THE CHAIRMAN OF PERSONAL DATA PROTECTION

Warsaw, day 11

January

2021

DECISION

DKN.5130.2815.2020

Based on Article. 104 § 1 of the Act of 14 June 1960 Code of Administrative Procedure (Journal of Laws of 2020, item 256, 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 art. 58 sec. 2 lit. b) in connection with Art. 5 sec. 1 lit. f), art. 24 sec. 1, art. 25 sec. 1, art. 32 sec. 1 and sec. 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 data protection regulations) (Journal of Laws UE L 119 of 04/05/2016, p. 1, as amended), after conducting administrative proceedings regarding the processing of personal data by the USA, President of the Office for Personal Data Protection,

finding a breach by U. S.A. the provisions of Art. 5 sec. 1 lit. f), art. 24 sec. 1, art. 25 sec. 1 and art. 32 sec. 1 and sec. 2 of Regulation 2016/679 of the European Parliament and of the Council of the EU 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 data protection) (Journal of Laws UE L 119 of 04/05/2016, p. 1 as amended), hereinafter referred to as "Regulation 2016/679", consisting in the selection of ineffective IT system security and the lack of appropriate testing, measurement 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, advises the US

Justification

Of Laws S.A. (hereinafter referred to as the "Company") on [...] May 2020, notified the President of the Personal Data Protection Office (hereinafter also referred to as the "President of the Personal Data Protection Office") of a breach of personal

data protection of employees, customers and patients, which occurred at night from [...] on [...] April 2020. The breach of personal data protection consisted in breaking the security of the Company's IT system used by it to process personal data, and then encrypting the data processed therein. As a consequence, the Company was denied access to the above-mentioned the system and the personal data contained therein. The company determined the scale of the infringement, which showed that the encrypted databases included about 80,000 data records of employees, clients and patients in the scope of first and last name, parents' names, date of birth, bank account number, home address, PESEL identification number, e-mail address. mail, series and number of ID card, telephone number and health data. According to the notification of [...] May 2020, the Company did not identify a high risk of violation of the rights or freedoms of natural persons due to the recovery of encrypted data and resigned from notifying data subjects about the breach.

By letters of [...] May 2020 and [...] June 2020, the President of the Personal Data Protection Office asked the Company to provide additional explanations, including:

whether, in connection with the reported breach of personal data protection, the Company conducted an internal investigation, which made it possible to determine how the data was encrypted by malicious software; what were the circumstances, source and reasons for the violation;

has the Company determined the scale of the data breach that has arisen, in terms of the number of people, as a result of malicious software;

whether the Company analyzed the impact of the lack of access to information systems affected by the violation on the rights and freedoms of data subjects and sent evidence confirming that the Company carried out the above-mentioned analysis;

whether, and if so, how did the Company regularly test, measure and evaluate the effectiveness of technical and organizational measures to ensure the security of personal data processed in the IT systems affected by the violation, in particular in terms of vulnerability, errors and their possible consequences for these systems, and actions taken to minimize the risk of their occurrence and sending evidence confirming that the Company is carrying out the above-mentioned activities;

on what basis the applied security measures to minimize the risk of recurrence of the breach (described in point 9B of the breach notification) were considered sufficient.

In the explanations provided by letters of [...] June 2020 and [...] July 2020, the Company informed that:

An analysis of the infected devices was carried out, however, due to the diversity of the IT infrastructure, it was not possible to

clearly identify the source and cause of the breach.

According to the information obtained from the Internet service provider, in the period preceding the data encryption, no increased network traffic to the Internet was observed, suggesting data derivation. There was also no suspicious network traffic suggesting an external attack.

An assessment of technical measures for IT infrastructure, backup procedures and security for software access and legality was carried out, on the basis of which hardware was replaced and software upgraded. […] Was introduced, the […] service was fully implemented, restrictions on workstations and the password policy were increased, and the backup policy was extended. In addition, it is planned to commission an audit of the local network and infrastructure by a certified external company. In the opinion of the Company, the applied security measures are aimed at minimizing the risk of a similar event occurring in the future.

