THE CHAIRMAN OF PERSONAL DATA PROTECTION

Warsaw, day 14

June

2022

DECISION

DKN.5131.56.2021

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 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 it. a) and h) and art. 58 sec. 2 it. b) and d) 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 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 119 of 04/05/2016, p. 1, as amended), after conducting administrative proceedings regarding the processing of personal data by Ms K.Z. running a business under the name K.Z. C ul. in W. (address for service: W.), President of the Office for Personal Data Protection

finding a breach by Ms K.Z. running a business under the name K.Z. C. 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 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 119 of 04/05/2016, p. 1, as amended), hereinafter referred to as "Regulation 2016/679", consisting in the selection of ineffective security measures of the IT system used to process personal data and the lack of regular testing , measuring 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 possible consequences for these systems: 1. Granted by Mrs. K.Z. running a business under the name K.Z. C. admonitions. 2. Ms K.Z. running a business under the name K.Z. C. adjusting the processing operations to the provisions of Regulation 2016/679 by: a. conducting a risk analysis to assess the appropriate level of risk related to the processing of personal data, in particular resulting from accidental or unlawful destruction, loss,

modification, unauthorized disclosure or unauthorized access to personal data transmitted, stored or otherwise processed, taking into account the state of technical knowledge, cost of implementation, nature, scope, context and purposes of processing as well as the risk of violating the rights or freedoms of natural persons, including threats related to the installation of malicious software interfering with data availability and threats in the form of the inability to effectively restore data from a backup, b. implementation of appropriate technical and organizational measures to ensure the ability to quickly restore the availability of personal data and access to them in the event of a physical or technical incident, c. implementation of appropriate technical and organizational measures to ensure regular testing, measurement and evaluation of the effectiveness of technical and organizational measures to ensure the security of processing,

within 30 days from the date of notification of this decision.

Justification

Mrs. K.Z. running a business under the name K.Z. C., hereinafter also referred to as C. ub Administrator, on [...] March 2021, reported to the President of the Personal Data Protection Office (hereinafter also referred to as the "President of the Personal Data Protection Office") a breach of personal data protection of C. employees and patients, consisting in the encryption of their personal data with the help of malware. According to the initial notification of the violation, as a result of the above-mentioned The activities were encrypted with the personal data of 6,000 people. Then, on [...] March 2021, Ms K.Z. submitted a supplementary report in which it indicated that the infringement concerned 7,000 people. The data covered by the violation are: "HR - concluding contracts with employees, remuneration, contracts with employees, statements - name, surname, PESEL number, address, company data: name, address, REGON, NIP, bank account number (files, binders, documents in paper form); ACCOUNTING - performance of contracts, purchases, payment of VAT invoices, contractors, invoices, contracts - Company data: Name, REGON, NIP, bank account number, address, telephone number, e-mail address, (files, binders, paper documents and electronic; Provision of medical services - patients, patient cards, declarations, declarations - name, surname, PESEL number, address, tax identification number of the ZUS contribution payer, e-mail address, telephone number, medical history, test results (files, paper binder and electronic, scans of test results, e-mail). ”The infringement was registered under the reference number [...].

Therefore, by letters of [...] March 2021 and then [...] May 2021, the supervisory authority asked C. to provide explanations, including, inter alia, about:

Indication of whether an investigation was conducted which resulted in establishing the circumstances of the breach, including whether there was a breach of security, and if so, what vulnerability was used.

An indication of how it was verified that there was no breach of confidentiality of the personal data.

Describing the security measures applied so far in order to avoid breach of personal data protection.

Indication of what technical and organizational measures the administrator has applied to minimize the risk of such breaches recurring in the future, including whether the actions described in point 9B of the personal data breach notification form were performed, regarding the security measures applied to minimize the risk of a recurrence of the breach.

Indication if the availability of personal data lost as a result of a ransomware attack has been recovered, and if so, when, how, how long the unavailability of personal data lasted, and whether all data was recovered or restored.

Indication of whether, and if so, how the administrator regularly tested, measured and assessed the effectiveness of technical and organizational measures (before the incident occurred) to ensure the security of personal data processed in the IT systems affected by the breach, in particular in terms of vulnerability, errors and their possible effects on these systems and the actions taken to minimize the risk of their occurrence.

Has the data controller developed and implemented any security procedures, and if so, how is compliance with them verified?

