THE CHAIRMAN OF PERSONAL DATA PROTECTION

Warsaw, 09

of December

2021

DECISION

DKN.5130.2559.2020

Based on Article. 104 § 1 and art. 105 § 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 sec. 1, art. 60, art. 102 paragraph. 1 point 1) and sec. 3 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 lit. h) and art. 58 sec. 2 lit. i) 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. 34 sec. 1, as well as art. 83 sec. 1 and 2, art. 83 sec. 4 lit. a) and art. 83 sec. 5 lit. a) 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 Regulation) (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 Warsaw University of Technology with its seat in Warsaw at Plac Politechniki 1, 00-661 Warsaw, President Personal Data Protection Office

1) finding a violation by the Warsaw University of Technology with its seat in Warsaw at Plac Politechniki 1, 00-661 Warsaw, of 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 of Regulation 2016/679 of the European Parliament and of the Council 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 EU L 119 of 04/05/2016, p. 1, as amended), hereinafter referred to as "Regulation 2016/679", consisting in failure to fulfill the obligations incumbent on the administrator, resulting from Regulation 2016 / 679, through:

a) failure to apply appropriate technical and organizational measures to ensure the ability to continuously ensure the confidentiality of processing services, failure to regularly test, measure and evaluate the effectiveness of technical and organizational measures aimed at ensuring the security of personal data processed in the IT system named [...], and this the

same improper consideration of the risk related to the processing of personal data in the above-mentioned system,

b) failure to take into account the risk related to the processing of [...] user passwords in the application in the form of a hash function, which does not provide a sufficient guarantee of security, which in the event of failure to apply other technical and organizational measures to ensure secure processing, in accordance with the provisions of Regulation 2016/679 , makes the data subjects vulnerable to increasing the risk of violating the rights or freedoms of natural persons in the event of a breach of the confidentiality of the data being processed,

c) no analysis of the validity of the 4-week storage of logs (event logs) of the virtual machine on which the system was located [...] and no analysis of the justification for the lack of a detailed event log in the application [...], which determines the failure to implement appropriate technical and organizational measures ensuring maintaining the ability to quickly and effectively identify any breaches to ensure that appropriate action can be taken,

imposes on the Warsaw University of Technology with its seat in Warsaw at Plac Politechniki 1, for violation of Art. 5 sec. 1 lit. f), art. 5 sec. 2, art. 25 sec. 1 and art. 32 sec. 1 and 2 of Regulation 2016/679, an administrative fine in the amount of PLN 45,000 (forty-five thousand zlotys);

2) the remainder of the proceedings is discontinued.

Justification

On [...] May 2020, the Warsaw University of Technology (hereinafter also referred to as: the "University" or the "Administrator") notified the President of the Personal Data Protection Office (hereinafter also referred to as: "the President of the Personal Data Protection Office" or the "supervisory authority") of the breach of personal data protection, which was registered under the reference number DKN.5130.2559.2020. The notification was completed by the University on [...] May 2020. The violation notification indicated that [...] in May 2020, an unknown and unauthorized person downloaded a database containing personal data of students and lecturers from the University's IT network [...], from 2008 - 2020, as well as 169 candidates for studies for the academic year 2019/2020 (a total of 5,013 people).

The categories of data concerned by the breach include: name and surname, parents' names, date of birth, address of residence or stay, PESEL number, e-mail address, username and / or password, mother's maiden name, series and number of ID card and no. phone.

In order to remedy the breach and minimize the negative consequences for the data subjects, the controller has relevant law

enforcement agencies and secured and separated from the internal network of the University IT resources that were the subject of the breach. Noting a high risk of violation of the rights and freedoms of data subjects, it informed by e-mail [...] and [...] on May 2020 all data subjects about the breach of personal data protection, in accordance with Art. 34 of the Regulation 2016/679 (the content of the notification is attached to the initial notification). In addition, the administrator indicated that he had also taken other information activities, such as an announcement on the University's website and a dedicated subpage with a list of frequently asked questions and answers.