Due to the suspension of health resorts from [...] March 2020, pursuant to the Regulation of the Minister of Health of March 13, 2020 on the declaration of an epidemic threat in the territory of the Republic of Poland (Journal of Laws of 2020, item 433)), at the time of the breach, the Company did not provide any services to clients and patients. Therefore, in the opinion of the Company, the interest of the data subjects has not been infringed.

In connection with the reported breach of personal data protection and the explanations provided by the Company with the above-mentioned in letters, the President of the Personal Data Protection Office on [...] October 2020 initiated ex officio administrative proceedings regarding the possibility of the Company, as a data controller, breaching the obligations arising from the provisions of Regulation 2016/679, i.e. Art. 5 sec. 1 lit. f), art. 24 sec. 1, art. 25 sec. 1 and art. 32 sec. 1 and 2, in connection with a breach of the protection of personal data of employees, clients and patients of the Company (letter reference [...]).

In response to the notification of the initiation of administrative proceedings, by letter of [...] October 2020, the Company provided explanations in which it indicated, inter alia, that:

Violation of the protection of personal data in the form of loss of their availability as a result of data encryption in the Company's systems revealed risks, the probability of which the Company assessed as negligible. The restriction of access to data due to the encryption malware called "Devos" resulted in a re-analysis of the risk, taking into account additional risks, and taking security measures to minimize the possibility of their occurrence in the future, as well as minimize the damage in the

event of their occurrence. As a result of the incident, actions were taken to seal the IT system and make it resistant to similar events in the future. The company replaced the used system software, among others, the A and B systems were replaced with C and D systems, and the E system with the F system. Additional changes were made in the scope of […]. In addition, changes were made to the access procedures and the backup procedure.

As part of an additional external audit, aimed at verifying the measures taken to tighten the infrastructure and minimize vulnerabilities, an audit of the infrastructure is planned by an independent, external specialist company.

The encrypted data recovery process was commissioned to a specialized external company.

The company has concluded an agreement with a law firm selected in 2018 for the standardization of procedures and security policy, which specifies the scope of work undertaken for this purpose. These works also include the analysis of the risk of organizational, physical and personal security, including the identification of potential risk areas in data processing. The original analysis took into account the vulnerabilities and threats to these systems and their possible effects, therefore measures were taken to minimize the risk of their occurrence. These are ongoing software and hardware updates, as well as the separation of the WiFi network for guests, implementation of the G […] solution in order to […]. The conducted analysis took into account protection against computer viruses, but the risk of data encryption was not included in it as an event with a high probability of occurrence.

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.

Article 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 "). Further provisions of the regulation make this principle more specific. 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 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 concern ..

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. In the first place, 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 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, if applicable, in accordance with lit. a), b) and d) of this Article should include measures such as pseudonymization and encryption of personal data, the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services, 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.

Considering the scope of personal data processed by the Company, including, inter alia, data of a specific category in the form of health data, and categories of persons whose data are processed (including patients), in order to properly fulfill the obligations imposed on the above-mentioned the provisions of the regulation, the Company was obliged to take actions ensuring an appropriate level of data protection by implementing appropriate technical and organizational measures, including by using software with up-to-date technical support from the manufacturer for the processing of personal data, activities aimed at the optimal configuration of the operating systems used, and regular measurement and evaluation of the effectiveness of technical and organizational measures to ensure the security of 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. In this context, it should be noted that the lack of technical support from the manufacturer is a vulnerability in terms of the security level of the software used, and thus poses a high risk of reducing the system's resilience, among others. to the action of malicious software. 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, which in the opinion of the Company had a low degree of probability, i.e. the security of the Company's IT system used by it to process personal data was breached, and then the data processed in it was encrypted.