Indication whether the administrator has developed and implemented a procedure that regulates the principles and method of making and storing backups and testing them.

By letter of [...] May 2021, the controller explained the following:

The IT company announced that the data had been encrypted but not removed from the server. Only access to them was blocked.

The personal data protection applied included: anti-virus programs, password-protected access, access only for authorized persons.

An IT company security audit was conducted, the company identified security weaknesses, installed new network security measures, interviewed employees about using network-connected equipment and how to avoid possible dangers.

Data was not fully recovered from the attacked server. It has been disconnected from the mains and power supply (waiting for the appropriate decryptor to appear). The data lost on the server is kept by the administrator in paper form, he also has copies of databases and has received a copy of some files from the National Health Fund. He gained access to paper data

immediately, and it took about a month to restore the database on the new server.

The applied technical and organizational measures to minimize the risk of such violations reoccurring in the future included updating antivirus programs, informing employees about possible dangers in the network, cooperation with an IT specialist and periodic password changes.

The facility's security policy has been developed.

The backup procedure was developed by an IT specialist. According to this procedure, a database backup is sent to an external disk once a week (automatic process). The administrator also downloads a copy of the database to a separate external drive manually once a week.

Then, on [...] July 2021, the supervisory authority asked the Administrator for further explanations, i.e. to:

Describing the security measures used so far to avoid violation of personal data protection, what anti-virus programs were used, and how the access was protected with passwords.

Re-indication of what technical and organizational measures have been applied by the Administrator to minimize the risk of such violations reoccurring in the future, ie what "new network security" has been installed.

Re-indication of whether, and if so, how the controller regularly tested, measured and assessed the effectiveness of technical and organizational measures (before the incident occurred) 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 effects on these systems and the actions taken to minimize the risk of their occurrence, because the described cooperation with an IT specialist is not a form of regular testing.

Indication whether the administrator has developed and implemented a procedure that regulates the principles and method of making and storing backups and testing them.

Forwarding the results of a security audit carried out by an IT company, containing information about which uneas and vulnerabilities were found and how they were removed.

By letter of […] October 2021, the Controller provided an electronic message from an IT company stating that “The attack on the server was carried out using ransomware […]. According to the specification of this attack, the data is encrypted by the window and is not sent anywhere (...). The server was infected with [...], the router had native port forwarding set [...]. (…) As part of restoring the environment, the clinic bought a new server and installed the medical software anew. The software

producer helped to recreate the database by importing the declarations sent from the National Health Fund ”.

To the above to the letter, the administrator attached a report on the verification of the compliance of personal data processing with the provisions on the protection of personal data of [...] March 2021 and the "Security Policy for the Protection of Personal Data of C. K.Z." of [...] May 2018

In connection with the explanations provided, on [...] October 2021, the supervisory authority asked the Administrator for further explanations, i.e. to:

Describing the security measures used so far to avoid breach of personal data protection, including in particular an indication of the anti-virus programs used and whether the access to the data was password-protected.

Reiterating what technical and organizational measures, apart from those described in point 5 of the letter of [...] May 2021, were used by the controller to minimize the risk of recurrence of this type of breach in the future, and what solutions were implemented as "new network security", what is mentioned in the above-mentioned writing.

Re-indication of whether, and if so, how the controller regularly tested, measured and assessed the effectiveness of technical and organizational measures (before the incident occurred) 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 effects on these systems and the actions taken to minimize the risk of their occurrence, because the described cooperation with an IT specialist is not a form of regular testing.

Provision of a photocopy of the risk analysis performed before and after the personal data breach.

Providing information on whether all personal data affected by the breach has been recovered and after what period their availability has been regained.

By letter dated [...] December 2021, C. explained that:

Before the attack, network security was used in the form of access passwords to the server, router, network and each network position (individual for each user, changed periodically), anti-virus software updated on a regular basis (avast anti-virus license version), services of an IT specialist.

After the attack, a security audit was performed and the following was used: a new server with the latest software ([...] 2019) and a device purchased: [...] with a license - Security system, providing many functions: firewall, IPS (protection against attacks), web content filtering, application control, bandwidth optimization, antivirus, VPN or spam protection. Other options

include DLP to protect against confidential data leakage, and a wireless controller for FortiAP.

