THE CHAIRMAN OF PERSONAL DATA PROTECTION

Warsaw, 23

June

2022

DECISION

DKN.5131.11.2022

Based on Article. 104 § 1 of the Act of 14 June 1960 Code of Administrative Procedure (Journal of Laws of 2021, item 735, as amended) in connection with Art. 7 and art. 60 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. b) 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 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 data) (Journal of Laws UE L 119 of 04/05/2016, p. 1, as amended), after carrying out an ex officio administrative procedure regarding the processing of personal data by the President of the City of O., President of the Office for Personal Data Protection,

finding a violation by the President of O. 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 data) (Journal of Laws UE L 119 of 04.05.2016, p. 1, as the effectiveness of technical and organizational measures to ensure the security of the processed personal data in the IT systems affected by the violation, in particular in terms of vulnerability, errors and their possible consequences for these systems and data processed with their use, reminds the Mayor of O.

Justification

The President of the City of O., hereinafter also referred to as the Administrator, on [...] October 2021, reported to the President of the Personal Data Protection Office (hereinafter also referred to as the "President of the Personal Data Protection Office") violations of the protection of personal data of employees, users, current and potential clients and clients of public entities of the Office The city of O., which most likely took place on [...] October 2021. The breach of personal data protection

consisted in breaking the security of the IT system and encrypting, using ransomware [...], three servers of the City of O., used to process personal data . As a consequence, the Administrator has been deprived of access to the above-mentioned the system and the personal data contained therein. The administrator determined the scale of the breach, which showed that the encrypted databases included about 50,000 personal data records in the scope including first and last name, parents' names, date of birth, bank account number, address of residence or stay, PESEL identification number, e-mail address , data on earnings and / or property, series and number of ID card, telephone number and maiden name of the mother. According to the notification of [...] October 2021, the Administrator did not find a high risk of violation of the rights or freedoms of natural persons, however, due to the loss of access to personal data, it issued a public message notifying data subjects of a breach of the protection of their personal data . The case was registered under the reference number […].

In connection with the above infringement, by letters of [...] October, [...] November, [...] December 2021 and [...] January, [...] February and [...] February 2022, the supervisory authority asked the Administrator to .in. for additional explanations regarding the above-mentioned events:

1) Did the administrator conduct an internal investigation in connection with the reported breach of personal data protection, which allowed to determine how the data was encrypted by malicious software; what were the circumstances, source and reasons for the violation; whether the data was encrypted through a breach of security or as a result of human error (e.g. phishing). 2) How long was the restriction of access to the IT systems affected by the breach, after what time they were restored, and whether all the data encrypted as a result of the breach was restored? malware actions; what actions have been taken by the administrator for this purpose, as well as an explanation, in connection with the information provided in the notification of a personal data breach, that "The backup disk array has been damaged in recent weeks and work is underway to restore its efficiency", what impact on the time and effectiveness of data recovery from backups had the above-mentioned problems and an indication of how the "IT specialist supervises the correctness of NAS and portable drive backups." 4) Has the administrator determined the scale of the resulting breach of data protection in terms of the number of computer workstations and servers that were encrypted by malicious software? 5) Whether and if so, how did the administrator regularly test, measure and assessing the effectiveness of technical and organizational measures to ensure the security of personal data processed in the IT systems affected by the infringement, in particular in terms of vulnerability, errors and their possible consequences for these systems, and the actions taken to minimize the risk of their occurrence. 6) How the administrator has

applied technical and organizational measures to minimize the risk of recurrence of such violations in the future; in particular, demonstration of the differences in the applied security of the network infrastructure before and after the personal data breach. 7) What was the server software installed before the breach of personal data protection, including information on why the servers had software without manufacturer support installed, i.e .: [...] and […] and without the main manufacturer support, ie […]. 8) Has a risk analysis been carried out, including the analysis performed before the personal data breach and the analysis performed after the incident, as well as the methodology for carrying out the risk analysis. a procedure for making backups at the Municipal Office was developed. 10) Was there training of employees of the Municipal Office in the field of cybersecurity and the use of social engineering (phishing) tools. 11) Was the backups also encrypted with ransomware?