The collected evidence shows that the technical measures implemented by the Company did not ensure an adequate level of security of data processed via IT systems. The consequence of the above was an incident as a result of which the security applied by the Company was breached and the data contained in the IT systems used by the Company to process personal

data was encrypted. The "Devos" encryption malware disabled antivirus protection, which resulted in the operating system security mechanisms from working. The infection took place at night, and the irregularities were not found until the morning (due to the fact that the spa was not functioning due to the pandemic - the IT department also operated with a reduced staff). Explaining the security issues, the Company informed that it has always used and uses IT systems for which it has licenses and software producer support, including in a letter of [...] July 2020, it indicated that "there is an exchange of seats with the previous version of the E system to the current version, supported by the manufacturer - […]. On the basis of the list of changes made by the Company after the infringement, aimed at the proper protection of the processed data, in the scope of software replacement, it was found that the E operating system was used for work, for which, according to the information provided on the manufacturer's website, the technical support period ended on [...] January 2020 (https: // […]) and database system B for which technical support ended on […] July 2019 (https: // […]). This means that from that moment, according to the information provided by the software manufacturer for the above-mentioned systems, software updates as well as security updates and patches were not released. Due to the lack of application by the data controller of other technical and organizational measures aimed at minimizing the risk of data security breach in connection with the end of support by the manufacturer of the software used by the Company to process personal data, it should be stated that the Company did not provide adequate security for the data processed using them. As a consequence, this determines the failure by the Company to implement appropriate technical and organizational measures at the time of processing personal data so that the processing takes place in accordance with Regulation 2016/679 and for the purpose of granting the necessary safeguards to be processed, which it was obliged to do in accordance with Art. 24 sec. 1 and 25 sec. 1 of the 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 continuously ensure confidentiality, integrity, availability and resilience of processing systems and services, to which the data controller is obliged by 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 related to 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 the judgment of August 26, 2020, file ref. II SA / Wa 2826/19 "(...) activities of a technical and organizational nature are the responsibility of the personal data administrator, but they cannot be selected in a completely free and voluntary manner, without taking into account the degree of risk and the nature of the personal data being protected."

In this context, it should be noted that the use of operating systems and IT systems used to process personal data after the end of technical support by their producer significantly reduces their level of security. The lack of built-in and updated security measures, in particular, increases the risk of malware infections and attacks by creating new vulnerabilities. These systems are becoming more vulnerable to cyber attacks, incl. ransomware that blocks access to data and demands a ransom for its recovery.

In the letters addressed to the President of the Personal Data Protection Office (UODO), the Company explained that it carried out periodic assessment of technical measures in the field of IT infrastructure. However, as follows from the Company's letter of [...] July 2020, quotation: "Until now, all tests were performed only for internal purposes, so there was no need to create additional documentation for such tests. The tests concerned mainly the performance of the components as part of the software used and resistance to failures (power failure, disk failure, component failure). Software legality audits were also carried out. "

In addition, as follows from the Company's letter of [...] October 2020, in accordance with the security policy adopted by the Company, the control is a continuous process and lasts from the moment the computer workstation is launched in the production environment and consists in verifying access rights and correct operation of system components. Irregularities were corrected on an ongoing basis through security patches, software updates and component replacement. In the case of the above activities, the Company did not prepare any additional documentation, as these were standard activities related to the maintenance and service of a computer station.

It should be noted that the tests performed in the above-mentioned scope do not fully meet the controller's obligation specified in Art. 32 sec. 1 lit. d) Regulation 2016/679. Technical and organizational security measures in relation to IT systems used to process personal data were not fully tested. Therefore, the controller was not able to demonstrate or state that the applied security measures were sufficient. It is recommended to test, measure and evaluate, so that it constitutes 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 consciously planning and organizing, 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 the data processing processes caused. However, the Company did not take such actions, which exaggerates the breach 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 a fundamental duty of every controller and processor under Art. 32 sec. 1 lit. d of 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. On the other hand, in the present state of facts, the Company partially fulfilled this obligation, verifying and modifying the level of effectiveness of the implemented security measures in situations where there was a suspicion of the existence of a vulnerability - then works were undertaken to protect against a given vulnerability. However, such action of the administrator cannot be considered as the fulfillment of the obligation specified in the provision of Regulation 2016/679. As mentioned above, tests were not carried out on a regular basis to verify the security of IT systems used to process personal data covered by the personal data breach in question.