Before the attack, the Administrator recommended checking security and taking care of the network to an IT specialist, and with his help he carried out audits. After the attack, a new IT company was hired, which constantly monitors the state of the network and introduced additional security measures.

All data was recovered with the help of copies of reports sent to the National Health Fund and backups on external disks, it took about 2 months.

In addition, in the attachment to the above-mentioned of the letter The administrator provided the risk analysis carried out on [...] December 2020 and the risk analysis carried out on [...] May 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 (UODO) on [...] December 2021 initiated ex officio administrative proceedings regarding the possibility of breach by Ms K.Z. running a business under the name K.Z. C., as the data controller, obligations under Regulation 2016/679, i.e. 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 a breach of the protection of personal data of patients of the clinic and employees of C. (letter reference [...]). At the same time, the Administrator was requested to provide further explanations in the following scope:

Indication of the actual number of persons affected by the breach (the initial notification of the breach of personal data protection indicated the number of 6,000 persons, and 7,000 persons in the supplementary report).

Clear indication of the reason for the breach of personal data protection, i.e. whether the breach was caused by opening a dangerous ink (in the explanations provided of [...] May 2021 it was indicated that: "A ransomware breach has been established (vulnerability, opening a dangerous incu)") or a breach of the server's security (the explanations of [...] October 2021 indicated that: "the audit of the IT company revealed an error in securing the server").

Providing explanations on how and with what frequency "informing employees about possible dangers in the network" took place, and in particular whether the Administrator conducted training for his employees in this area, including in the field of cybersecurity, if so, when and whether all employees participated in such training.

Providing information on what server software was used by the Administrator before the personal data breach occurred.

In a letter of [...] February 2022, the Administrator responded to the notice of initiation of administrative proceedings, stating

that:

The actual number of people affected by the infringement is 6,591.

The first information was given incorrectly (misunderstanding of information from an IT specialist), the reason was a breach of the server's security.

Employees are constantly informed about the possible dangers in the network (it is a small facility with a small number of employees), and they are also provided with online training.

The server software used by the Administrator before the personal data breach occurred is Windows Server 2012.

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), the President of the Personal Data Protection Office is the competent authority for data protection and the supervisory authority within the meaning of Regulation 2016/679. Pursuant to Art. 57 sec. 1 it. (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 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 ("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 it. 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 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.

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 violation of 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 likelihood 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 regular testing, measurement and evaluation of the effectiveness of technical and organizational measures to ensure the security of processing. 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.

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 it. 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 Administrator, 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. Incorrect estimation of the risk level makes it impossible to apply appropriate security measures for a given resource and increases the probability of its occurrence. As a result of the above, the risk materialized, as a result of which the security of the Administrator's IT system used by him to process personal data was broken, and then the data processed in it was encrypted with the use of malicious software.

The controller informed that prior to the occurrence of the personal data breach, on [...] December 2020, it carried out a risk analysis for the resource covered by this breach. However, in the analysis performed, the administrator did not predict the risk of data encryption with ransomware. The analysis generally indicated the risk of unavailability to the database server. The risk defined in this way for the processed personal data does not, however, indicate the reason for the loss of data availability, which is important for the selection of effective technical and organizational measures to reduce this risk to an acceptable level. This is because the reasons for unavailability may be different than installing ransomware, such as power failure, flooding, fire or failure.

Moreover, the Administrator's findings show that "The server was infected with RDP". It should therefore be noted that the use

of […] Windows increases the probability of an infringement due to the presence of the above-mentioned software for potential errors (vulnerabilities) that allow unauthenticated attackers to exploit these vulnerabilities, and thus break the authentication mechanism. Before implementing this solution, the Administrator should therefore analyze the risks associated with its use and the impact on the security of personal data processed, which, however, was not done.