In response, the Administrator informed by letters of [...] November and [...] December 2021 and [...] January, [...] February, [...] February and [...] February 2022 that:

1) An internal investigation was carried out that showed no breach of anti-virus, firewall, or known CVE vulnerabilities in the edge router. In addition, an external audit of the incident was commissioned to an independent entity, which most likely indicated the source of the attack, which was the electronic device for issuing keys (e-caretaker). The device had an embedded operating system […] (without updating) and was connected to an IT network. The device was also encrypted.2) The restriction of data availability lasted from [...] October 2021 to [...] November 2021. All data encrypted from system backups and paper documentation were successfully restored.3) According to the ransomware specification [...]. it should be assumed that the attackers obtained the ability to copy the data to their servers in order to try to decompile them in the specifications appropriate for databases, which is not the same as the possibility of their easy reading or modification. 4) Three database servers with a file server service and a control module were encrypted mechanism of the e-caretaker system. 5) In the Municipal Office of O. the processing of personal data, including work on database systems, takes place internally. No data is made available externally and the Office does not expose its services to suppliers / partners outside. The IT department supervises the processes of updating antivirus systems, firewall and making a backup on an ongoing basis. Permanent, regular application of system security tests by the internal IT department until the incident occurred was impossible due to staff shortages and restructuring of the IT department. over the keys in the Office; password-protected computers (computers in the Office are password-protected under the authorization mechanism, [...] entering the password is required automatically after a longer hardware inactivity); antivirus system. Each computer protected with anti-virus program [...], backup system for

workstations and servers (daily backup to NAS network drive is performed) .7) Technical and organizational measures additionally applied after the incident: dedicated VLAN for less secure systems, separate LAN zone without access to the main network and the Internet, dedicated, separate network shares on the NAS disk for servers (a copy of each server is sent to a separate resource with unique authorization), forced change of all passwords as part of the password policy - changed passwords for all accounts, including administrative accounts .8) The servers had software [...], [...], [...] and [...]. 9) Server backups (with the content of files and databases) are created in an automated manner based on the use of the software function of the server, backups are also prepared for documentation stored on users' workstations in a selected directory (e.g. in cat alogu C: / Documents), incremental copies are made every day at 6.00 p.m., and full copies are made once a month. 12 monthly copies are kept for a year (the oldest copies are overwritten in a rotation cycle). Copies are made on a dedicated NAS server. Every month, a copy of the NAS is backed up to a removable drive and stored in a safe in the IT chief's room. The IT specialist supervises the correctness of NAS and removable backups. The destruction of disks with copies is carried out in a commission commission, and the media are destroyed by physical destruction, cutting after removing from the housing. 10) Cybersecurity training for employees of the City Hall of O. was conducted on [...] November 2021.11) from five disks in Synology mode, where 2 disks were logically damaged without affecting the backup process. However, during the recovery, the array had to be fully repaired with the manufacturer's mechanisms (replacement of two problematic disks), which, due to the total capacity of 7TB, took less than 5 days. The entire operation had no impact on restoring data from backups that were restored correctly.12) Backup testing is performed within the scope of the IT specialist's job responsibilities, using the built-in backup mechanism [...]. The correctness of the backup process is based on fully unpacking the backup from the portable drive / NAS once every six months. Due to the incident, however, all logs confirming the correctness of these operations were lost.13) [...] was the operating system for an independent key issuing device (e-caretaker). In the case of server systems [...], in 2021 the Office obtained funds for the purchase of new servers and licenses, however, due to staff shortages, it was only in September that the process of migrating the entire IT environment of the Office to the current version 2019/2021 [...] including virtualization and SQL databases.14) Backups are made to unmapped NAS shares using unique credentials, therefore the backups have not been encrypted.15) Due to the increased risk level for the threat "Unauthorized access to data during storage" in the risk analysis carried out in Appendix No. 3 to the letter of [...] November 2021. The administrator indicated what additional security measures have been implemented to reduce it, i.e .: change of the backup execution, measurement and

testing procedure, upgraded versions of server operating systems to the 2019/2021 version, the level of functionality was increased [...] 2019/2021, shutdown and withdrawal from use of the e-caretaker system, d setting up and testing an additional backup replication matrix (from the NAS matrix) - the second matrix is located in a different location. In addition, communication between devices takes place in a separate, closed subnetwork (VLAN) without any access from the internal and external network.

