THE CHAIRMAN OF PERSONAL DATA PROTECTION

Warsaw, 01

June

2022

DECISION

DKN.5131.2.2022

Based on Article. 104 § of the Act of June 14, 1960, Code of Administrative Procedure (Journal of Laws of 2021, item 735, as amended) in connection with Art. 7 sec. 1 and art. 60 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 it. a) and h) and art. 58 sec. 2 it. b) in connection with Art. 5 sec. 1 it. 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) (Journal of Laws UE 119 of May 4, 2016, p. 1, Journal of Laws UE 127 of May 23, 2018, p. 2 and EU Official Journal 74 of March 4, 2021, p. 35) , after conducting administrative proceedings initiated ex officio on the processing of personal data by the Municipal Social Assistance Center in O., President of the Office for Personal Data Protection

finding a violation by the Municipal Social Welfare Center in O. of the provisions of Art. 5 sec. 1 it. 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) (Journal of Laws UE 119 of May 4, 2016, p. 1, Journal of Laws UE 127 of May 23, 2018, p. 2 and EU Official Journal 74 of March 4, 2021, p. 35) , hereinafter: Regulation 2016/679, consisting in the failure of the Municipal Social Assistance Center in O. to apply appropriate organizational measures ensuring a level of security corresponding to the risk of data processing using portable storage media, including protection against unauthorized or unlawful processing and accidental loss, destruction or damage, which resulted in the loss by an employee of the Municipal Social Welfare Center in O. regularly testing, measuring and evaluating the effectiveness of organizational measures to ensure the security of processing, gives the Municipal Social Welfare Center in O. a warning.

JUSTIFICATION

On [...] June 2021, the President of the Personal Data Protection Office, hereinafter referred to as the President of the Personal Data Protection Office, received an initial notification of a personal data breach made by the Municipal Social Assistance Center in O. (hereinafter: MOPS in O. or administrator), registered under the reference number [...], informing about a breach of personal data protection by 50 people, i.e. employees of the administrator and charges of MOPS in O., including children, in terms of names and surnames, parents' names, dates of birth, addresses of residence or stay, PESEL registration numbers and health data. The incident constituting the subject of the notification took place at an unspecified time and consisted in the loss of an unencrypted external USB flash drive (hereinafter referred to as a portable memory device) by an employee of MOPS in O. The administrator was notified about the event by the President of UODO in a letter of [...] June 2021. , no. [...], in which the administrator was informed about the transfer by an anonymous person to the Office for Personal Data Protection of the found external USB flash drive with personal data.

Due to the scope of the disclosed personal data, the indicated breach resulted in a high risk of violating the rights or freedoms of natural persons. In view of the above, the controller informed in the supplementary notification of [...] August 2021 that on [...] June 2021 it had notified data subjects of the breach of their personal data, increasing the number of persons affected by the breach from 50 to 200. 55 persons affected by the infringement were notified individually by means of correspondence sent via the postal operator Poczta Polska S.A., while the remaining persons were notified by means of a message published on the websites of MOPS in O. at the addresses: […] and […].

In connection with the notification of a breach of personal data protection, in a letter of [...] August 2021, the President of the Personal Data Protection Office requested the controller to notify persons again about the breach of their personal data in order to provide them with all the required information, in accordance with Art. 34 of the Regulation 2016/679, and to provide explanations, including, inter alia, about:

Providing information on whether it was established, when and how the portable storage medium containing personal data was lost.

Indication whether a procedure has been developed specifying the rules for the use, storage, transport and protection of portable memory devices used by MOPS in O ..

Providing information on how the compliance with the rules described in the above-mentioned procedure was verified by the administrator's employees.

Providing information on whether it was permissible for the administrator's employees to use private storage media by the administrator's employees before the breach of personal data protection, and if so, on what terms.

Indication of whether the administrator has carried out a risk analysis taking into account the risks related to the loss of the portable storage medium and the use of private storage media by the administrator's employees.

In response to the above-mentioned the letter, the administrator on [...] September 2021, in the letter with reference number [...], informed that:

It has not been established when and how the portable storage medium containing personal data was lost.

The MOPS in O. defines the rules for securing portable storage media, which are included in the Personal Data Protection Policy of the Municipal Social Welfare Center in O.