The evidence collected in the course of the proceedings indicates that the Administrator has developed a data backup procedure. From this procedure, described in the "Security Policy for the Protection of Personal Data of C. K.Z." shows that the database is backed up once a week to external media. At the same time, in the submitted explanations, the Administrator first informed that "The data has not been fully recovered from the attacked server. (...) We have hard copy of the data lost on the server, we also have copies of databases and we received a copy of some files from the National Health Fund. We got access to paper data immediately, it took about a month to restore the database on the new server "to finally indicate that" all data was recovered with the help of copies of reports sent to the National Health Fund and backups on external disks, it took about 2 months " . The above means that the backups performed by the Administrator did not fulfill their role, i.e. they did not ensure the ability to quickly restore the availability of personal data and access to them in the event of a physical and technical incident, which is required pursuant to Art. 32 sec. 1 it. c) of Regulation 2016/679. There is no doubt that the restoration of data for a period of 2 months and the need to use for this purpose data contained in the resources of another entity (the National Health Fund) cannot be considered as the correct implementation of the obligation resulting from the above-mentioned provision of Regulation 2016/679. In addition, the inability to quickly and effectively restore data from the backups held, the Administrator should foresee in the risk analysis as a significant threat to data security, the more so that the procedures developed by C. in this respect do not provide for performing backup tests for the correctness of their preparation. and reconstruction in the event of a technical or physical incident. However, the administrator did not take into account such a threat in the risk analysis.

In view of the above, it should be stated that the risk analysis carried out by the Administrator prior to the breach of personal data protection did not take into account all potential threats to the personal data being processed, including the risks associated with the loss of access to personal data by encrypting it with ransomware, using the RDP mechanism and the inability to restoring data from backups. Moreover, the conducted analysis does not indicate the method of dealing with the identified risk - C. contented himself only with the percentage and point determination of its level, without indicating, however,

the accepted acceptable level of risk. It also did not indicate what technical and organizational measures were used by the Administrator to reduce the risk to an acceptable level or mitigate its effects. The occurrence of the violation indicates that the selection of technical measures was inappropriate and inadequate.

In the submitted risk analysis performed after the breach of personal data protection of [...] May 2021, the controller re-assessed the risk of unavailability to the database server, however, it did not update it in terms of the risk of lack of access to personal data as a result of their malicious encryption. ransomware by listing this specific type of threat that affects the possibility of losing access to personal data. The above-mentioned analyzing the risks associated with the use of the RDP mechanism and the inability to restore data from backups. It may also be disturbing, in the context of the newly assessed level of risk of unavailability to the database server and due to the personal data breach being the subject of this proceeding, the adoption by C. in the risk analysis of [...] May 2021 of much lower values of this risk compared to the risk analysis carried out on […] December 2020 due to a lower probability of its occurrence (from 'possible' to 'unlikely').

In view of the above, it should be pointed out that a properly conducted risk analysis should take into account all threats affecting the security of personal data processed. What's more, when conducting further analyzes of this type, the Administrator should use the knowledge acquired, among others in connection with handling personal data breaches that occurred in his organization. This means, on the one hand, the necessity to depart from general terms for the identified threats, and, on the other hand, to properly estimate the level of risk of their occurrence, which, in consequence, should ensure the selection of adequate security measures.

Taking into account both the analysis carried out on [...] December 2020 and carried out on [...] May 2021, it should be stated that the Administrator was not (and still is not) aware of the existing threats to the personal data being processed. As a consequence, it should be stated that the Administrator, in the conducted risk analyzes, did not properly take into account the risk related to the processing of data, including, inter alia, PESEL number and data on health, in particular the risk related to the lack of access to personal data, which was infringed by Art. 32 sec. 1 and 2 of Regulation 2016/679. The judgment of the Provincial Administrative Court in W. of May 13, 2021, file ref. II SA / Wa 2129/20, in which the Court indicated that "the data controller should (...) conduct a risk analysis and assess the threats he is dealing with".

The obligation to ensure the security of the processed data, resulting, inter alia, from Art. 32 sec. 1 of Regulation 2016/679, constitutes the foundation for the legal protection of personal data. Regulation 2016/679, however, does not impose specific

actions that should be taken to ensure data security, leaving freedom in this matter to the data controller. By introducing a risk-based approach, Regulation 2016/679 in Art. 32 sec. 1 indicates at the same time the criteria on the basis of which the administrator 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. The selection of security measures should, consequently, be conditioned by the circumstances and conditions of data processing as well as the probability and seriousness of events that may lead to violation of the rights or freedoms of persons whose data is processed. It should be emphasized that the security measures selected as a result of the analysis carried out taking into account the criteria under Art. 32 sec. 1 of Regulation 2016/679, must be effective, i.e. ensure proper protection of personal data processed.

As already shown above, the consequence of incorrectly conducted risk analysis was the selection of inappropriate safety measures or their unforeseeability at all.