In a letter of [...] May 2020, the President of the Office for Personal Data Protection notified the Warsaw University of Technology about the initiation of administrative proceedings, the subject of which is the possibility of violating by the University, as a data controller, the obligations arising from the provisions of Regulation 2016/679 in the scope of obligations under Art. 5 sec. 1 lit. f), art. 24 sec. 1, art. 25 sec. 1, art. 32 sec. 1 and 2 and article. 34 sec. 1 and 3. Above the administrative procedure, in a letter of [...] July 2021, was also extended to the possibility of violating by the University, as the data administrator, the obligations arising from the provisions of the above-mentioned regulation to the extent referred to in article 1. 5 sec. 2.

In the course of the proceedings conducted in this case, the President of the Office for Personal Data Protection, in letters of: [...] May, [...] July, [...] September 2020, [...] January and [...] July 2021, called the University to submit explanations. Based on the explanations provided by the University in letters from: [...] June, [...] July, [...] September 2020, [...] January 2021 and [...] July 2021, the supervisory authority established the following facts :

The organizational unit of the University, i.e. [...], hereinafter also [...], in order to perform its tasks uses an IT system called [...] (hereinafter referred to as [...]), under which the application - [...] (hereinafter also referred to as [...]), operating for about 10 years and used by students to enroll in courses and gain access to the history of study and settlement of fees, as well as to prepare certificates, statistics and other documents to which the University is obliged. As part of this system, lecturers could place files related to the subject they were teaching.

The application […] was created from scratch by the University's employees, as none of the solutions offered on the market was able to meet the needs of […].

The application […] was modified on an ongoing basis depending on the current needs of the Administrator. Ultimately, the functionalities of the system were gradually transferred to the system […], ie […].

Apart from the […] application, the […] application functioned in parallel within the […] system. They both had access to […] which contained the personal data concerned by the infringement.

[...] January 2020 (according to the file metadata marking), an unauthorized third party, having the credentials, used the functionality of placing files in the application [...] by a person having lecturer rights (explanations of [...] June 2020 with attachments and clarifications of [...] January 2021) and placed the backdoor file in the application directory [...], intended for file storage by lecturers. In the intention of the application developers […], the possibility of writing to this directory should be limited only to logged in users with the lecturer status.

An unauthorized person obtained login data in the application [...] via the system [...] (probably [...], the user probably used the same login data in different systems).

[...] April 2020 (according to the file metadata marking), a second backdoor file was placed in the application directory [...]. The administrator indicated that no trace of the malicious file being uploaded via the [...] application was found.

[...] May 2020 (according to the marking of server logs), an unauthorized download of personal data was made using a file placed on [...] April 2020. According to the author of the report of the preliminary intrusion analysis, this file was probably placed using the functionality provided by the file placed on the server [...] January 2020 The server logs constitute Annex No. 1 to the letter of [...] July 2020. The report on the preliminary intrusion analysis of [...] May 2020 constitutes Annex No. 2 to the letter of [...] June 2020.

[...] in May 2020, the editors [...] sent an e-mail to the University regarding the violation in question.

[...] in May 2020, after learning about a potential violation, the University disconnected the server from [...] from the public network. As a result of finding a violation, the administrator decided to completely decommission the system from use.

[...] in May 2020, the editors [...] also informed the University about the violation, indicating the address of the SQL file being the database of the system [...], which is 2.8 GB in size.

[...] in May 2020, the University commissioned an external entity to carry out a forensic analysis (the analysis is attached as Annex 2 to the letter of [...] June 2020).

The information indicated in the report from the preliminary intrusion analysis shows that the logs of the system logs were deleted after 4 weeks. Also the application itself […] did not have a detailed log of events.

Passwords in the [...] application were stored as MD5 hashes without any additional solutions, and its complexity required 8

characters, one capital letter and a special character. The administrator indicated that from December 2019, work was underway on the implementation of a new login system and the method of storing passwords, however, they have not been completed and implemented (explanations of [...] June 2020 and [...] July 2020).

The university did not perform penetration tests of applications [...], allowing for the detection of the system's vulnerability to attacks from the public network (administrator's explanations of [...] January 2021).

As part of regular testing, measuring and assessing the effectiveness of technical and organizational measures, the University indicated that it uses [...] to search for vulnerabilities of applications and systems available from the outside (administrator's explanations of [...] June and [...] September 2020).