Verification of compliance with the principles of securing portable memory devices took place during checks made by the IT Systems Administrator and the Data Protection Inspector.

In MOPS in O. it is forbidden to use private storage media by employees.

The administrator carried out a risk analysis in this respect (the analysis was attached to the letter of […] September 2022).

In connection with the presented explanations, in a letter of [...] and November 2021, the President of the Personal Data Protection Office asked the controller to provide additional explanations, i.e. about:

Presentation of written evidence of the conducted verification of compliance by MOPS employees in O. with the provisions of the personal data protection policy regarding the use of portable storage media for the processing of personal data, including their protection.

Specification whether the verification covered the person who lost the removable storage medium.

Clear confirmation that the lost medium was a private medium.

Indication whether training courses for employees of MOPS in O. in the field of personal data protection were carried out, along with the dates of these training and their program.

Clarification whether the person responsible for the breach of personal data protection has been issued a company portable memory device.

In response to the above-mentioned a letter from the supervisory authority, the controller, in a letter of [...] and November 2021, no. [...], explained that:

He does not have written evidence of the conducted verification of compliance by MOPS employees in O. with the provisions of the personal data protection policy regarding the use of portable storage media for the processing of personal data, including their protection.

The verification also covered the person who lost the portable storage medium.

The lost medium is a private medium belonging to an administrator's employee.

Due to the finding of a data protection breach, on [...] June 2021, training on "Personal Data Security" was carried out at the Family Assistants Team. In addition, taking into account the current state of the epidemic caused by the SARS-CoV-2 virus, employees of MOPS in O. were provided with training materials in the following scope: "Basic violations - what must not be done with personal data" and "Personal data protection - responsibility". In addition, in December 2021, online training courses for the administrator's employees in the field of personal data protection are planned.

The person responsible for the breach of personal data protection has been handed an official flash drive.

Then, in connection with the presented explanations, in a letter of [...] December 2021, the President of the Personal Data Protection Office (UODO) addressed the administrator, inter alia, about:

Indication whether the settings of IT systems in MOPS in O. block the possibility of saving data on unregistered media.

Description of the applied technical measures (including cryptographic) regarding the equipment (e.g. aptop, flash drive) taken outside the MOPS area in O.

How the administrator monitored the use of portable data carriers in his organization.

Has the recommended use of devices enabling content encryption been implemented in the organization, and if not, why was this security measure abandoned?

Did the employee responsible for the breach notify his superior about the incident, as referred to in § 18 para. 2 of the Personal Data Protection Policy, and if not, why and whether any professional consequences have been incurred against him.

Are the controller's employees (including the person who contributed to the violation) familiar with the provisions of the Personal Data Protection Policy.

How was compliance with security measures in the administrator's organization monitored, including the developed and implemented procedures (in accordance with the information provided that "in the administrator's organization a Personal Data Protection Policy has been developed and implemented, hereinafter referred to as" policy ". The above-mentioned document

describes in detail the issue of identifying incidents and violations in the organization (§ [...] - § [...] policy) and securing portable data carriers (§ [...] policy) ”.

Indication of the reasons for which the personal data was stored on a private storage medium (bearing in mind the information that: "in accordance with § [...] section 2 of the Data Protection Policy, ASI ensures with the use of available tools that only registered media are allowed for official use For this purpose, it has the right to block communication of any unregistered devices with the ICT resources of MOPS ”).

In response to the above-mentioned the administrator's letter on [...] December 2021, in the letter with reference number [...], explained that:

Settings of IT systems in MOPS in O. block the possibility of saving data on unregistered media, attaching as proof a print screen of anti-virus software settings [...] along with a message about the impossibility of installing an unregistered device.

The following technical measures were applied regarding the equipment taken outside the area of personal data processing: antivirus software [...] with automatic software update is loaded on the laptops, access to the computer's operating system requires authentication by selecting a user name and entering an access password, computer hardware settings make it impossible to the use of an unregistered data carrier, the computer user is not assigned the administrator role, and thus there is no possibility of unauthorized installation of the software. As for portable data carriers (flash drives), which do not have encryption software built in, MOPS employees in O. are obliged to encrypt files containing personal data by using software for this purpose […] or by encrypting a document in the program […].

