THE CHAIRMAN OF PERSONAL DATA PROTECTION

Warsaw, on 25

May

2022

DECISION

DKN.5131.14.2021

Based on Article. 104 § 1 of the Act of 14 June 1960 Code of Administrative Procedure (Journal of Laws of 2021, item 735, as amended) in connection with Art. 7 and art. 60 of the Act of May 10, 2018 on the Protection of Personal Data (Journal of Laws of 2019, item 1781) and Art. 57 sec. 1 lit. a) and h) and art. 58 sec. 2 lit. b) and d) in connection with Art. 5 sec. 1 lit. f), art. 5 sec. 2, art. 24 sec. 1, art. 25 sec. 1, art. 32 sec. 1 and 2 and article. 33 sec. 1 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 data protection) (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 Ms W. S., running a business under the name of W. S. (K.), President of the Office for Personal Data Protection ,

finding that Mrs. W. S., conducting business activity under the name of W. S. (K.), breached the provisions of Art. 5 sec. 1 lit. f), art. 5 sec. 2, art. 24 sec. 1, art. 25 sec. 1, art. 32 sec. 1 and 2 and article. 33 sec. 1 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 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 security measures for the IT system used to process personal data and the lack of appropriate 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 their possible consequences for these systems and the actions taken to minimize the risk of their occurrence, as well as failure to notify the President of the Data Protection Office Personal data breaches without unnecessary delay, no later than 72 hours after finding the violation, 1. Grant Mrs. W. S., running a business under the name of W. S. (K.) a warning. 2. Orders

Mrs. W. S., running a business under the name of W. S. (K.) to adapt 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, 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,

b) 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 on which this decision becomes final.

Justification

In July 2020, the Office for Personal Data Protection received information about an incident concerning the website ([...]) of the store of Mrs. W. S., running a business under the name W. S. (K.), hereinafter also referred to as the Administrator. In connection with the above, the President of the Personal Data Protection Office (hereinafter also referred to as the "President of the Personal Data Protection Office"), applied in letters dated: [...] August 2020, [...] October 2020 and [...] November 2020. to the Administrator to provide explanations in the matter in question. Only by letter of [...] December 2020 (date of posting: (...) December 2021), the Administrator replied to the above-mentioned summons and reported to the President of the Personal Data Protection Office a breach of the protection of personal data of customers "who placed an order in the store on [...] 12.2019 to [...] 04.2020", although, as he himself stated, he was informed about the incident already on [...] July 2020. According to the application, which was registered under the reference number [...], the breach of personal data protection consisted in the possibility of unauthorized access to the catalogs of the store's website [...], run by Ms. W. S., containing data on customer orders and, consequently, the collection of by a third party repository from the website server containing the above-mentioned information. The administrator defined the scale of the violation as follows - "No direct finding. Files to which unauthorized access took place could contain data of up to 1208 people. Maximum 1337 records (number of orders) ". The scope of personal data covered by the violation in question, as reported, included names and surnames, e-mail addresses, telephone numbers and addresses for shipping the order. According to the notification, the Administrator did not find a high risk of violation of the rights or freedoms of natural persons, and therefore did not notify data subjects about the breach of the protection of their personal data.

By letters dated: [...] January 2021 and [...] February 2021, the President of the Personal Data Protection Office asked the Administrator to provide additional explanations, including:

Indication of the reasons for the delay in notifying the supervisory authority about the breach of personal data protection.

Information whether it has been verified that the data has been downloaded by an unauthorized person.

Indication of whether a risk analysis has been carried out for the processing of customers' personal data via the store's website.

Indication whether the above-mentioned the analysis showed the vulnerabilities and their possible consequences for the website, as well as whether measures were taken to minimize the risk of their occurrence.

Information on whether, and if so, how the administrator regularly tested, measured and assessed the effectiveness of technical and organizational measures to ensure the security of personal data processed in the infringed system, in particular to protect against unauthorized access to customer data.

Indication of whether regular testing was carried out against attacks from the public network in order to identify as many vulnerabilities and weaknesses as possible that could pose a threat to the security of the site, and if so, to provide relevant evidence.

In the explanations provided in the letters of [...] January 2021 and [...] March 2021, the Administrator informed that:

1) On [...] July 2020, he learned about an incident regarding a personal data breach. The source of the information was an e-mail from M. M. from the portal […]. After obtaining the above-mentioned In the first place, the administrator focused on identifying the type of problem and the causes of the incident. Then, he took the necessary steps to safeguard personal data in an appropriate manner. Full protection took place no later than [...] August 2020, i.e. a few days after receiving information about the incident. Therefore, no more than 7 days elapsed from the disclosure of the incident to the complete protection of the data. Then, the controller assessed the risk of violating the rights or freedoms of natural persons. Among other things, the size of the potential damage and the probability of its occurrence were taken into account. The administrator has determined with certainty that there has been no breach of special categories of personal data, including those revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership and genetic data, biometric data, data concerning health, sexuality or orientation sexual person. The breach concerned such data as, inter alia, name, surname, e-mail address, shipping address or information about purchased products. It turned out that the administrator did not store data such as: NIP,