In the administrator's opinion, the security measures were adequate to the risk, and the perpetrator's action scenario went beyond the scheme adopted in the risk assessment. The university did not carry out a formal audit of the application's source code [...] and did not perform a formal risk assessment for this application. It stated that during the development, implementation and operation of the system, the revision was carried out by its authors (persons employed under an employment contract at the Warsaw University of Technology), and in the further operation period by IT department employees [...]. The reliability of these revisions was justified by the Administrator with the knowledge and experience of the authors and the analysis of the existing industry reports on IT vulnerabilities and attacks (explanations by the administrator of [...] July 2020 and [...] September 2020).

The software used for the functioning of the IT infrastructure of the Warsaw University of Technology is up-to-date and constantly updated. At the time of the infringement, the application [...] was functioning in the [...] version, as of [...] September 2020 it was upgraded to the latest version [...] (explanations of [...] June and [...] September 2020).

Before the infringement, there were [...] and [...] within the structure of the Warsaw University of Technology, constituting an appendix to the Regulation No. [...] of the Rector of the Warsaw University of Technology of [...] May 2018 (the documents constitute an appendix to the letter of [...] July 2021 r.).

The structure of the Warsaw University of Technology currently includes [...] and [...], constituting an annex to the Regulation No. [...] of the Rector of the Warsaw University of Technology of [...] July 2020 (the documents constitute an annex to the letter of [...] July 2020).

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 the wording of 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 severity, 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. This means that when assessing the proportionality of the safeguards, the controller should take into account the factors and circumstances relating to the processing (e.g. type, method of data processing) and the risks associated with it. At the same time, the implementation of appropriate safeguards is an obligation which is a manifestation of the implementation of the general principle of data processing - the principle of integrity and confidentiality, as defined in Art. 5 sec. 1 lit. f) of Regulation 2016/679, according to which personal data should be processed in a manner ensuring adequate data security, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, by appropriate technical or organizational measures.

Pursuant to Art. 5 sec. 2 of Regulation 2016/679, the controller is responsible for compliance with the provisions of para. 1 and must be able to demonstrate compliance with them ("accountability").

Pursuant to Art. 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.

Art. 32 sec. 1 of Regulation 2016/679 provides that the controller is obliged to apply technical and organizational measures corresponding to the risk of violating the rights or 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, one should take 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 likelihood and severity. 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.

Pursuant to Art. 32 sec. 2 of Regulation 2016/679, when assessing whether the level of security is adequate, 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.

Considering the fact that the breach of personal data protection related to the functioning of security measures in the IT system, in a letter of [...] May 2020 (and in the form of clarifying questions in letters of [...] July 2020, [...] September 2020, and [...] January 2021), the President of the Personal Data Protection Office asked the University to indicate and present relevant evidence, and if so, when and how, the Administrator regularly tested, measured and assessed the effectiveness of technical and organizational measures ensure the security of the processed personal data in the IT systems affected by the breach. In particular, did he perform penetration tests of the application [...], whether he performed risk assessment and identified threats related to the possibility of unauthorized access to the IT environment, and if so, when and what measures to reduce the assumed risk he applied, how does he monitor and review this risk. In the explanations of [...] June 2020, [...] July 2020, [...] September 2020 and [...] January 2021, the University indicated that it had not performed penetration tests to find vulnerabilities to attacks with public network. It indicated that these systems are scanned for vulnerability using solutions […] and […], however, it did not indicate when it performs such scanning, did not provide relevant evidence confirming its performance, detected vulnerabilities and how to deal with them. At no stage of the administrative procedure, the university has not presented relevant evidence that could be considered sufficient to demonstrate compliance with the obligations under Art. 32 sec. 1 and 2 of Regulation 2016/679. The administrator merely made a statement that he had not carried out a formal risk assessment, identified threats related to unauthorized access to IT environments "(...) by collecting information from university units". In addition, he used the above-mentioned tools and "(...) mutual revisions of the system's source code [...] between its authors" and, in the further period of operation, of IT department employees [...] whose competences were verified "[...] as part of recruitment procedures and then in their daily work by their superiors ". In the opinion of the Administrator, such activities did not require a formal audit of the system's source code [...].

In the opinion of the supervisory body, this method of the administrator's operation did not ensure proper control over the data processing process in the above-mentioned system, and consequently identifying the risks of violating the rights or freedoms of natural persons.