In connection with the recommendation contained in the risk analysis of [...] December 2020, MOPS in O. implemented the use of devices enabling the encryption of their content. Verification of the use of portable storage media in accordance with the provisions of the Data Protection Policy was performed during checks carried out by the IT Systems Administrator and the Data Protection Officer.

The employee responsible for the incident did not fulfill the obligation specified in § 18 section 2 of the Data Protection Policy, i.e. he did not notify his superior about the incident. The employee's lack of reaction was due to his ignorance of the loss of his portable data carrier. Due to the non-compliance with the provisions of the Data Protection Policy, the employee who contributed to the incident was deprived of the possibility of receiving a cash bonus in December 2021. the employee was removed from the function of the coordinator of the Team of Family Assistants.

Employees of MOPS in O. (including the person who contributed to the occurrence of the violation) were familiarized with the provisions of the applicable Personal Data Protection Policy. Compliance with the implemented security measures, including the developed and implemented procedures, was verified during checks carried out by the IT Systems Administrator and the Data Protection Officer.

Despite the implementation in MOPS in O. of the communication blockade of all unregistered devices with ICT resources, the probable reason for saving data on a private medium was the possibility of downloading them from the official mail.

Due to the above, on [...] January 2022, the supervisory body initiated ex officio administrative proceedings, due to the possibility of the Municipal Social Assistance Center in O., as the data controller, breaching the obligations under Art. 5 sec. 1 it. 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 personal data protection (ref. [...]). Moreover, the President of the Personal Data Protection Office called MOPS in O. to provide further explanations:

Has the administrator determined whether the work mail was received on the private computer equipment of the employee.

Do the procedures adopted by the Administrator allow such a possibility, and if so, what are the technical and organizational measures used to secure data processing on private computer equipment?

In response, the administrator, in a letter of [...] January 2022, No. employee's computer equipment.

Then, in the course of the pending administrative proceedings in the above-mentioned on the matter, the supervisory authority asked the administrator on [...] March 2022 for additional explanations:

In connection with the information contained in the letter of [...] January 2022 that "the procedures adopted in the Municipal Social Welfare Center in O. do not allow the possibility of receiving official mail on the employee's private computer equipment", how MOPS in O. verifies compliance with them.

Can MOPS employees in O. use private equipment while performing their official duties, and if so, who is responsible for the configuration and protection of this equipment?

How was it determined that the data saved on the lost private storage medium was retrieved from the official mail on the private computer of the MOPS employee in O ...

By letter of [...] April 2022, no. [...], being a reply to the above-mentioned letter, the controller indicated the following:

The method of using e-mail by employees of MOPS in O. is specified in § 28 of the Policy for the Protection of Personal Data

of the Municipal Social Assistance Center in O.

Employees of MOPS in O. cannot use private equipment while performing their official duties.

Information about downloading data from the company mail on a private computer was obtained from the employee who owned the lost media.

Due to the submitted explanations, the President of the Personal Data Protection Office (UODO) requested on [...] April 2022 for additional explanations:

Was the reasons for which the MOPS employee in O. copied the data to a private storage medium been established, and if so, whether it was for private or business purposes?

Has MOPS in O. implemented a system that allows you to monitor business e-mail, informing the administrator in particular about opening e-mails on private computer equipment and about copying data (data files) processed as part of business e-mail.

Sending written evidence that the person guilty of the violation was familiarized with "the provisions of the Personal Data Protection Policy in force at the Center" and evidence confirming that "Compliance with the implemented security measures, including the developed and implemented procedures, was verified during checks carried out by the IT Systems Administrator and the Data Protection Officer ", together with an indication of the number of checks and the dates in which they were carried out.

About the number and dates of training courses in the field of personal data protection, including training on the principles of using portable storage media and business e-mail, before the occurrence of a personal data breach, along with the presentation of written evidence for their conduct, indication of their detailed scope (possibly an indication of that the thematic scope of the abovementioned trainings covered the scope specified in the letter of [...] November 2021) and with the demonstration that the employee responsible for the infringement took part in each such training.