Attached to the letter of [...] November 2021, the Controller provided a risk analysis carried out before a personal data breach (of [...] February 2021) and a risk analysis carried out after a personal data breach (of [...] October 2021).

In connection with the reported breach of personal data protection and explanations provided by the Administrator of the above-mentioned in letters, the President of the Personal Data Protection Office on [...] March 2022 initiated ex officio administrative proceedings regarding the possibility of violation by the Mayor of O., as the data controller, of the obligations arising from the provisions of Regulation 2016/679, i.e. 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 personal data protection reported by the Mayor of O. (letter reference [...]).

After the initiation of the administrative procedure, by letters of [...] March 2022 and [...] and [...] May 2022, the supervisory authority asked the Administrator to provide additional explanations, including:

1) Does the Administrator currently regularly test, measure and evaluate the effectiveness of technical and organizational measures affecting the security of personal data being processed? of the attack, a tool called [...] was used, which is a component of the above-mentioned software, causing files to be sent to another location, which would result in the loss of confidentiality of personal data. 3) Did the Administrator contact the operator providing Internet access services, whether there was an unjustified collection of data from the Municipal Office in O. directly before the attack or during its duration (eg whether the size of the data transfer did not differ from the standard). 4) Whether the Administrator had purchased the extended support service [...] (valid until [...] October 2023) before the personal data breach occurred.

In response, the Administrator informed by letters of [...] March 2022, [...] May 2022 and [...] June 2022 that:

1) Currently, it regularly tests, measures and assesses the effectiveness of technical and organizational measures affecting the security of personal data processed by the Mayor of O. to the systems of the Municipal Office of O. He also pointed out that the module [...] does not automatically, automatically send data to an external location, however, it allows data to be

transferred in an encrypted form via the http protocol. After completing its operation, this module removes the traces of operation. In the administrator's opinion, this mechanism did not work properly due to the parameters of the infected host, both hardware and software-related. 3) The amount of data transfer, both before and during the incident, did not differ from the standard one. 4) Did not have purchased extended service support […].

In this factual state, after reviewing all the evidence gathered in the case, the President of the Personal Data Protection Office considered the following:

Pursuant to Art. 34 of the Act of May 10, 2018 on the Protection of Personal Data (Journal of Laws of 2019, item 1781) - hereinafter: the Act of May 10, 2018, the President of the Personal Data Protection Office is the competent authority for data protection and supervisory within the meaning of Regulation 2016/679. Pursuant to Art. 57 sec. 1 lit. (a) and (h) of Regulation 2016/679, without prejudice to the other tasks set out under that Regulation, each supervisory authority on its territory shall monitor and enforce the application of this Regulation; conduct proceedings for breaches of this Regulation, including on the basis of information received from another supervisory authority or other public authority.

Art. 5 of Regulation 2016/679 lays down rules regarding the processing of personal data that must be respected by all administrators, i.e. entities that independently or jointly with others determine the purposes and methods of personal data processing. Pursuant to Art. 5 sec. 1 lit. 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 ("confidentiality and integrity "). 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"). Specification of the confidentiality principle referred to in Art. 5 sec. 1 lit. f) of Regulation 2016/679, constitute further provisions of this legal act. 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 violation of the rights or freedoms of natural persons of varying probability and seriousness, the controller implements appropriate technical and organizational measures for the processing to be carried out in accordance with this Regulation and to be able to demonstrate it . These measures are reviewed and updated as necessary.

In accordance with Art. 25 sec. 1 of Regulation 2016/679, taking into account the state of technical knowledge, the cost of implementation and the nature, scope, context and purposes of processing as well as the risk of violating the rights or

freedoms of natural persons with different probabilities and severity resulting from the processing, the controller - both in determining the methods of processing and 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 this Regulation and protect the rights of persons whose data relate to.