PESEL or other identifiers. The type of breach was identified as a loss of confidentiality. There has been no loss of availability or breach of data integrity. The administrator runs an online store at […]. It is addressed mainly to young people who use social networking sites, where often at least some of the data whose confidentiality has been breached is voluntarily disclosed, including the name, surname and image. The products offered by the Administrator's online store are mainly original clothing and accessories. The customers of the online store make a purchase decision not because of the functional properties of the offered products, but mainly because of the desire to identify themselves with the W. brand. In other words, they do not have a secret to make purchases in the store [...], on the contrary, the customers of the store [... ] willingly display the purchased products. This takes place both in public spaces such as school, university, workplace, and also in social media. In the opinion of the Administrator, this element was significant from the point of view of the context of data processing and the type of data whose confidentiality has been breached (including the type of products purchased). When assessing the risk, the circumstances of the breach of confidentiality and the disclosure of this fact were also taken into account. Namely, the Administrator determined that the potential confidentiality breach existed for several months. From the content of the portal article itself that revealed the violation, it appeared that the person who gained access to the data was observing the changes in the database. The administrator, analyzing all the information he had at that time, came to the conclusion that despite the potentially long time in which the data was unsecured, none of the customers of the online store [...] or the administrator himself suffered any inconvenience. Administrator until receiving the above-mentioned The e-mail from Mr. M. M. did not receive any information or complaints in this regard. The same thing happened more than a month after notifying the customers of the online store about the incident. It was also recognized, bearing in mind the above-mentioned the fact that only one person was granted access to the data, who informed the portal about it […], and provided some of the data in order to authenticate the information. This person had to have above-average knowledge and skills in the field of computer science. The administrator judged him to be passionate in his field, not a scammer. The administrator assessed that despite having personal data whose confidentiality was breached in the incident in question, it is not easy to identify a specific natural person. Ultimately, after analyzing all the circumstances, the Administrator concluded that it is unlikely that the incident in question would result in a risk of violating the rights or freedoms of natural persons. As a result, the notification was not filed within the legal deadline. The assessment described above changed after receiving a letter from the Office of [...] November 2020, which the Administrator interpreted as a request to submit a notification and a request to inform persons whose personal data had

been violated about the incident. Therefore, in response to the above-mentioned the letter was reported on the incident on [...] December 2020, and the information to persons whose personal data was breached was sent by e-mail on [...] December 2020.

2) The circumstances of the data collection were described in the article on the [...] portal, and the Administrator learned about the incident from this source. As a result of an internal audit, it was found that none of the persons cooperating with the Administrator had committed this act. At the same time, an external audit commissioned by the Administrator confirmed that the data was collected by an unauthorized person.

3) Before launching sales in the online store [...], he started cooperation with IT professionals with many years of experience in the industry. This concerned both the design of the online store, its ongoing IT service and data security monitoring. The administrator in cooperation with the above-mentioned entities took into account the resources that will be used to process personal data, hardware and software, place of data processing, people involved in data processing and their knowledge, experience and skills in this area, the scope of data obtained from customers of the online store, the amount of this data and other elements necessary for risk assessment. The entities responsible for securing the processing of personal data also performed periodic inspections from which reports were prepared. As a result of the analysis carried out prior to the launch of the sale, no high risk of violation of the rights or freedoms of natural persons in the processing of personal data of customers via the website of the shop was found […].

4) After the disclosure of the incident, he commissioned a detailed audit to reveal the reasons for the loss of confidentiality of the data, and to determine what actions should be taken to prevent access to the data and secure it for the future. The audit showed that the website and server required the following actions:

a) blocking direct referencing to the server and configuring white lists of addresses for public servers; b) strengthening security by blocking external traffic at source file addresses; c) strengthening security by implementing double authentication for all access points; d) migration of backup files to external servers with an additional blockade of external traffic; e) re-installation of servers, databases and content management system with accompanying modules.

All the above activities were performed after an extensive external and internal audit. The administrator was convinced that no later than [...] August 2020 data security is fully ensured. In addition, the Administrator carried out an intensive and regular review of the security of files and data.

1) He cooperated in the design and maintenance of the online store with professional subcontractors. As part of the services provided to the Administrator, periodic safety checks of technical and organizational measures were carried out. Regular activities were carried out to minimize the risk of access to any sensitive data, along with securing the system's stability. These activities boiled down to a systematic analysis of the server event log along with current updates of the software used. Additionally, development works of the systems used were carried out on an ongoing basis. In particular, the following were performed:

a) supervision works in the form of traffic and load monitoring on the infrastructure during periods of increased traffic; b) periodic verification of the server event log; c) development works within the server infrastructure; d) installation of software for exporting data from virtual servers to the server aggregating metrics; e ) updating and verifying the stability of the content management system; f) periodic supervision works on the main sales module, including the review of additional modules; g) updating the database server software.