By letter of [...] May 2022, no. [...], the controller indicated the following:

On the basis of the information obtained from the employee responsible for the infringement, it was found that the reason for copying the data to a private storage medium was damage to the corporate storage medium, about which the administrator was not notified. The information obtained from the employee shows that the activity referred to above was performed solely for business purposes.

MOPS in O. has not implemented a system allowing for the monitoring of business e-mail, informing the administrator, among others on opening electronic messages on private computer equipment and on copying data (data files) processed as part of business e-mail.

In terms of compliance with the rules of use, storage, transport and protection of portable memory devices used by MOPS in O., three checks were carried out with the participation of the IT Systems Administrator and the Data Protection Inspector. The first check took place in the period from [...] .10.2019 to [...] .10.2019, the second check took place in the period from [...] .06.2020 to [...] .06.2020 and the third check was place in the period from […] .01.2021 to […] .01.2021

Before the breach of personal data protection, two training sessions were organized at the Municipal Office of O. for employees of MOPS in O. Only one of the training sessions was attended by the employee who was guilty of the breach. In addition, MOPS in O. held ongoing training for the administrator's employees in the field of personal data protection, including the rules of using portable storage media and business e-mail, the number and timing of which depended on the needs reported by the managers of individual organizational units. PUG.

In addition, in the attachment to the above-mentioned of the letter, the administrator sent a scan of the statement of the employee responsible for the infringement on reading the provisions on the protection of personal data, including the Personal Data Protection Policy in force at MOPS.

Therefore, by letter of [...] May 2022, the supervisory authority asked the controller to:

Indication of the date of submission by the person guilty of violation of the "Employee's statement on reading the provisions on the protection of personal data".

Provision of written evidence for "three checks with the participation of the IT Systems Administrator and the Data Protection Inspector. The first check took place in the period from [...] .10.2019. until [...] .10.2019, the second check took place in the period from [...] .06.2020. until [...] .06.2020 and the third check took place in the period from [...] .01.2021. until [...] .01.2021 ".

Provision of information on the training program conducted by the Municipal Office of O. and indication of the training in which the person responsible for the infringement participated.

Provision of information on a detailed training program in the field of personal data protection, including the rules of using portable storage media and business e-mail, conducted by MOPS in O. and indication of whether the person responsible for the breach of personal data protection participated in them, along with the dates of these trainings.

In response, the administrator, by letter of [...] May 2022, [...], explained the following:

It is not able to determine the exact date of the submission by the person guilty of violating the declaration of familiarization with the provisions on the protection of personal data.

He does not have written evidence that three checks were carried out with the participation of the IT System Administrator and the Data Protection Inspector in the field of compliance with the rules of use, storage, transport and securing of portable storage devices used by the Municipal Social Welfare Center in O.

The person responsible for the infringement participated in the training organized at the O. City Hall on [...] May 2018, which was confirmed by her signature on her actual presence at position 82.

The rules of using portable memory devices and business e-mail have been discussed, among others during trainings organized at the Municipal Office of O. on [...] .05.2018 and on [...] .04.2019 when discussing the principle of "integrity and confidentiality" referred to in Art. 5 sec. 1 it. f) Regulation 2016/679.

Attached to the above-mentioned of the letter, the administrator provided a presentation on training organized at the Municipal Office of O. for employees of MOPS in O. on [...] .05.2018 and on [...] .04.2019.

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

Article 5 of Regulation 2016/679 sets out the rules for the processing of personal data that must be respected by all administrators, i.e. entities designated by EU law or the law of a Member State and entities that independently or jointly with others determine the purposes and methods of personal data processing. Pursuant to Art. 5 sec. 1 it. f) of Regulation 2016/679, personal data must be processed in a manner ensuring adequate security of personal data, including protection against unauthorized or unlawful processing and accidental loss, destruction or damage, by appropriate technical or organizational measures ("integrity and confidentiality "). Pursuant to Art. 5 sec. 2 of Regulation 2016/679, the controller is responsible for compliance with the provisions of para. 1 and must be able to demonstrate compliance with them ("accountability").

Pursuant to Art. 24 sec. 1 of 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 of varying probability and seriousness, the controller implements appropriate technical and organizational measures to ensure that the processing is carried out in accordance with

this Regulation and to be able to demonstrate it . These measures are reviewed and updated as necessary.