When analyzing the above explanations and the collected evidence, it should be emphasized that in accordance with § [...], constituting Annex No. [...] to the Regulation No. [...] of the Rector of the Warsaw University of Technology, ensuring the security of personal data is based on continuous improvement, the basis of which is annual risk analysis in the scope of ensuring the security of personal data. On the other hand, according to § [...], constituting Appendix no. [...] to the above-mentioned Risk management and analysis are carried out by a person or a team of persons designated respectively by the administrator. After the analysis process is completed and initialed by the Data Protection Officer, the results are approved by the Administrator. Risk analysis in accordance with the above-mentioned document, consists in particular of estimating the consequences, estimating the probability of an incident and determining the level of risk. This method also requires the prior identification of hazards. The analysis of the above documents shows that the administrator's failure to perform a formal risk assessment was not only a violation of the provisions of Regulation 2016/679, but also of internal regulations aimed at ensuring the correct and safe processing of personal data in the organization. It should be emphasized that the principles contained in the above-mentioned documentation, in force in accordance with the Regulation [...] of the Rector of the Warsaw University of Technology from [...] May 2018, resulted directly from Regulation 2016/679, in particular Art. 24 sec. 1, art. 25 sec. 1, art. 32 sec. 1 lit. b) and d) and art. 32 sec. 2 of Regulation 2016/679. Therefore, limiting ourselves only to the use of mechanisms provided by dedicated solutions available on the market […] and the ad hoc review of the application code should be considered insufficient.

This understanding of the obligations imposed on the administrator is also confirmed in the judgment of the Provincial Administrative Court of September 3, 2020, II SA / Wa 2559/19. The court ruled that "Regulation 2016/679 introduced an approach in which risk management is the foundation of activities related to the protection of personal data and is a continuous process. Entities processing personal data are obliged not only to ensure compliance with the guidelines of the above-mentioned of the regulation through a one-off implementation of organizational and technical security measures, but also to ensure the continuity of monitoring the level of threats and ensuring accountability in terms of the level and adequacy of the introduced security. This means that it becomes necessary to prove to the supervisory authority that the solutions

introduced to ensure the security of personal data are adequate to the level of risk, as well as take into account the nature of the organization and the personal data processing mechanisms used. The administrator is to independently carry out a detailed analysis of the data processing processes carried out and assess the risk, and then apply such measures and procedures that will be adequate to the assessed risk. The consequence of this orientation is the abandonment of the lists of security requirements imposed by the legislator, in favor of independent selection security based on threat analysis. Administrators are not informed about specific security measures and procedures. The administrator is to independently carry out a detailed analysis of the data processing processes carried out and perform a risk assessment, and then apply such measures and procedures that will be adequate to the assessed risk. "

In a letter of [...] May 2020, the President of the Personal Data Protection Office asked the University to indicate the actions that the administrator took to assess the reasons for the failure to detect undesirable actions that interfere with the confidentiality of data, which took place in January and April 2020. In the explanations from [...] June 2020 The administrator indicated that "[s] the price list of the perpetrator's actions went beyond the scheme adopted in the risk assessment". Despite theses formulated in this way, the Administrator at no stage of the proceedings presented any evidence to justify the adequacy of the security measures applied to the risk. He described only the IT infrastructure safeguards which, in his opinion, were the best in relation to his expectations, experiences and financial capacity, and not in the context of risks to the data processed as part of the infringement process.

In the opinion of the President of the Personal Data Protection Office, these activities were therefore not adequate to all threats and risks related to the possibility of obtaining unauthorized access to data processed in the system [...]. Taking into account the established facts, in the opinion of the President of the Personal Data Protection Office, the Administrator did not perform a risk analysis, and thus did not comply with the obligation under Art. 32 sec. 2 in connection with Art. 5 sec. 2 of Regulation 2016/679, i.e. has not properly demonstrated whether the level of security is adequate to the risk of unlawful, unauthorized access to personal data. It should be emphasized again that the Administrator in his explanations only indicated the purchase of a high-class edge device with a set of licenses extending the device's capabilities in the field of monitoring and securing access from outside. He also pointed to the use of an antivirus solution and regular updates. In the opinion of the President of the Personal Data Protection Office, the administrator's implementation of the above-mentioned technical measures, without prior risk analysis for the data processed as part of the infringement process, did not guarantee at any stage of data

processing that these measures would be adequate and would effectively minimize the risk of unauthorized access by third parties to data processed in the system [...] .