The data controller provided reports on IT activities from March, May and July 2020.

2) In the scope of ensuring the security of the website [...] cooperated with professional subcontractors who performed regular testing against attacks from the public network in order to identify as many vulnerabilities and deficiencies as possible that could pose a threat to the website. Such activities included, among others:

a) systematic analysis of the event log; b) security improvements for databases in the period February-June 2020; c) regular verification of the stability of the system and the software used; d) a series of development works aimed at increasing the level of security and stability of services.

The data administrator provided invoices confirming the purchase of the necessary machines and services to perform the above-mentioned IT activities.

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 [...] April 2021 initiated ex officio administrative proceedings regarding the possibility of breach by Mrs. 5 sec. 1 lit. f), art. 5 sec. 2, art. 24 sec. 1, art. 25 sec. 1 and 2, art. 32 sec. 1 and 2 and article. 33 sec. 1 of Regulation 2016/679, in connection with the breach of the protection of personal data of shop customers [...] (letter reference [...]).

In response to the notification of the initiation of administrative proceedings, by letter of [...] April 2021, the Administrator

provided explanations in which he indicated, inter alia, that:

1) In the letter of the Administrator's plenipotentiary of [...] January 2021 (to the previous reference number [...]), it was indicated that, at the request of the Administrator, regular IT inspections of the online store operating at [...] were carried out in 2020. After each inspection, the contractors, i.e. Mr. M. G. and Mr. D. P., prepared reports, which showed, inter alia, that the website traffic was monitored, the server event log was verified, and the stability of the content management system was updated and verified (M. G., running a business under the name of M. G. I. z / s in K., NIP: [...]). The server infrastructure is maintained at an external service provider, ie O. Sp. z o.o. z / s we W. The infrastructure provider provides logs from servers not older than 30 days. For this reason (but also on the date the incident was detected), more detailed data retention reports could not be recreated.

The data controller provided the above-mentioned reports and additional reports on traffic, acquisition, user paths, as well as demographic data for the period [...] .02.2020 - [...] .08.2020.

2) The activities aimed at improving the security of the databases were carried out both before and after the incident. Activities in February-June 2020 include:

(a) hiding the user interface for the database management tool […] to increase security; (b) migrating the database from the application server to an external server.

After the incident was detected (July 2020), additional measures were taken, i.e .:

a) complete reinstallation of the database; b) separation of the database from the external environment (connection possible only by machines from the network); c) reinstallation and increased security for the distributed version control system; d) change of passwords to encryption […].

The data administrator submitted an application to change the server location to improve the operation of the services and an invoice documenting the purchase of the server.

3) The main tools used for research and development to maximize the security and stability of services are:

a) [...] - file search; b) [...] - port scanning; c) [...] - metric aggregation; d) [...] - metrics visualization; e) [...] - process monitoring; f) [...] - disk occupancy monitoring, g) […] - load balancing, h) […] - automated system alerts, i) […] - cross-platform text editor.

Data analysis using the above-mentioned tools allowed the Administrator to make decisions on development activities that also take into account security.

4) Actions taken to increase the level of security and stability of services in the period of January-June 2020:

a) migration of the application server from France to Poland; b) expansion of the server infrastructure aimed at scaling the traffic; c) scaling the traffic by introducing a second execution machine; d) implementing software [...] to prevent intrusions.

Actions taken to increase the level of security and stability of services in the period of July-December 2020:

a) introducing a new internal security policy; in particular, it was established that each employee who has contact with the store's software [...] has an individual account that can be monitored; b) additional, non-standard security measures for the administration panel for the store's software were introduced [...]; c) automatic reports and notifications about unauthorized d) configuration of the traffic blocking mechanism for attacks such as […]; e) automatic migration of graphic files to external servers […] in order to increase service performance.

As explained, for the Administrator and the IT company that supports him, the incident contributed to an increase in financial and organizational outlays aimed at improving the quality of the services provided, as well as the security of the processed data. The administrator has started work on a new log centralization solution, which will allow for a more in-depth analysis of events from all used machines.

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 lit. (a) and (h) of Regulation 2016/679, without prejudice to the other tasks set out under that Regulation, each supervisory authority on its territory shall monitor and enforce the application of this Regulation; conduct proceedings for breaches of this Regulation, including on the basis of information received from another supervisory authority or other public authority.