The provision of art. 24 sec. 1 of Regulation 2016/679 specifies the basic and main obligations of the administrator, who is charged with the implementation of appropriate technical and organizational measures to ensure the compliance of processing with the requirements of Regulation 2016/679. This is, in particular, about the implementation of the principles set out in Art. 5 sec. 1 of Regulation 2016/679.

However, according 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 violation of the rights or freedoms of natural persons with different probabilities and severity of risks resulting from processing, the controller both in determining the methods of processing and in during the processing itself - implements appropriate technical and organizational measures, such as pseudonymisation, designed to effectively implement data protection principles, such as data minimization, and to provide the processing with the necessary safeguards to meet the requirements of the regulation and protect the rights of data subjects (taking data protection into account in the design phase).

Pursuant to Art. 32 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, the controller and the processor implement appropriate technical and organizational measures to ensure the level of security corresponding to this risk, including, inter alia, the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services (point b), as appropriate, and regular testing, measurement and evaluation of the effectiveness of technical and organizational measures to ensure the security of processing (letter d).

Pursuant to Art. 32 sec. 2 of Regulation 2016/679, the controller, when assessing whether the level of security is appropriate, takes into account in particular the risk associated with the processing, in particular resulting from accidental or unlawful destruction, loss, modification, unauthorized disclosure or unauthorized access to personal data sent, stored or otherwise processed.

The provisions of Art. 25 sec. 1 and art. 32 sec. 1 and 2 of Regulation 2016/679, along with art. 24 sec. 1 above of the regulation, thus constitute a specification of the provisions referred to in Art. 5 sec. 1 it. f) Regulation 2016/679, the principles of integrity and confidentiality.

Data confidentiality is a property that ensures, in particular, that data will not be disclosed to unauthorized entities, obtained, inter alia, through the use of technical and organizational measures, adequate to the scope of the data, the context of processing and identified risks. The indicated principle, as follows from the established facts, was violated by MOPS in O. by the administrator's failure to implement adequate organizational measures to ensure the security of personal data processing and the lack of verification of compliance with personal data protection procedures by the administrator's employees, which as a result of loss by the administrator an employee of MOPS in O. private storage medium containing personal data, resulted in a breach of personal data protection and, as a consequence, allowing unauthorized persons to access personal data processed on this medium. As it was established, the above-mentioned the carrier did not have any security to protect it and the personal data processed on it against unauthorized access.

As indicated by the Provincial Administrative Court in Warsaw in the judgment of 3 September 2020, file number II SA / Wa 2559/19, "Regulation 2016/679 introduced an approach in which risk management is the foundation of activities related to the protection of personal data and is a continuous process. . Entities processing personal data are obliged not only to ensure compliance with the guidelines of the above-mentioned of the regulation through a one-off implementation of organizational and technical security measures, but also to ensure the continuity of monitoring the level of threats and ensuring accountability in terms of the level and adequacy of the introduced security. This means that it becomes necessary 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 personal data processing mechanisms used. The administrator is to independently carry out a detailed analysis of the data processing processes carried out and assess the risk, and then apply such measures and procedures that will be adequate to the assessed risk.

The consequence of this orientation is the resignation of the existing security requirements imposed by the legislator, in favor of the independent selection of security measures based on the analysis of threats. Administrators are not informed about specific security measures and procedures. The administrator is to independently carry out a detailed analysis of the data processing processes carried out and assess the risk, and then apply such measures and procedures that will be adequate to the assessed risk ".

In the context of the above-mentioned judgment, it should be noted that the starting point for the correct determination and selection of technical and organizational measures aimed at ensuring the security of the processed data and reducing the risks

associated with this processing to an acceptable level is the risk analysis correctly carried out by the administrator. The performed risk analysis should be documented and justified on the basis of, first of all, determination of the actual state at the time of its performance. In particular, the characteristics of the processes involved, assets, vulnerabilities, threats and existing safeguards as part of the ongoing processes of personal data processing should be taken into account. The scope and nature of personal data processed in the course of activities carried out by the data controller cannot be overlooked during this process, 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.