The position of the President of UODO is justified in the judgment of August 26, 2020 (file no. II SA / Wa 2826/19) of the Provincial Administrative Court in Warsaw, which ruled, inter alia, that Art. 32 of Regulation 2016/679 "(...) does not require the data controller to implement any technical and organizational measures that are to constitute personal data protection measures, but requires the implementation of adequate measures. Such adequacy should be assessed in terms of the manner and purpose for which personal data are processed, but also the risk related to the processing of such personal data, which may be characterized by a different amount, should be taken into account. " In addition, the Court also stressed that "[p] r measures are to be effective, in specific cases some measures will have to be low risk mitigating measures, others must mitigate high risk, but it is important that all measures (and every measure) separately) are adequate and proportional to the degree of risk. ".

As the University itself pointed out, the above-mentioned the measures turned out to be ineffective in the case of a malicious tool used (a backdoor file) which made it possible for an unauthorized person to gain access to personal data. In addition, in a letter of [...] January 2021, the University indicated that the login data used to place the backdoor files were probably obtained from the [...] system used for internal code exchange of software developed by employees, doctoral students and selected students. The above explanations, as well as the established facts, unquestionably, in the opinion of the President of the Personal Data Protection Office, indicate that the administrator focused his attention on the threats related to the functioning of the IT infrastructure, and not related to the functioning of the application created by the University's employees. This applies in particular to the area of functionality that allows you to upload files, which is a critical functionality from the point of view of IT systems security and good practices. This is especially important if you know that the files may come from untrusted sources. It is in the interest of each administrator to verify whether such functionality is properly secured, for example against the possibility of manipulating the paths on which they will be saved, and the files themselves are properly validated in terms of threats to the personal data being processed.

Verification of such functionalities and identification of threats resulting from the vulnerabilities that this functionality may contain should be carried out both at the design stage, in accordance with Art. 25 sec. 1 of Regulation 2016/679, and each time it is modified, which is the fulfillment of the obligations referred to in the above-mentioned in the article, as well as in art.

24 sec. 1, art. 32 sec. 1 lit. b) and d) or Art. 32 sec. 2 of Regulation 2016/679.

Art. 32 sec. 1 lit. d) of Regulation 2016/679 obliges the controller to regularly test, measure and evaluate the effectiveness of technical and organizational measures to ensure the security of processing, taking into account, inter alia, the context of processing, the state of technical knowledge, or the risk of violating the rights or freedoms of natural persons. Taking into account the context of processing in each organization should involve the identification of internal and external threats.

The administrator, when analyzing the risk for data processed in the IT system, especially available from the public network, should, in particular and with due diligence, identify threats, taking into account, for example, such circumstances as the scope of data processed, the number of application users, the nature of their rights and the conditions of the IT environment, in which the application functions, as well as the potential influence of third parties who gain unauthorized access to the application and may affect the confidentiality, integrity and availability of personal data processed. Taking into account the proprietary nature of the application [...], in the opinion of the President of the Personal Data Protection Office, failure to conduct a formal risk analysis, which would involve the need to conduct a security test aimed at detecting all vulnerabilities of the application, contributed to the violation, which is also confirmed by the recommendations contained in the Report on the preliminary forensic analysis. This is a violation of the principle set out in Art. 5 sec. 1 lit. f) Regulation 2016/679, i.e. the principles of confidentiality and integrity, which are reflected in the obligations set out in Art. 24 sec. 1, art. 25 sec. 1, art. 32 sec. 1 and art. 32 sec. 2 of Regulation 2016/679.

It is not possible to justify the indicated security measures as adequate to the risk by pointing to the perpetrator's action scenario that goes beyond the scheme adopted in the risk assessment, without presenting any evidence for it (risk analysis). It is difficult to talk about making certain assumptions about threats without conducting a full formal system audit, including penetration tests, and thus not being aware of the possibilities of a person gaining unauthorized access to an IT system. It should be clearly emphasized that when analyzing the risk in the adopted scenarios (vectors of a potential attack), one should be aware of the real possibilities of the attacker, taking into account e.g. social engineering methods, the state of technical knowledge, physical aspects of security, including ICT security, the attacker should be considered both from the point of view of a person unfamiliar with the administrator's organization and its IT infrastructure, as well as a person who has this knowledge.