Art. 5 of Regulation 2016/679 lays down rules regarding the processing of personal data that must be respected by all administrators, i.e. entities that independently or jointly with others determine the purposes and methods of personal data processing. Pursuant to Art. 5 sec. 1 lit. f) of Regulation 2016/679, personal data must be processed in a manner ensuring adequate security of personal data, including protection against unauthorized or unlawful processing and accidental loss, destruction or damage, by appropriate technical or organizational measures ("confidentiality and integrity "). Pursuant to Art. 5

sec. 2 of Regulation 2016/679, the controller is responsible for compliance with the provisions of para. 1 and must be able to demonstrate compliance with them ("accountability"). Specification of the confidentiality principle referred to in Art. 5 sec. 1 lit. f) of Regulation 2016/679, constitute further provisions of this legal act. Pursuant to Art. 24 sec. 1 of Regulation 2016/679, taking into account the nature, scope, context and purposes of processing as well as the risk of violation of the rights or freedoms of natural persons of varying probability and seriousness, the controller implements appropriate technical and organizational measures for the processing to be carried out in accordance with this Regulation and to be able to demonstrate it . These measures are reviewed and updated as necessary.

In accordance with Art. 25 sec. 1 of Regulation 2016/679, taking into account the state of technical knowledge, the cost of implementation and the nature, scope, context and purposes of processing as well as the risk of violating the rights or freedoms of natural persons with different probabilities and severity resulting from the processing, the controller - both in determining the methods of processing and during the processing itself - implements appropriate technical and organizational measures, such as pseudonymisation, designed to effectively implement data protection principles, such as data minimization, and to provide the processing with the necessary safeguards to meet the requirements of this Regulation and protect the rights of persons whose data relate to.

From the content of art. 32 sec. 1 of Regulation 2016/679 shows that the administrator is obliged to apply technical and organizational measures corresponding to the risk of violating the rights and freedoms of natural persons with a different probability of occurrence and the severity of the threat. The provision specifies that when deciding on technical and organizational measures, the state of technical knowledge, implementation cost, nature, scope, context and purposes of processing as well as the risk of violating the rights or freedoms of natural persons with different probability and severity should be taken into account. It follows from the above-mentioned provision that the determination of appropriate technical and organizational measures is a two-stage process. First of all, it is important to determine the level of risk related to the processing of personal data, taking into account the criteria set out in Art. 32 sec. 1 of Regulation 2016/679, and then it should be determined what technical and organizational measures will be appropriate to ensure the level of security corresponding to this risk. These arrangements should, where appropriate, include measures such as the pseudonymisation and encryption of personal data, the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services, the ability to quickly restore the availability and access of personal data in the event of a physical incident. or

technical, and regularly testing, measuring and evaluating the effectiveness of technical and organizational measures to ensure the security of processing. Pursuant to Art. 32 sec. 2 of Regulation 2016/679, the administrator, when assessing whether the level of security is appropriate, takes into account in particular the risk related to the processing, in particular resulting from accidental or unlawful destruction, loss, modification, unauthorized disclosure or unauthorized access to personal data sent, stored or otherwise processed.

As indicated in Art. 24 sec. 1 of Regulation 2016/679, the nature, scope, context and purposes of processing as well as the risk of violating the rights or freedoms of natural persons of varying probability and severity are factors that the controller is obliged to take into account in the process of building a data protection system, also in particular from the point of view of other obligations indicated in art. 25 sec. 1, art. 32 sec. 1 or Art. 32 sec. 2 of Regulation 2016/679. The aforementioned provisions detail the principle of confidentiality specified in Art. 5 sec. 1 lit. f) of Regulation 2016/679, and compliance with this principle is necessary for the proper implementation of the accountability principle resulting from Art. 5 sec. 2 of Regulation 2016/679.

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. 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, which, in the Administrator's opinion, had a low degree of probability, i.e. by downloading the repository from the website server used by the Administrator to process personal data, unauthorized access to catalogs with information about customer orders, including personal data, took place. It is important, however, that the Administrator did not provide the President of the Personal Data Protection Office with evidence confirming the risk analysis, but limited himself only to presenting reports of IT activities for individual months. In addition to them, he pointed out that in the case in question, "(...) there was no high risk - insufficient amount of personal data to take significant actions violating the welfare of persons", and additionally, "As a result of the analysis carried out prior to the launch of the sale, no high risk of violation of the law was