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 a different probability of occurrence and the severity of the threat. The provision specifies that when deciding on technical and organizational measures, the state of technical knowledge, implementation cost, 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. It follows from the above-mentioned provision 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 related to the processing of personal data, taking into account the criteria set out 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 the level of security corresponding to this risk. These arrangements should, where appropriate, include measures such as the 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 of personal data in the event of a physical incident. or technical, and regularly testing, measuring and evaluating the effectiveness of technical and organizational measures to ensure the security of processing. Pursuant to Art. 32 sec. 2 of Regulation 2016/679, the administrator, when assessing whether the level of security is appropriate, takes into account in particular the risk related to 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.

As indicated in 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 of varying probability 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 aforementioned provisions

detail the principle of confidentiality 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 O., in order to properly fulfill the obligations imposed on the above-mentioned the provisions of Regulation 2016/679, the Administrator was obliged to take actions ensuring an appropriate level of data protection by implementing appropriate technical and organizational measures, as well as activities aimed at the optimal configuration of the operating systems used by regularly 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 conducted risk analysis, in which the 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 the processed data, as specified, inter alia, in Art. 32 sec. 1 of Regulation 2016/679. This provision introduces a risk-based approach, indicating at the same time the criteria on the basis of which the controller should select appropriate technical and organizational measures to ensure the level of security corresponding to this risk. In addition to the risk of violating the rights or freedoms of natural persons, it is therefore necessary to take into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing. As indicated by the Provincial Administrative Court in Warsaw in its judgment of September 3, 2020, file ref. 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 conduct 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 such an orientation is the resignation from the lists of 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 perform a risk assessment, and then apply such measures and procedures that will be adequate to the assessed risk. "

In the facts of the case at hand, the risk related to the threat of data encryption by malware encrypting ransomware. One of the methods to prevent such attacks is the effective management of possible vulnerabilities as well as ongoing analysis and detection of weak points in the ICT infrastructure. The basis of security is in particular the use of up-to-date software for all elements of the ICT infrastructure.

In the risk analysis presented by the Administrator, carried out before the personal data breach (on [...] February 2021), the risk of unauthorized access to data during storage was taken into account, including as "Unprotected access to databases or directories with files or to the cloud via the Internet (against hackers and malware)." For the above-mentioned the probability of its occurrence and its effect have been determined. The risk level was defined as the product of the probability and the effects of the occurrence of a given hazard. In addition, the Administrator indicated the security measures that were to be minimized by the identified threat by referring primarily to the instructions and procedures applicable in its organization, e.g. procedures for granting authorizations to process personal data and procedures for securing the IT system. One of these procedures, contained in the "Management Manual - [...] in the Municipal Office of O.", in the section "Protection against unauthorized access to the local network", with the purpose of using security measures described as securing IT systems against unauthorized access to the local network, e.g. by spyware and hackers, indicates that "The software of systems and applications is being updated (workstation operating systems / server operating systems / web browsers / Adobe / Flash / Java / others). The update is made in accordance with the manufacturers' recommendations and the market opinion regarding the security and stability of new versions (eg updates, service packs, patches) ". As part of the indicated security catalog, the Administrator did not provide for the replacement of operating systems or other systems used to process personal data that have already lost the support of their producer with systems that have such support. The obligation to ensure the use of systems supported by the manufacturer does not result from the instructions and procedures that the Administrator listed as measures to protect the processed personal data against the above-mentioned. a threat. Moreover, in the risk analysis itself,

the Administrator did not foresee the risk of using personal data without the support of the IT system manufacturer in the processing. Meanwhile, the findings show that it was through the operating system of the device for issuing keys (e-caretaker), ie […], which was not supported by the manufacturer, that the security breach by malicious software took place.