Above Due to the lack of awareness of the threats resulting from the unidentified vulnerabilities of the system [...], it was only

after the infringement and the recommendations of the intrusion analysis that the Administrator decided to "[...] not develop and shut down the system from use" (explanations from [...] September 2020). Considering the 10-year period of operation of the application [...] and the Administrator's explanations on how to maintain it, it should be stated that the care for the protection of data processed using this application was ad hoc, and the obligations resulting from Regulation 2016/679, including the transitional period to adapt this area to the new provisions on the protection of personal data, were not an impulse for full verification of security and identification of vulnerabilities.

Explaining the issues related to the protection of passwords in the application [...], the administrator pointed out that the passwords were stored in the form of MD5 hash without salt, ie an additional random parameter of the encryption function, and their complexity was limited to [...]. The university indicated that work on the implementation of a new method of storing passwords was ongoing, but not completed and implemented.

The President of the Personal Data Protection Office points out that the use of the hash function (also known as hashing) in relation to passwords stored in ICT systems is one of the most common measures to ensure the confidentiality of a password and limit its knowledge only to the person who uses it. In this way, the negative consequences related to the potential risk of using such a password by a person who unauthorized access to it are limited. A person who knows the user's credentials for a specific service can freely access their account. It should be noted that, in the present case, such a situation could lead to, for example, identity fraud. Moreover, the user could use the same username and password on other websites.

Although the use of the hash function does not completely eliminate the likelihood that an unauthorized person will reverse the process and obtain the password content, its proper execution makes password cracking attacks time-consuming and even impractical. The purpose of such a process is, inter alia, obtaining adequate time for taking remedial actions both by the administrator and the data subject, especially in cases where the administrator does not find a breach of personal data protection at a time close to its actual occurrence. Therefore, when deciding on such a solution, the administrator should assess whether it will actually fulfill its role. The use of the hash function based on the MD5 algorithm (without additional security techniques) and limiting the complexity of the password protected in this way to [...], in the opinion of the President of the Personal Data Protection Office, constitutes an insufficient technical measure, which constitutes a violation of Art. 32 sec. 1 of Regulation 2016/679. The weakness of the MD5 algorithm is widely known, and its use in current ICT systems is not recommended. In addition, despite the use of password complexity in the above-mentioned scope, the applied algorithm

reduces the time-consuming effect of obtaining the original content of the password.

In the opinion of the President of the Personal Data Protection Office, it is therefore essential that the controller, as part of the implementation of the obligations arising from Regulation 2016/679, periodically verifies whether the technical and organizational solutions used do not contain any weaknesses that may affect the risk of violating the rights or freedoms of data subjects. Guidelines in this regard are issued, inter alia, by European Union Agency for Cybersecurity ENISA, e.g. "Algorithms, key size and parameters report 2014" (available at https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014). The lack of such verification determines the violation by the University of art. 25 sec. 1 of Regulation 2016/569. It should be emphasized that the concept resulting from this provision is based on the proactive and preventive approach of the controller consisting in ensuring the security of personal data at every stage. The adoption of such solutions by the EU legislator aims to strengthen the confidentiality principle expressed in Art. 5 sec. 1 lit. f) of Regulation 2016/679, in order to ensure the necessary security of the processed data, corresponding to the risks related to their processing. The lack of actions of the administrator in this regard also constitutes a violation of Art. 24 sec. 1, art. 32 sec. 1 lit. d) and art. 32 sec. 2 of Regulation 2016/679 by failing to take into account the risk associated with the processing of users' passwords in the form of a hash function, the weakness of which is commonly known, which in the event of failure to apply other technical and organizational measures to ensure secure processing, in accordance with the above-mentioned the provisions of Regulation 2016/679, provides for the exposure of data subjects to an increased risk of violating the rights or freedoms of natural persons in the event of a breach of the confidentiality of the data processed.