identified or the freedom of natural persons in the processing of clients' personal data via the website (…) ". The above reports and explanations cannot, however, constitute grounds for recognition, in the light of the principle of accountability resulting from Art. 5 sec. 2 of Regulation 2016/679 that the Administrator has performed a risk analysis in this respect, 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. A properly conducted risk analysis should allow the Administrator to identify all threats to personal data as part of the processing processes carried out and to estimate the probability of their materialization in accordance with the adopted methodology, which should result in the selection of effective security measures to reduce the identified risks to an acceptable level and, consequently, ensure an adequate level of protection of personal data. On the other hand, the reports presented by the Administrator on IT activities for individual months document only the activities that the Administrator undertook on the IT infrastructure owned, without referring to specific threats, the implementation of which could possibly be eliminated or limited. In addition, the description of the activities contained in the content of the above-mentioned reports is very general, which makes it impossible to assess their effectiveness in securing the processed data. Finally, due to the lack of description of the results of these activities and the conclusions resulting therefrom, it cannot be assumed that they constitute a manifestation of regular testing, measurement and evaluation of the effectiveness of technical and organizational measures to ensure the security of processing, and thus the fulfillment of the requirement specified in Art. 32 sec. 1 lit. d) Regulation 2016/679. It follows from the above that the lack of a reliable risk analysis carried out by the Administrator led to deficiencies in the form of failure to implement appropriate technical and organizational measures, resulting in the breach of security and, consequently, the occurrence of a breach of personal data protection. As emphasized by the Provincial Administrative Court in Warsaw in the judgment of May 13, 2021, file ref. II SA / Wa 2129/20 "The data controller should (...) perform a risk analysis and assess the threats he is dealing with".

The collected evidence shows that the technical measures implemented by the Administrator did not ensure an adequate level of security of the personal data of customers processed in connection with the operation of the online store [...]. The consequence of the above was an incident as a result of which an unauthorized person gained access to names, e-mail addresses, telephone numbers and addresses for shipping orders of the Administrator's customers. 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. Explaining the security issues, the Administrator informed that "(...) before launching sales in the online store, he started cooperation with IT professionals with many years of experience in the industry. This concerned both the design of the online store, its ongoing IT service and data security monitoring. " As it turned out later, both the above activities and "(...) periodic inspections" performed by "(...) entities responsible for securing the processing of personal data (...)" did not prove to be effective enough to avoid a breach. The above only confirms the importance of a reliable risk analysis. It should also be emphasized that appropriate actions were taken by the Administrator only "after the disclosure of the incident in question (...)" and commissioned a detailed audit by him. On its basis, it was found that “the website and the server required the following actions: a) blocking direct referring to the server and configuration of white lists of addresses for public servers; strengthening security by blocking external traffic at source file addresses; strengthening security by implementing double authentication for all access points; migration of backup files to external servers with additional blocking of external traffic; re-installation of servers, databases and content management system with accompanying modules ”. This means that in the period preceding the infringement, the Administrator did not ensure adequate security of the processed data, which he himself confirmed, indicating that, "(...) he is convinced that no later than [...] August 2020, data security is fully ensured "And that it" established that the potential breach of confidentiality existed for several months. " 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 lit. b) of Regulation 2016/679 and failure to assess 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 its judgment of August 26, 2020, file ref. II SA / Wa 2826/19 "(...) technical and organizational activities are the responsibility of the personal data administrator, but they cannot be selected freely and voluntarily, without taking into account the degree of

risk and the nature of the personal data being protected". The consequence of violating the above-mentioned provisions of Regulation 2016/679 was a breach of the confidentiality principle expressed in Art. 5 sec. 1 lit. f) Regulation 2016/679, and consequently also the accountability principle referred to in Art. 5 sec. 2 of Regulation 2016/679. The above is confirmed by the judgment of the Provincial Administrative Court in Warsaw of February 10, 2021, file ref. II SA / Wa 2378/20: "The principle of accountability is therefore based on the legal responsibility of the controller for the proper fulfillment of obligations and imposes an obligation on him to demonstrate, both to the supervisory authority and the data subject, evidence that all data processing rules have been complied with". Similarly, the issue of the principle of accountability is interpreted in the judgment of August 26, 2020 of the Provincial Administrative Court in Warsaw, file no. 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 responsible for the violation of the provisions on the protection of personal data. The principle of accountability expressly implies that it is the data controller that should demonstrate and therefore prove that it complies with the provisions set out in Art. 5 sec. 1 of Regulation 2016/679 ".

In the letters addressed to the President of the Personal Data Protection Office, the Administrator explained that "periodic safety checks of technical and organizational measures" were carried out. As follows from the Controller's letter of [...] January 2021, quotation: "Regular activities were carried out to minimize the risk of access to any sensitive data, along with securing the stability of the system. These activities boiled down to a systematic analysis of the server event log along with current updates of the software used. Additionally, development works of the systems used were carried out on an ongoing basis ".

It should be noted that the tests performed in the above-specified 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, e.g. there were no tests of applied security measures for the detection of security gaps and vulnerabilities. Moreover, the administrator himself indicated in the explanations that "[...] the potential breach of confidentiality existed for several months", and therefore was not able to demonstrate or state that the security measures applied were sufficient. In addition, the above statement of the Administrator, in the context of his explanations contained in the letter of [...] January 2021, clearly indicates that the actions taken in this respect before the infringement of personal data protection were ineffective.

