation 2016/679 due to the lack of implementation of appropriate technical and organizational measures, however, based on the elements indicated in this provision, the Administrator made the necessary assessments and drew appropriate conclusions, because he conducted a risk analysis and determined appropriate security measures to ensure a level of security corresponding to the risk, which proves that Art. 32 sec. 1 of Regulation 2016/679 has not been completely disregarded. The above could not be indifferent to the determination of the penalty and was assessed as a mitigating circumstance. The Head of the Commune also took a number of corrective actions to minimize the risk of recurrence of the breach (change of procedures, implementation of encryption of hard drives of portable computers).

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

1. 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 by the Head of the Commune. 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.'

2. 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) - in this case, the measures referred to in Art. 58 sec. 2 of Regulation 2016/679.

3. 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 Commune Head does not apply approved codes of conduct or approved certification mechanisms referred to in the provisions of Regulation 2016/679.

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 Commune Head is necessary and justified by the weight, nature and scope of the violations alleged against the Commune Head. 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 itself to a warning (Article 58(2)(b)) would not be proportionate to the identified irregularities in the processing of personal data and would not guarantee that the Head of the Commune will not commit further negligence in the future .

Referring to the amount of the administrative fine imposed on the Head of the Commune, the President of the Personal Data Protection Office decided that in the circumstances of this case - i.e. in view of finding a violation of several provisions of Regulation 2016/679 (principle of data confidentiality, expressed in Article 5(1)(a) f), and reflected in the form of the obligations set out in Art. 25 sec. 1, art. 32 sec. 1, art. 32 sec. 2 of Regulation 2016/679, and consequently also (rules of accountability) Art. 5 sec. 2 of Regulation 2016/679 and the fact that the Commune Head 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 Commune Head will be effective, because it will lead

to a state in which the Commune Head will apply such technical and organizational measures that will ensure the level of security of the processed data corresponding to the risk of violating the rights and freedoms of data subjects and the severity of the threats accompanying the processes processing of this personal data. The effectiveness of the penalty is therefore equivalent to the guarantee that the Head of the Commune, 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 violation found, in particular its weight, effect, the circle of affected individuals and the high risk of negative consequences that they may suffer in connection with the violation. According to the President of the UODO, the administrative fine imposed on the Head of the Commune 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 infringement 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 the UODO, the Commune Head should and is able to bear the consequences of his negligence in the sphere of data protection, hence the imposition of a fine of PLN 8,000 (eight 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 violation of the provisions of Regulation 2016/679 by the Mayor of the Municipality, but also preventive, as it will contribute to preventing future violations of the obligations of the Mayor of the Municipality resulting from the provisions about personal data protection.

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 that the Mayor of the Commune will comply 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.

Metadata

Provider:

Inspection and Infringement Department

Produced information:

Wioletta Golanska

2022-11-02

Entered the information:

Edith Magziar

2023-01-09 14:01:00

Recently modified:

Edith Magziar

2023-01-09 14:18:52