In particular, as indicated in the report on the "Audit of the ransomwere incident", prepared on [...] November 2021, "the electronic key keeper was also encrypted (...). It was a single station with a built-in computer based on […] (without any updates) without anti-virus system and protection. Officially known vulnerabilities and the possibility of taking control of the system [...] give hard grounds to assume that this is a probable explanation of the whole incident ". Further in the above-mentioned the report stressed that "This is where an attack was carried out on a domain controller with a functional level […]. This is another system that has been unsupported for a long time and has many vulnerabilities (...) ". The report also indicated the errors that contributed to the violation, i.e .: "connecting the e-janitor to the main LAN vlan of the O. City Hall (...)" and "when purchasing the e-janitor's solution, the product specification was not checked (you can was to force the manufacturer to update the operating system and install an anti-virus system) ".

In connection with the above, it should be pointed out that the use by the President of O. of the software without the manufacturer's support, i.e. [...], contributed to the materialization of the risk of a breach of personal data protection, as a result of which the security of the e-caretaker system used by The administrator to issue keys and then encrypt the data processed therein with the use of malicious software. As previously indicated, this device had an embedded operating system […] (not updated). What's more, as the Administrator's explanations show, this device was connected to an IT network, which caused other devices to be attacked, as a result of which there was a loss of access to personal data processed by the Mayor of O. It should be noted that the above-mentioned the system lost the producer's basic support on […] January 2011, while the extended support service ended on […] January 2016.

In the course of the proceedings, however, it was found that the […] system was not the only IT system used by the Administrator that did not have the support of its producer. Another software used in the O. City Hall without such support was the operating system [...]. It should be noted that the above-mentioned the system lost manufacturer support on […] January 2020 ([…]). This means that from […] January 2016 (for the […] system) and from […] January 2020 (for the […] system), according to the information provided by the software manufacturer, for those systems, software updates, security updates and patches were not released.

In addition to the above. systems, prior to the occurrence of a breach of personal data protection, the Administrator used the system [...]. At this point, it should be noted that [...] had the manufacturer's support ([...]) until [...] October 2018, with the option of purchasing extended support until [...] October 2023 (...) - link to the website [...]. Extended Security Update (ESU) is an option for customers who need to run - like O. City Mayor - some of the company's legacy products […] after end of support. It is characterized by the fact that it contains critical or important security updates for a maximum of three years from the date of product end of support. However, the extended support service for […] was not purchased by the Administrator. Therefore, according to the information provided by the software manufacturer, for the ones used in the City Hall in O. systems, software updates, security updates and patches have not been issued, which leads to the conclusion that in the absence of the Administrator's use of other technical or organizational measures to mitigate the risk of personal data breach in connection with the further use of these systems - it did not provide an adequate level of security personal data processing carried out with their use. It should therefore be emphasized once again that the Administrator's failure to use software with the manufacturer's support when processing personal data and failure to take into account the related risks in the risk analysis (which should result in the implementation of additional security measures), consequently, the mayor's failure to implement appropriate technical and organizational measures during the processing of personal data so that the processing takes place in accordance with the provisions of Regulation 2016/679 and in order to provide the necessary security for processing, for which the Administrator, in accordance with art. 24 sec. 1 and 25 sec. 1 of Regulation 2016/679 was obliged, as well as not to apply technical and organizational measures ensuring a level of security corresponding to this risk by ensuring the ability to continuously ensure confidentiality, integrity, availability and resilience of processing systems and services, which in turn is required by the Administrator of art. 32 sec. 1 lit. b) of Regulation 2016/679, and not assessing whether the level of security is appropriate, taking into account the risk associated with the processing of personal data, the obligation to perform which results from art. 32 sec. 2 of Regulation 2016/679. The above statement is also supported by the views of the judicature. As indicated by the Provincial Administrative Court in the judgment of August 26, 2020, file ref. II SA / Wa 2826/19 "technical and organizational activities are the responsibility of the personal data administrator, but they cannot be selected freely and voluntarily, without taking into account the degree of risk and the nature of the personal data being protected."