As indicated by the administrator in the conclusions of the risk analysis of [...] December 2020 (document called "Risk analysis for resources processing personal data: Portable Data Carriers"), in the case of portable storage media, "[...] there is an average probability of violation of the rights and freedoms of persons whose personal data are processed using this resource ". In addition, it was indicated that "[...] it is recommended to monitor the media used by employees [...] on an ongoing basis" and "[...] to use data media containing embedded encryption software [...]".

The "Risk analysis for resources processing personal data: Portable Data Media" submitted to the supervisory authority shows that the administrator has identified the risk of "using private data carriers for business use" and has defined measures to mitigate this risk. As part of the above activities, MOPS in O. provided, in particular, "the lack of possibility to connect an unregistered data carrier to the device" and "training of employees in the encryption of data stored on portable data carriers", and introduced "a ban on the use of private data carriers". Despite the security measures defined in this way, the collected evidence shows that not all of them were implemented. While there is no doubt as to the method of applying the measure in the form of blocking the possibility of connecting private storage media to business computer equipment, the remaining ones have not been properly implemented. The findings show that, prior to the breach of personal data protection, the administrator conducted two trainings for its employees, organized at the Municipal Office of O. on [...] May 2018 and [...] April 2019, including only one of them, carried out on [...] May 2018, the person responsible for the personal data breach took part. Moreover, the presentation documenting the training program attached to the administrator's letter of [...] May 2022, No. [...] shows that it was of a general nature, informing only about the nature of the obligations arising from the application of the provisions of Regulation 2016/679. Subsequent trainings for MOPS employees in O. were conducted only after the breach of personal data protection occurred, which clearly indicates that this measure to ensure the security of data processing was not

carried out correctly. It should also be noted that the "Risk analysis for resources processing personal data: Portable Data Media" was prepared on [...] December 2020, and the decision to conduct training in the use of portable storage media and related risks was made only after breach of personal data protection, i.e. after [...] June 2021. Doubts may also arise from the narrowing of the scope of the training described in the above-mentioned analysis only for the encryption of data saved on portable storage media, excluding the risks associated with the use of, for example, private storage media and regulations adopted in this regard by the administrator in the "Personal Data Protection Policy of the Municipal Social Welfare Center in O.", constituting an appendix to the regulation No. [...] of the Director of the Municipal Social Welfare Center in O. of [...] May 2018. It can therefore be assumed that MOPS in O. before the occurrence of a personal data breach did not provide its employees with basic knowledge about the rules of using mobile of storage media and proceedings in the event of, for example, damage to the official portable storage medium issued to them, which is also confirmed by the administrator's explanations in the letter of [...] May 2022, No. [...] that "the reason for copying data to a private storage medium was damage official storage medium of which the Administrator has not been notified ".

In the submitted explanations, the administrator indicated that the rules for the use of portable storage media were described in the "Personal Data Protection Policy of the Municipal Social Welfare Center in O." and that all employees, including the person responsible for the breach of personal data protection, are familiar with the above-mentioned document. The "Employee's statement on reading the provisions on the protection of personal data" presented by the administrator, which also includes a reference to the above-mentioned regulation, signed by the person guilty of the infringement, was not dated, which does not allow for verification when this document was signed by that person and, consequently, has he actually acquainted himself with the above-mentioned regulations against breach of personal data protection.

Therefore, the above findings clearly indicate that in this respect the administrator has not implemented effective organizational measures to ensure the security of personal data processed using portable storage media, despite, which should be emphasized once again, the risk analysis includes the identified threat in the form of private use for business use. storage media. 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 reminding and, consequently, consolidation of the rules for the processing of personal data covered by the training. In addition, such training must be attended by all persons authorized to process personal data, and the training itself must cover all issues related to the processing of personal data within the

agreed training topic. If one of these elements is omitted, the training will not fulfill its role, because some people will not be trained at all or the training participants will not receive full knowledge in a given field. The consequence of the above may be a breach of personal data protection, as in the case being the subject of this proceeding. Moreover, the lack of training in the manner described above means that this security measure, despite its indication in the risk analysis as a risk mitigating measure, in practice does not reduce this risk, which undoubtedly contributes to the weakening of the level of personal data protection and determines the need to recognize breach of the provisions of Regulation 2016/679 relating to the administrator's obligations in the field of data security. As already indicated, before the breach of personal data protection, the employee guilty of the breach of personal data protection participated only in one training in the field of personal data protection, which focused on general issues related to the obligations arising from the provisions on the protection of personal data, and not on specific issues. regarding the security of personal data processing with the use of portable storage media. It should also be noted that the indicated training was conducted on [...] May 2018, i.e. before the adoption of the "Personal Data Protection Policy of the Municipal Social Welfare Center in O.", which defined the rules for the use of portable storage media.