It should be noted that the letters provided by the Administrator do not contain information that, for example, penetration tests were carried out, software vulnerabilities and vulnerabilities to attacks from the internal and external networks were detected. They also do not indicate that such tests covered the Windows RDP mechanism, through which the server's security was breached (as mentioned in the e-mail of [...] October 2021, sent to the Administrator by the IT company conducting the audit, quoted: "The server was infected with RDP, the router had native port redirection [...]"), as well as the process of data recovery from a backup in the event of a physical or technical incident, i.e. data encryption with malware.

Due to the lack of application by the administrator of adequate technical and organizational measures aimed at minimizing the risk of data security breach, it should be stated that the Administrator did not provide adequate security for the data processed with their use. As a consequence, this determines the Administrator's failure to implement appropriate technical and organizational measures during the processing of personal data, so that the processing takes place in accordance with Regulation 2016/679 and in order to provide the necessary security for processing, which he was obliged to do in accordance with art. 24 sec. 1 and 25 sec. 1 of Regulation 2016/679, as well as the failure to apply technical and organizational measures ensuring the level of security corresponding to this risk by ensuring the ability to ensure the confidentiality, integrity, availability and resilience of processing systems and services on an ongoing basis, to which the data controller is obliged by art. 32 sec. 1

it. 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. As indicated by the Provincial Administrative Court in Warsaw in its judgment of August 26, 2020, file ref. II SA / Wa 2826/19, "(...) actions of a technical and organizational nature are at the discretion of the personal data administrator, but cannot 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." In the above-mentioned of the judgment, the Court also emphasized that "The measures adopted 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 individually) were adequate and proportional to the degree of risk. "

On the other hand, the consequence of not taking into account in the risk analysis the threats related to the inability to quickly and effectively restore data from the backups held, is the lack of an effective procedure in this regard. It is true that the Administrator in the "Security Policy for the Protection of Personal Data C. K.Z." defined a procedure for backing up databases, but this procedure cannot be considered, as already shown above, as a tool ensuring the ability to quickly restore the availability of personal data and access to them in the event of a physical or technical incident, and thus the fulfillment of the data controller's obligation resulting from joke. 32 sec. 1 it. c) of Regulation 2016/679. This procedure does not provide, inter alia, performing backup tests for the correctness of their preparation and restoration in the event of a technical or physical incident, which is a necessary condition to meet the requirement specified in the above-mentioned provision of Regulation 2016/679. It seems that this problem was noticed by the Administrator, who in the "report on checking the compliance of personal data processing with the provisions on the protection of personal data" submitted to the supervisory body, drawn up on [...] March 2021, constituting Annex 4 to the letter from on […] October 2021, indicates the need to update the backup procedure (paragraph 6 of the report). Unfortunately, due to the lack of a detailed description of what this update would consist of and the fact that C. did not submit changed procedures in this respect, it is difficult to accept the provisions contained in the above-mentioned recommendation as a manifestation of the Administrator's actions aimed at proper (and in accordance with the above-mentioned provision of Regulation 2016/679) to regulate the issue of making backups. It should also be emphasized that the document in which the procedure in question was concluded is dated [...] May 2018, which only confirms the long-term lack of actions of the Administrator in this regard. Therefore, the lack of comprehensive procedures regulating all aspects related to the preparation of backups and their verification, resulting, as in the discussed case, in the inability to quickly and

effectively restore data from backups, means the Administrator violates the above-mentioned provision of Regulation 2016/679.