Therefore, 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 basic duty of each administrator under Art. 32 sec. 1 lit. d) Regulation 2016/679. The administrator is therefore obliged to verify both the selection and the level of effectiveness of the technical measures used at each stage of processing. The comprehensiveness of this verification should be assessed through the prism of adequacy to risks and proportionality in relation to the state of technical knowledge, implementation costs and the nature, scope, context and purposes of processing. On the other hand, in the present state of facts, the Administrator fulfilled this obligation partially, verifying and modifying the level of effectiveness of the implemented security measures only after "(...) disclosure of the incident in question" and commissioning an audit, which showed that "(...) the website and the server required undertaking (…) Actions ". However, the above cannot be considered as the fulfillment of the obligation imposed on the Administrator and specified in the provision of Regulation 2016/679. 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 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.

Objections may also be raised by evidence of the effectiveness of these tests, which, in the Administrator's explanations, were limited only to the list of works, statements and invoices. The "Reports on IT activities" presented by the Administrator contain only statements about the implementation of, inter alia, periodic verification of the event log, monitoring of traffic and load on the infrastructure and software updates. With the above. the reports do not clearly indicate what technical infrastructure the measures were related to, and whether the infrastructure that was attacked was subject to the above-mentioned tests. As indicated above, due to the lack of description of the results of the actions taken and the resulting conclusions in the "Reports on IT activities" submitted by the Administrator for each month, it cannot be assumed that the Administrator fulfills the obligation under Art. 32 sec. 1 lit. d) of Regulation 2016/679 are provided by these reports. The effect of carrying out the activities indicated in them should be a determination whether the technical or organizational measure applied by the Administrator, subjected to such a test or assessment, still fulfills its function, i.e. whether it still effectively protects the processed personal data, or has been compromised due to e.g. detection of an existing security gaps in it, which should mean resigning from its use and replacing it with another effective measure or applying additional security measures to ensure an adequate level of protection for personal data (which should also be reflected in the risk analysis performed). A certain change

in the Administrator's approach in this regard can be seen in the presented "Report on IT activities" prepared on [...] April 2021, which included the assessment of the extensions used for the content management system. However, it should be emphasized that in order for these activities to be considered as the proper implementation of the requirement to test, measure and evaluate the effectiveness of technical and organizational measures used by the Administrator to ensure the security of processing, they must cover all aspects related to the security of personal data processing, and derived from their conclusions comprehensively describe all, and not only selected, elements of the ICT infrastructure that affect data security.

Therefore, the findings do not provide a basis for stating, which should be emphasized again, that the technical and organizational measures used by the Administrator 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 also 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 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 Administrator 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 action. In view of the above, the safety assessment turned out to be insufficient in terms of 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.

Bearing the above in mind, as well as the content of Art. 58 sec. 2 lit. d) of Regulation 2016/679, the President of the Personal Data Protection Office ordered the controller to adapt the processing operations to the provisions of Regulation 2016/679 by performing a risk analysis taking into account the state of technical knowledge, implementation cost, nature, scope, context and purposes of processing and the risk of violating the rights or freedoms of natural persons, and also 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.

Joke. 33 sec. 1 of Regulation 2016/679 shows that in the event of a breach of personal data protection, the data controller shall, without undue delay - if possible, no later than 72 hours after finding the breach - report it to the competent supervisory authority pursuant to art. 55, unless it is unlikely that the violation would result in a risk of violating the rights or freedoms of natural persons. The notification submitted to the supervisory authority after 72 hours shall be accompanied by an explanation of the reasons for the delay.

In connection with the breach in question, the controller not only failed to comply with the obligation according to which without undue delay - if possible no later than 72 hours after the breach was discovered - he should report it to the supervisory authority (the date of finding the breach is indicated in the form sent: [...] July 2020, and the date of notification of the violation: [...] December 2020), but also decided to implement it only, (...) after receiving a letter from the Office of [...] November 2020 ., which the administrator interpreted as a request to submit a notification (...) ". The Article 29 Working Party in the guidelines indicates that even the lack of all detailed information related to the incident should not be an obstacle to timely notification of a breach and, although in some cases the GDPR allows for delayed reporting, such situations should be treated as emergency situations ".

In the case in question, which clearly results from the findings made, there was an unauthorized access to the data, resulting in

a security breach leading to the disclosure of data "up to 1208 people" ("customers who placed an order in the store on [...]. [...] .04.2021 "), i.e. to breach the confidentiality of these persons' data, which decides that there has been a breach of personal data protection.