As indicated above, one of the important elements affecting the security of personal data is to ensure that the software used for the processing of personal data has the latest version made available by its manufacturer. The latest updates should be

installed on an ongoing basis as soon as they are released. As a result, the Administrator ensures that such software has all the updates issued by the manufacturer, including security updates and patches affecting security. However, actions in this regard were taken by the Administrator only after a breach of personal data protection occurred. At that time, the Administrator decided to disable and withdraw from use the key issuing device (e-caretaker system) on which the [...] system was installed, as well as to upgrade the server operating systems to the version [...] and to increase the level of functionality [...] 2019/2021. Taking these measures earlier, in particular when the systems used so far lost the manufacturer's support, would significantly reduce the risk of a breach. In addition, in order to minimize the risk of such violations recurring in the future, the Administrator indicated that he used, inter alia, "Dedicated VLAN for less secure systems, separated LAN zone without access to the main network and the Internet, dedicated, separate network shares on the NAS disk for servers, a copy of each server sent to a separate resource with unique authorization, all passwords forced under the password policy, changed passwords for all accounts, including administrative accounts ”.

Moreover, the Mayor of the City of O. was unable to demonstrate the proper fulfillment of the obligation related to the performance, measurement and testing of data backup, indicating, inter alia, "That due to the incident all logs confirming the correctness of the backup have been lost", including the presentation of written evidence of taking action in this regard in 2020-2021, referring to personnel changes at the IT Department in September 2021. Administrator every True, he had a backup procedure developed, in which he predicted, among others, that an IT specialist supervises the correctness of NAS and removable backups, but due to the above-mentioned circumstances cannot be judged on its effectiveness. The need to make changes in their preparation was also indicated by the report on the "Audit of the ransomwere incident", prepared on [...] November 2021, "However, the backup process itself should be improved (...) in order to select and separate the systems and services included in backup independently of each other. The entire infrastructure could be restored to working order faster. "

Therefore, it should be assumed that prior to the occurrence of the personal data breach in question, the Administrator's backup rules did not ensure the fulfillment of the obligations under Art. 32 sec. 1 lit. b) and c) of Regulation 2016/679, i.e. the ability to ensure the continuous availability of processing systems and services and the ability to quickly restore the availability of personal data and access to them in the event of a physical or technical incident. First of all, as established, the data was restored almost one month after the breach of personal data protection from backup and paper documents (data restoration lasted from […] October 2021 to […] November 2021). There is no doubt that the reproduction of data for a period of almost

one month and the need to use for this purpose data processed in a traditional (paper) form cannot be considered as the correct implementation of the obligation resulting from the above-mentioned provisions of Regulation 2016/679. In addition, the inability to quickly and effectively restore data from the backups held should be taken into account by the Administrator in the risk analysis performed. In the risk analysis of [...] February 2021, i.e. prepared before the occurrence of a personal data breach, the Administrator foresaw a threat in the form of "accidental or unlawful loss" with the description "Cryptovirus attack (encrypting files) on backup copies" and "No backups or copies impossible to restore", and also specified a security measure, i.e. a backup procedure, however, in practice, this procedure turned out to be ineffective, as restoring the data encrypted as a result of a malicious software attack, which should be emphasized again, took time nearly a month and required the use of data from paper documents. Only after the violation, the Administrator updated the procedures related to the creation, testing and restoration of backups, which is to ensure, in particular, full accountability of activities in this area.

The analysis of the breach and the evidence collected in the course of the administrative procedure shows that "constant and regular application of system security tests by the internal IT department until the incident occurred was impossible due to staff shortages and restructuring of the IT department". The above arrangements clearly indicate the Administrator's failure to perform the obligations set out in art. 32 sec. 1 lit. d) Regulation 2016/679. Therefore, the controller was not able to demonstrate or state whether the applied security measures were sufficient.

It should be emphasized that regular testing, measuring and evaluating the effectiveness of technical and organizational measures to ensure the security of processing is the primary duty of each administrator under Art. 32 sec. 1 lit. d) Regulation 2016/679. The administrator is therefore obliged to verify both the selection and the level of effectiveness of the technical 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. However, in the present state of facts, it should be considered that the Administrator did not fulfill the obligation imposed on him to measure and evaluate the effectiveness of technical and organizational measures to ensure the security of personal data processing.

It should also be emphasized that the indicated testing, measurement and evaluation, in order to constitute the fulfillment of the requirement resulting from Art. 32 sec. 1 lit. d) of Regulation 2016/679, must be performed on a regular basis, which means conscious planning and organization, as well as documenting (in connection with the accountability principle referred to in

Article 5 (2) of Regulation 2016/679) of this type of activities in specified time intervals, regardless of changes in the organization and the course of data processing processes.