When analyzing the explanations submitted by the Administrator regarding the applied technical and organizational measures to ensure the security of data processing, it should be indicated that C was used before the violation of personal data protection as the system server software [...]. 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 (Extended End Date; ink to the page [...] ]). Extended Security Update (ESU) is an option for customers who need to run - like C. - 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 up to three ata from the date of the end of extended product support. Therefore, according to the information provided by the software manufacturer, only basic software updates as well as security and patch updates were issued for the system used by the Administrator [...], which leads to the conclusion that from [...] October 2018 - due to the lack of application by the Administrator other technical or organizational measures to mitigate the risk of a breach of personal data protection - it did not ensure an adequate level of security for the processing of personal data carried out with its use. In this context, it must be undoubtedly acknowledged that the use of operating systems and IT systems for the processing of personal data after the end of the main technical support by their producer significantly reduces the level of security of the processing processes carried out in this way. The lack of built-in and updated security measures, in particular, increases the risk of infection with malware and attacks through the emergence of new security tools. These systems are becoming more vulnerable to cyber attacks, incl. ransomware, blocking access to data and demanding a ransom for its recovery. The analysis of the evidence collected in this case clearly shows that no measures were taken to ensure the most recent versions of the software used, despite the fact that the Administrator, in the risk analysis carried out, foresaw the risk of not updating the operating systems of the servers, which also includes the lack of update caused by the manufacturer ceasing to support a given system. Actions in this respect, in the form of the installation of an operating system supported by the manufacturer, were taken by the Administrator only after the violation of personal data protection occurred, thus allowing the data to be processed before the violation using outdated IT systems, i.e. systems that do not guarantee an appropriate level. safety measures without additional safety measures.

In the light of the explanations submitted by the Administrator in this regard, it should be stated that C. also incorrectly fulfilled the obligation specified in Art. 32 sec. 1 it. d) Regulation 2016/679. According to the letter of [...] December 2021, "before the

attack, the administrator instructed an IT specialist to check security and take care of the network, and with his help, he carried out audits. After the attack, a new IT company was hired to monitor the state of the network on an ongoing basis and introduced additional security measures. " As proof of the above, the Administrator submitted one "report on the verification of the compliance of personal data processing with the provisions on the protection of personal data", drawn up on [...] March 2021. The report specifies the areas to be checked ("network security, technical procedures, employee "), but it was done in such a general way that it does not allow to determine the detailed scope of the study, especially with regard to the above-mentioned procedures. Moreover, the area of verification defined in this way clearly indicates that not all technical measures aimed at securing the processed personal data were tested, measured and assessed, but only those relating to network security. Meanwhile, for the proper performance of the obligation under Art. 32 sec. 1 it. d) of Regulation 2016/679, it is necessary to cover all elements of the ICT infrastructure used to process personal data with this measure. Therefore, the Administrator was not able to demonstrate or state that the applied security measures are sufficient. In addition, the one-time verification of the said check indicates rather that it was undertaken only as a result of a breach of personal data protection, and not to meet the requirement referred to in the above-mentioned provision of Regulation 2016/679. This is also evidenced by the date of its conduct ([...] March 2021). Incidentally, it should be noted that in the risk analyzes submitted to the supervisory body, the Administrator indicated the risks as "Lack of regular audits (supervision)" and "Lack of regular reviews carried out by the management". Therefore, the lack of C.'s activities in the field of regular testing, measurement and evaluation of the applied security measures means the materialization of the risks identified by him and additionally confirms the violation of the provisions of Regulation 2016/679 in this regard. In addition, a one-off check is in contradiction with the rules adopted by the Administrator in the "Security Policy for the Protection of Personal Data of C. K.Z.", which specifies the types of checks (scheduled, ad hoc and if requested by the President of UODO), as well as the dates of scheduled checks. Taking into account the terminology adopted by C. in the above-mentioned in the document, it should be considered that the "report on checking the compliance of personal data processing with the provisions on the protection of personal data", drawn up on [...] March 2021, was an ad hoc check related to the breach of personal data protection. Consequently, this means that the Administrator did not carry out scheduled checks, thus violating not only Art. 32 sec. 1 it. d) of Regulation 2016/679, but also by acting contrary to the regulations adopted by them. In the absence of these checks, it is unnecessary to analyze the appropriateness of the adopted period of their carrying out (at least once a year), although it should be noted that such a

period may raise doubts in the context of the nature of the activity and the scope of personal data processed, including health data, so data subject to special protection pursuant to Art. 9 of Regulation 2016/679.

It should be pointed out that in order for the testing, measurement and evaluation of the applied security measures to constitute the fulfillment of the requirement resulting from art. 32 sec. 1 it. 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. As a consequence, it should be stated that the Administrator did not take actions which he is obliged to do in the light of art. 32 sec. 1 it. d) of Regulation 2016/679, which resulted in the violation of this provision of Regulation 2016/679.

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 it. 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 properly 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.

Therefore, the findings do not provide grounds for stating that the technical and organizational measures used by the Administrator to ensure the security of personal data were adequate to the state of technical knowledge, implementation costs and the nature, scope, context and purposes of processing; In the opinion of the President of the Personal Data Protection Office, these measures were not properly reviewed and updated, which consequently did not ensure the effective implementation of data protection principles.