The breach of personal data protection (data confidentiality) that occurred in the present case results in the risk of violating the rights or freedoms of natural persons. As indicated by the Article 29 Working Party in the guidelines on reporting personal data breaches in accordance with Regulation 2016/679, hereinafter also referred to as "guidelines": "When assessing the risk to individuals resulting from the breach, the controller should therefore take into account the specific circumstances of the breach, including the importance of the potential impact and the likelihood of it occurring ". The Article 29 Working Party therefore recommends that the assessment should take into account the following criteria: "(…) Number of individuals affected by the breach. The breach may affect only one person, several people, or several thousand people - or many more. Typically, the potential impact of a breach increases with the number of people affected. However, depending on the nature of the personal data and the context in which they were disclosed, a breach could have serious consequences for up to one individual. Again, the most important thing is to analyze the likelihood of consequences for those affected by the breach and how severe the consequences will be. ' There is no doubt that in the case at hand, the infringement concerns many people, which significantly increases the gravity of the infringement and the probability of the risks related to the infringement materializing. The fact that, as a result of the breach, the disclosure of, for example, PESEL identification numbers of the affected persons was not revealed, it does not mean that these persons cannot be identified and that they cannot suffer negative consequences as a result of disclosing their personal data to an unauthorized person. As a consequence, this means that there is a risk of violation of the rights or freedoms of persons covered by the violation in question, which in turn results in the Administrator being obliged to report the violation of personal data protection to the supervisory authority, in accordance with art. 33 sec. 1 of the Regulation 2016/679, which must contain the information specified in art. 33 sec. 3 of Regulation 2016/679.

In the case at hand, as already mentioned, the personal data of "1208 persons" was disclosed in the form of: names and surnames, e-mail addresses, telephone numbers and addresses for shipping the order. Disclosure of such data is not associated with a high risk of violation of the rights or freedoms of natural persons, which is determined by, inter alia, the fact raised by the Administrator that as a result of a breach of personal data protection, there was no disclosure of data revealing racial or ethnic origin, political views, religious or philosophical beliefs, trade union membership and genetic data, biometric

data, data concerning health, sexuality or sexual orientation of a natural person "(and thus, the Administrator was not obliged to notify the data subjects of the breach, in accordance with Article 34 of Regulation 2016/679), nevertheless, this risk exists in such a case - hence the need to notify the President UODO on the infringement. The possible risk related to the event that has occurred is, in particular, the loss of data subjects' control over their data. These data may, for example, be used by persons who come into their possession, e.g. unwanted by data subjects, contacts by e-mail or telephone - also those during which attempts will be made to obtain additional data of these persons. Finally, using this data, accounts can be set up in various types of social networking sites and internet portals, which may have a negative impact on the perception of these people in their professional or family environment, and even lead to their discrimination. Therefore, the above means that in the case of the personal data breach in question, there is a risk of violating the rights or freedoms of natural persons.

It is worth emphasizing that the possible consequences of the event that occurred do not have to materialize - in the content of Art. 33 sec. 1 of Regulation 2016/679, it was indicated that the mere occurrence of a breach of personal data protection, which involves the risk of violating the rights or freedoms of natural persons, implies an obligation to notify the breach to the competent supervisory authority. Thus, the circumstance raised by the Administrator that quoted: “(...) it is unlikely that the incident in question would result in a risk of violating the law or freedom of natural persons. As a result, the notification was not made within the time stipulated by law "is irrelevant to the fact that the Administrator has an obligation to report this breach of personal data protection to the President of the Personal Data Protection Office, pursuant to Art. 33 sec. 1 of Regulation 2016/679. In a similar case, the Provincial Administrative Court in Warsaw, in the judgment of September 22, 2021, file ref. II SA / Wa 791/21 stated that "(...) in the case at hand, it is not important whether an unauthorized recipient actually came into possession and became acquainted with the personal data of other persons, but that there was such a risk and, consequently, there is also a potential risk of violating the rights or freedoms of data subjects ”. Further on, the Court also emphasizes that “the possible consequences of an event that has occurred do not have to materialize. In the wording of Art. 33 sec. 1 of Regulation 2016/679 indicates that the mere occurrence of a breach of personal data protection, which involves the risk of violating the rights or freedoms of natural persons, implies an obligation to notify the breach to the competent supervisory authority, unless it is unlikely that the breach would result in a risk of violating the rights or freedoms natural persons.

Therefore, the fact raised by the Administrator that the quotation: "no information has been received by the University that could have an impact on the change of the risk level or requiring taking other technical and organizational measures extending

the catalog of actions taken" remains irrelevant for determining the Administrator's obligation to report the breach of protection in question personal data to the President of the Personal Data Protection Office, in accordance with the above provision ”.

The Provincial Administrative Court in Warsaw made a similar opinion in the judgment of January 21, 2022 (file reference: II SA / Wa 1353/21), indicating that "(...) the possible consequences of the event of a personal data breach do not have to materialize - as in Art. . 33 sec. 1 GDPR, the mere occurrence of a breach of personal data protection, which involves the risk of violating the rights or freedoms of natural persons, implies an obligation to notify the breach to the competent supervisory authority. The circumstance raised by the Company that the breach did not result in the occurrence of physical or damage to natural persons is irrelevant for the determination of the Company's obligation to notify the President of the Personal Data Protection Office of the breach of personal data protection, in accordance with the above-mentioned recipe ".