In this context, it should be noted that the Provincial Administrative Court in Warsaw, in its judgment No. II SA / Wa 2826/19 of August 26, 2020, stated that "(...) actions of a technical and organizational nature are at the discretion of the data controller personal data, but may not be selected in a completely free and voluntary manner, without taking into account the degree of risk and the nature of the personal data protected ". Moreover, as the Provincial Administrative Court in Warsaw pointed out in the judgment No. II SA / Wa 2826/19 of August 26, 2020, "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 also the risk related to the processing of such personal data, which may vary in size, should be taken into account. (...) The adopted measures are to be effective, in specific cases some measures will have to be low-risk mitigating measures, others - must mitigate high risk, but it is important that all measures (and each separately) are adequate and proportional to the degree of risk ".

In addition, the administrator, in a letter of [...] and November 2021, No. personal data of portable storage media, including their protection ". It is true that in another letter (of [...] May 2022, No. [...], the administrator explained that "Referring to the checks on compliance with the rules of use, storage, transport and securing of portable memory devices used by the Municipal

Social Welfare Center in O. I would like to inform you that three checks were carried out in this respect with the participation of the IT Systems Administrator and the Data Protection Officer. The first check took place in the period from [...] .10.2019. to [...]. in the period from […] .06.2020. to [….] .06.2020 and the third check took place in the period from […] .01.2021 to […] .01.2021 ", however requested to provide evidence of the execution of the above-mentioned checks, he informed that "he does not have written evidence of three checks with the participation of the IT Systems Administrator and the Data Protection Officer in the field of compliance with the rules of use, storage, transport and securing transfers. other storage devices used by the Municipal Social Welfare Center in O. ".

In connection with the above, it should be noted that the verification of compliance by employees with the provisions of the "Policy for the Protection of Personal Data of the Municipal Social Welfare Center in O.", including provisions relating to the use of portable storage media, is an element of regular testing, measuring and evaluating the effectiveness of organizational measures to ensure the security of personal data processing, to which the administrator is obliged pursuant to art. 32 sec. 1 it. d) Regulation 2016/679. It should also be indicated that the administrator has not introduced any mechanisms for testing, measuring and assessing the knowledge of MOPS employees in the O. in the scope of the training provided, in order to check whether the employees understood the content of the material provided and are aware of the risks related to the use of portable storage media and the risks associated with related.

In connection with the above, it should be emphasized that in order to properly meet the requirement specified in Art. 32 sec. 1 it. d) of Regulation 2016/679, indicated in the above-mentioned judgment of the Provincial Administrative Court in Warsaw as the obligation to ensure the continuity of monitoring the level of threats and ensuring accountability in terms of the level and adequacy of the implemented security measures, the administrator should regularly test, measure and evaluate the effectiveness of the technical and organizational measures applied to ensure the security of processing. Regular testing, measuring and assessing the effectiveness of technical and organizational measures to ensure the security of processing is the basic duty of every controller and processor resulting not only from Art. 32 sec. 1 it. d) of Regulation 2016/679, but also from the fact that during the implementation of individual processing activities, new or previously unknown risks for the security of this processing may appear or arise. The administrator is therefore obliged to verify both the selection and the level of effectiveness of the technical and organizational measures used at each stage of processing. The comprehensiveness of this verification should be assessed through the prism of adequacy to risks and proportionality in relation to the state of technical

knowledge, implementation costs and the nature, scope, context and purposes of processing. On the other hand, the lack of verification of compliance by employees of MOPS in O. with the rules for the processing of personal data adopted by the administrator, including those related to the use of portable storage media, deprives the administrator of knowledge about essential elements of the personal data protection system, which in turn prevents the proper implementation of the obligation specified in Art. 32 sec. 1 it. d) Regulation 2016/679.