Objections may also be raised by the effectiveness of these tests, which, as the Company explains, were carried out in relation to the "performance of components as part of the software used and resistance to failures". Their result was not the replacement of those IT systems that lost the producer's support, which, as indicated above, significantly reduced the level of security of the data processed by the Company.

The arrangements made do not give rise to a conclusion that the technical and organizational measures used by the Company 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 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 implemented solutions aimed at ensuring the security of personal data are adequate to the level of risk, as

well as taking 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 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 assess the risk, and then apply such measures and procedures that will be adequate to the assessed risk. " The analysis of the breach shows that the methodology of internal tests adopted by the Company was not able to demonstrate a reliable assessment of the security of IT systems, indicating all vulnerabilities and resistance to attempts to breach security as a result of unauthorized third party activity and malicious software. In view of the above, the safety assessment turned out to be insufficient as regards the application of appropriate technical and organizational safeguards. It should be pointed out that the earlier application of security measures, which were implemented only after the breach, would significantly reduce the risk of this type of threat.

In connection with the above findings, it should be stated that the Company, by failing to apply technical and organizational measures ensuring the security of the processed data, which resulted in a breach of personal data protection reported to the President of the Personal Data Protection Office on [...] May 2020, breached Art. 5 sec. 1 lit. f) of Regulation 2016/679, reflected in the form of obligations specified in Art. 24 sec. 1, art. 25 sec. 1, art. 32 sec. 1 and art. 32 sec. 2 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 deems it justified to issue a reminder to the Company in the scope of the breach found art. 5 sec. 1 lit. f) in connection with 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, in order for the enforcement of the Regulation to be more effective, infringements should be sanctioned, including administrative fines, in addition to or in place of the appropriate measures imposed by the supervisory authority under this Regulation. If the infringement is minor, the fine may be replaced by an

admonition. However, due attention should be paid to the nature, gravity and duration of the breach, whether the breach was not intentional, the steps taken to minimize the harm, the degree of liability or any previous relevant 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 the determination of the extent to which the processing meets the two key elements of the "purpose limitation" principle, ie the 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 selecting the duration of the breach, it can be stated that it was immediately removed, lasted for a short time or for a long time, 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" encompasses 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 Company is a sufficient measure. As a mitigating circumstance, the President of the Personal Data Protection Office found that the Company took a number of remedial actions to minimize the risk of a recurrence of the breach (replacement of hardware and software, changing procedures, re-analyzing the risk, conducting a security audit). In addition, the Company 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 damage as a result of this breach, due to the suspension of the operation of health resorts from [...] March 2020 pursuant to the Regulation of the Minister of Health of 13 March 2020 - at the time of the violation, the Company did not provide any services to clients and patients.

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 is processed by the Company. The above circumstances justify granting the Company a reminder for the infringement found, which will also ensure that similar events will not take place in the future. Nevertheless, if a similar event repeats itself in the future, each reminder issued by the President of the Personal Data Protection Office against the Company will be taken into account when assessing the premises for a possible administrative penalty, 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.

The decision is final. Based on Article. 7 sec. 2 of the Act of May 10, 2018 on the Protection of Personal Data (Journal of Laws of 2019, item 1781, as amended) in connection with Art. 13 § 2, art. 53 § 1 and article. 54 § 1 of the Act of August 30, 2002 - Law on proceedings before administrative courts (Journal of Laws of 2019, item 2325), the party has the right to lodge a complaint against the decision with the Provincial Administrative Court in Warsaw, within 30 days from the date of its delivery to the party. The complaint is lodged through the President of the Personal Data Protection Office. The entry fee for the complaint is PLN 200. The party has the right to apply for the right to assistance, including exemption from court costs.

2021-02-17