In order to establish the existence of the Administrator's obligation to notify the President of the Personal Data Protection Office of the above-mentioned breach of personal data protection, in accordance with art. 33 sec. 1 of Regulation 2016/679, it is also irrelevant that the Administrator takes actions to minimize the risk of recurrence of the breach, as indicated in correspondence with the supervisory authority. The nature of these activities indicates that they are to prevent the occurrence of such violations in the future; However, these activities do not in any way affect the assessment that due to the occurrence of the data breach in question there is a risk of violating the rights or freedoms of natural persons. Moreover, the Article 29 Working Party clearly states in the guidelines that "in case of any doubts, the controller should report the breach, even if such caution could turn out to be excessive". It is also irrelevant the fact raised by the Administrator that "only one person, who informed the hazardnik.pl portal about this, was granted access to the data, and provided some of the data in order to authenticate the information. This person had to have above-average knowledge and skills in the field of computer science. The administrator judged him to be passionate in his field, not a scammer. " This person is an unauthorized person to access this data. Moreover, the Administrator cannot be sure that, in addition to the above-mentioned no other unauthorized person or persons had access to the indicated personal data.

In a situation where, as a result of a breach of personal data protection, there is a risk of violating the rights or freedoms of natural persons, the controller is obliged to implement all appropriate technical and organizational measures to immediately identify the breach of personal data protection and promptly inform the supervisory authority. The administrator should fulfill this obligation as soon as possible.

Recital 85 of the preamble to Regulation 2016/679 explains: "In the absence of an adequate and prompt response, a breach of personal data protection may result in physical harm, property or non-material damage to natural persons, such as loss of control over own personal data or limitation of rights, discrimination, theft or falsification of identity, financial loss, unauthorized reversal of pseudonymisation, breach of reputation, breach of confidentiality of personal data protected by professional secrecy or any other significant economic or social damage. Therefore, as soon as it becomes aware of a personal data breach, the controller should notify it to the supervisory authority without undue delay, if practicable, no later than 72 hours after the breach has been discovered, unless the controller can demonstrate in accordance with the accountability principle that it is unlikely to be that the breach could result in a risk of violation of the rights or freedoms of natural persons. If the notification cannot be made within 72 hours, the notification should be accompanied by an explanation of the reasons for the delay and the information may be provided gradually without further undue delay. '

Consequently, it should be stated that the Administrator did not notify the supervisory authority of the breach of personal data protection within the period specified in Art. 33 sec. 1 of Regulation 2016/679, which means the Administrator's violation of this provision. The explanations provided by him show that he was informed about the violation on [...] July 2020, and he did not notify the President of the Personal Data Protection Office until [...] December 2020. The statement contained by the Administrator in the explanations, i.e. "(...) I did not make reporting the incident to the Personal Data Protection Office in the manner specified by you, because (despite the determination of the vulnerability, weaknesses in the website security system), unauthorized access to customer data could only concern the following scope: names and surnames, data on telephone numbers, e-mails, addresses to the shipment of the order, the type of services ordered / performed, which in my opinion would not allow for a serious, real violation of the rights and freedoms of our customers ”does not justify such a significant exceeding of the 72-hour period referred to above. Moreover, in the case at hand, the controller could meet the deadline without any major obstacles, using the option of successive submission of the notification referred to in the guidelines of the Article 29 Working Party.

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 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 regarding the breach of the law. art. 5 sec. 1 lit. f) and art. 5 sec. 2 in connection with Art. 24 sec. 1, art. 25 sec.

1, art. 32 sec. 1 and sec. 2, as well as art. 33 sec. 1 of Regulation 2016/679.

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

Determining the nature of the infringement consists in determining which provision of Regulation 2016/679 has been infringed and classifying the infringement to the appropriate category of infringed provisions, i.e. those indicated in Art. 83 sec. 4 of the Regulation 2016/679 or / and in art. 83 sec. 5 and 6 of Regulation 2016/679. The assessment of the seriousness of the breach (eg low, medium or significant) will be indicated by the nature of the breach as well as "the scope, purpose of the processing concerned, the number of data subjects affected and the extent of the damage they have suffered". The purpose of the processing of personal data is related to determining to what extent the processing meets the two key elements of the "purpose limited" principle, ie determination of the purpose and consistent use by the controller. 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, was short or long, 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 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 "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 found that the Administrator took a number of remedial actions to minimize the risk of a recurrence of the breach by implementing additional solutions to ensure the security of the website. In addition, the Administrator finally reported a breach of personal data protection to the President of the Personal Data Protection Office. On the basis of the circumstances of the case, there are also no grounds to believe that the data subjects have suffered any harm as a result of this breach. The breach therefore concerns a one-off event, and therefore we are not dealing with a systematic action or omission that would pose a serious threat to the rights of persons whose personal data are processed by the 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. 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 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.

2022-07-15