Actions in this regard were taken by the Administrator only after the breach of personal data protection, presenting evidence in the form of sample protocols from the tests of the ICT infrastructure.

In connection with the above, it should be emphasized that the functioning of any organization, especially in the field of personal data protection, cannot be based on unreliable or unrealistic grounds, and disregarding the value of basic information may result, as indicated above, in a false sense of security and failure by the data controller to take activities to which he is obliged, which in turn may result in a breach of personal data protection, resulting in, due to the scope of the personal data being breached and the lack of access to personal data for a period of about a month, a high risk of violating the rights or freedoms of persons physical.

An unreliably conducted risk analysis resulting in the selection of ineffective security measures and the lack of regular testing, measurement and evaluation by the Administrator of the effectiveness of the implemented technical and organizational measures to ensure the security of processing led, which should be emphasized again, not only to a breach of personal data protection, but also to Of the Mayor of O. 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 lit. 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 Provincial Administrative Court in Warsaw in the judgment of February 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 ".

Acting pursuant to Art. 58 sec. 2 lit. b) of Regulation 2016/679, according to which each supervisory authority has the right to

issue a reminder to the controller or processor in the event of violation of the provisions of this Regulation by processing operations, the President of the Personal Data Protection Office considers it justified to issue a reminder to the President of O. found violation 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 sec. 2 of Regulation 2016/679.

Recital 148 of Regulation 2016/679 states that, for the enforcement of the Regulation to be more effective, infringements should be sanctioned, including administrative fines, in addition to or in lieu of 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 a 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.

Determining the nature of the infringement consists in determining which provision of Regulation 2016/679 has been infringed and classifying the infringement to the appropriate category of infringed provisions, i.e. those indicated in Art. 83 sec. 4 of the Regulation 2016/679 or / and in art. 83 sec. 5 and 6 of Regulation 2016/679. The assessment of the seriousness of the breach (eg low, medium or significant) will be indicated by the nature of the breach as well as "the scope, purpose of the processing concerned, the number of data subjects affected and the extent of the damage they have suffered". The purpose of the processing of personal data is related to determining to what extent the processing meets the two key elements of the "purpose limitation" principle, ie determination of the purpose and compatible use by the controller / processor. When selecting a remedy, the supervisory authority takes into account whether the damage was or could be sustained due to a breach of Regulation 2016/679, although the supervisory authority itself is not competent to award specific compensation for the harm suffered. By marking the duration of the breach, it can be stated that it was immediately removed, was short or long, which in turn allows for the assessment of e.g. the purposefulness or effectiveness of the administrator's or processor's actions. The Article 29 Working Party in the Guidelines on the application and setting of administrative fines for the purposes of Regulation 2016/679 adopted on 3 October 2017 with reference to the intentional or unintentional nature of an infringement indicated that, in principle, "intention" includes both knowledge and intent. , due to the characteristics of a prohibited act, while "inadvertent" means no intention to cause an infringement, despite the controller / processor's failure to comply with the duty of care

required by law. Intentional violations are more serious than unintentional violations and, consequently, more often involve the imposition of an administrative fine.

The President of the Personal Data Protection Office decided that in the established circumstances of this case, issuing a reminder to the Administrator is a sufficient measure. As a mitigating circumstance, the President of the Personal Data Protection Office decided that President O. had taken a number of corrective actions to minimize the risk of a recurrence of the infringement (change of procedures, re-analysis of the risk). In addition, the Administrator reported a breach of personal data protection to the President of the Personal Data Protection Office. On the basis of the circumstances of the case, there are also no grounds to believe that the data subjects have suffered any harm as a result of this breach.

Thus, the breach concerns a one-off event, and therefore we are not dealing with a systematic action or omission that would pose a serious threat to the rights of persons whose personal data are processed by the President. The above circumstances justify granting the Administrator a reminder for the violation found, which will also ensure 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 President of O. 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.

2022-07-18