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 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 perform a risk assessment, and then apply such measures and procedures that will be adequate to the assessed risk. "

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 C. 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 ”.

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 in a false sense of security and failure by the personal data controller to take action to which he is obliged to do, which in turn may result, as in the present case, in a breach of personal data protection, resulting in a high risk of violating the rights or freedoms of natural persons due to the scope of the personal data being breached and the lack of access to personal data for a period of approximately 2 months.

Taking into account the explanations provided by the Administrator in connection with the personal data breach in question and the actions taken by the Administrator, both immediately after the breach, as well as at a later stage, in order to ensure the protection of the processed personal data, his approach to security, showing in the infringements of the provisions of Regulation 2016/679 identified in this decision. Determining the circumstances of the breach is important from the point of view of the risk of violating the rights or freedoms of natural persons, which should be a priority for every controller in the event of a breach of personal data protection. The above is confirmed by the Administrator's lack of awareness of what procedures in the field of personal data protection should apply and how the personal data protection system should be built to ensure effective protection of personal data.

It should be emphasized that only after the breach of personal data protection, the Administrator took additional measures to apply technical and organizational measures to ensure the security of personal data processing. An example of such actions was the installation of a firewall […] and raising awareness of cybersecurity threats among C employees. In connection with taking these actions, it should be pointed out that the earlier application of security measures, which were implemented only after a breach, would significantly reduce the risk of this type of threat. The administrator, however, did not take steps to correctly fulfill his obligations related to the ability to quickly restore the availability of personal data and access to them in the event of a physical or technical incident and to regularly test, measure and evaluate the effectiveness of technical and organizational measures to ensure the security of processing. referred to in Art. 32 sec. 1 it. c) and d) of Regulation 2016/679.

Bearing the above in mind, as well as the content of Art. 58 sec. 2 it. d) of Regulation 2016/679, the President of the Personal Data Protection Office ordered the controller to adjust the processing operations to the provisions of Regulation 2016/679 by conducting a risk analysis in order to assess the appropriate level of risk related to the processing of personal data, in particular resulting from accidental or unlawful destruction, loss, modification, unauthorized disclosure or unauthorized access

to personal data transmitted, stored or otherwise processed, taking into account 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, including risks related to installation malware interfering with the availability of personal data and threats in the form of the inability to quickly restore data from a backup, implementation of appropriate technical and organizational measures to ensure the ability to quickly restore access the availability of personal data and access to them in the event of a physical or technical incident, and regular testing, measurement and evaluation of the effectiveness of technical and organizational measures to ensure the security of processing.

Moreover, acting pursuant to Art. 58 sec. 2 it. b) of Regulation 2016/679, according to which each supervisory authority has 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 recognizes that it is justified to issue a reminder to the Administrator in the scope of the breach 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, for the enforcement of the Regulation to be more effective, infringements should be sanctioned, including administrative fines, in addition to or instead 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 in art. 83 sec. 5 and 6 of Regulation 2016/679. The assessment of the seriousness of the breach (e.g. low, average or significant) will be based on the nature of the breach, as well as the scope, purpose of the processing in question, the number of data subjects affected and the extent of the damage they have suffered. 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 violation, it can be stated that it was immediately removed, lasted a short or long time, which in turn allows for the assessment of e.g. the purposefulness or effectiveness of the administrator'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, referring to the intentional or unintentional nature of the infringement, indicated that, in principle, "intention" includes both knowledge and intent. , due to the characteristics of a prohibited act, while "negligence" 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 assumed that there were no grounds to believe that the data subjects suffered any damage as a result of this breach, due to the temporary unavailability of C.'s IT systems from [...] March 2021. In addition, the Administrator reported a breach of personal data protection to the President of the Personal Data Protection Office. Therefore, 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 of persons whose personal data are processed by the Administrator. The above circumstances justify granting the Administrator a reminder for the breach found, which will also ensure that similar events do not occur in the future. The issuing of the reminder was also influenced by the fact that a possible administrative fine would constitute a disproportionate burden on the administrator. Nevertheless, if a similar event repeats itself in the future, each reminder issued by the President of the Personal Data Protection Office against the Administrator 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.

2022-07-18