Moreover, that testing, measuring and evaluating the effectiveness of the adopted security measures should fulfill the requirement resulting from art. 32 sec. 1 it. d) of Regulation 2016/679, must be performed on a regular basis, which means consciously planning and organizing such activities in specific time intervals, regardless of e.g. changes in the organization and the course of data processing processes. It is also important to properly document (in connection with the principle of accountability referred to in Article 5 (2) of Regulation 2016/679) of these activities. Only then is the controller able to demonstrate that monitoring is carried out in this respect, formulate specific conclusions and present the proposed remedial measures. Documentation will also allow the comparison of actions taken in various time periods and solutions adopted in terms of their effectiveness in ensuring security for the personal data processed. In the present case, however, the administrator did not keep such documentation, which means that he did not demonstrate, in accordance with the above-mentioned principle of accountability, that he had effectively carried out such activities.

Lack of regular testing, measurement and evaluation by MOPS in O. of the effectiveness of the implemented organizational measures to ensure the security of processing and failure to implement in an effective manner organizational measures securing the processed personal data in the form of periodic training of the administrator's employees on the adopted rules for the processing of personal data using portable storage media, it has led, which should be emphasized again, not only to a breach of personal data protection, but also prejudices the breach by MOPS in O. of the obligations incumbent on the data controller, resulting from art. 24 sec. 1, art. 25 sec. 1, art. 32 sec. 1 and art. 32 sec. 2 of Regulation 2016/679, and consequently also the confidentiality principle expressed in Art. 5 sec. 1 it. f) Regulation 2016/679. The effect of violating the principle of confidentiality is the violation of Art. 5 sec. 2 of Regulation 2016/679. As indicated by the Voivodship Administrative Court in Warsaw in the judgment of May 10, 2021, file ref. II SA / Wa 2378/20, "The principle of accountability is therefore based on the legal responsibility of the controller for the proper fulfillment of obligations and imposes an obligation on him to demonstrate, both to the supervisory authority and the data subject, evidence of compliance with all data processing rules."

Similarly, the issue of the principle of accountability is 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 norms of Regulation 2016/679, it should be emphasized that the controller has considerable freedom in the scope of the applied safeguards, but at the same time is liable for violation of the provisions on the protection of personal data. The principle of accountability expressly implies that it is the data controller that should demonstrate and therefore prove that it complies with the provisions set out in Art. 5 sec. 1 of Regulation 2016/679 ".

In view of the above, acting pursuant to Art. 58 sec. 2 it. b) of Regulation 2016/679, according to which each supervisory authority has, in the scope of conducted proceedings, the right to issue a reminder to the controller or the processor, in the event of a breach of the provisions of this Regulation by processing operations, the President of the Personal Data Protection Office deems it justified to issue a reminder to the administrator in the scope of the breach of the provisions found art. 5 sec. 1 it. f), art. 5 sec. 2, art. 24 sec. 1, art. 25 sec. 1 and art. 32 sec. 1 and 2 of Regulation 2016/679.

Recital 148 of Regulation 2016/679 states that, in order for the enforcement of the Regulation to be more effective, infringements should be sanctioned, including administrative fines, in addition to or in place of the appropriate measures imposed by the supervisory authority under this Regulation. If the infringement is minor, the fine may be replaced by an admonition. However, due attention should be paid to the nature, gravity and duration of the breach, whether the breach was not intentional, the steps taken to minimize the harm, the degree of liability or any prior breach, how the supervisory authority became aware of on breach, on compliance with the measures imposed on the controller or processor, on the application of codes of conduct, and on any other aggravating or mitigating factors.

The President of the Personal Data Protection Office decided that, in the established circumstances of the present case, issuing a reminder to the administrator is a sufficient measure. The breach concerns a one-off event, and therefore we are not dealing with a systematic act of omission that would pose a serious threat to the rights or freedoms of persons whose personal data are processed by MOPS in O. The above circumstances justify issuing a warning to the administrator for the breach found, which will ensure also so that similar events do not occur in the future. Nevertheless, if a similar event repeats itself in the future, each admonition issued by the President of the Personal Data Protection Office against the controller will be taken into account when assessing the premises for a possible administrative fine, in accordance with the principles set out in Art. 83 sec. 2 of Regulation 2016/679.

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

2022-07-15