In reference to regular testing, measuring and assessing the effectiveness of technical and organizational measures, the University, apart from indicating that it uses software to search for application vulnerabilities, indicated that it does not analyze the internal logs of the system (explanations from [...] September 2020). As can be seen from the administrator's explanations and from the Initial Breakdown Analysis, the configuration of the server on which the [...] application was located resulted in the deletion of logs (system logs) after 4 weeks, and the analysis of the legitimacy of adopting such a log storage period was not performed. In addition, from the above-mentioned The preliminary analysis shows that the application operating the system [...] itself did not have a log of events detailed enough to identify any traces of the origin of the first file that was used by an unknown and unauthorized person to access the database.

In accordance with the principle of accountability, the controller should demonstrate, in particular, that the data is processed in accordance with the requirements of Regulation 2016/679, regarding the fulfillment of the requirements for the application of appropriate technical and organizational measures to ensure that the processing takes place in accordance with the confidentiality requirements set out in the regulations. , data integrity and availability. It should be emphasized that the principle of accountability is directed both outside the organization and inwards. For this purpose, in addition to introducing general mechanisms that log basic events in the IT system, the administrator should analyze, taking into account the scope, context and purposes of processing, at what level of detail and for which period of time events should be recorded in order to maintain compliance of data processing in the organization with provisions on the protection of personal data. It is commonly assumed that accountability in IT systems is carried out in the form of automatically generated records (the so-called logs) containing a specific set of information that allows to identify who, when, what operations, for what data was performed in the system. The detail of log records is an individual matter, depending on the implemented functionalities and user tasks. In the context of the processing of personal data, the controller should also be able to demonstrate that the persons authorized to process personal data process them in accordance with the principles set out in Regulation 2016/679, i.e. only when it is necessary to obtain a specific processing purpose and to the extent it is essential.

The principle of accountability set out in Art. 5 sec. 2 of Regulation 2016/679 has been detailed in Art. 24 sec. 1 and art. 32 sec. 1 of this regulation, which imposes an obligation on the controller to implement appropriate technical and organizational measures so that the processing takes place in accordance with the regulation and to be able to demonstrate it. When implementing these measures, the controller should take into account the nature, scope, context and purposes of the processing as well as the risk of violation of the rights or freedoms of natural persons with different probability and severity. Considering the above, the allegation of infringement of these articles in connection with joke. 5 sec. 2 of Regulation 2016/679. Failure by the University to sufficiently take into account this principle in the process of using the IT system used to process personal data and failure to undertake analytical activities of system logs, as part of the obligation to monitor the adequacy of security, in the opinion of the supervisory body, based on the collected evidence, contributed to the materialization of threats in the form of obtaining unauthorized access to the IT system and the personal data processed therein. Moreover, the data protection system functioning in such a way does not guarantee the controller's full readiness to respond to threats, and if they materialize, take appropriate preventive and remedial measures to minimize the risk of a recurrence of the breach.

Pursuant to § [...], each IT system used to process data must, inter alia, ensure: confidentiality, integrity, authenticity, accountability and non-repudiation. In accordance with § [...], the obligation to ensure these attributes of information security rests with the IT system administrator and computer network administrators. Taking into account the established facts and the above-mentioned allegation of not carrying out a risk analysis for data processed in the system [...], it is justified to conclude that the Administrator did not fully comply with the provisions of the above-mentioned [...] and [...], constituting Appendix No. [...] to Regulation No. [...] of the Rector of the Warsaw University of Technology, according to which, when estimating the probability of an incident, the types of vulnerability, existing safeguards as well as experience and statistics on similar events should be taken into account in particular .

The provisions of Regulation 2016/679 oblige both controllers and processors to adopt appropriate technical and organizational measures to ensure a level of security corresponding to the risk related to the processing of personal data. The above-mentioned provisions, as well as recital 87 of Regulation 2016/679, also show that the regulation required the adoption of the above-mentioned measures to immediately find a breach of personal data protection. This is decisive for determining whether the obligations under Art. 33 sec. 1 and art. 34 sec. 1 of Regulation 2016/679.

The obligation to notify the supervisory authority about the breach and the deadline for its submission is related to the moment when the controller "detects" the breach of personal data protection. The Article 29 Working Party, in the guidelines on reporting personal data breaches pursuant to Regulation 2016/679, adopted on October 3, 2017, last amended and adopted on February 6, 2018 (hereinafter: breach notification guidelines), indicates that the controller finds a breach as soon as it has obtained reasonable certainty that a security incident has occurred that led to the disclosure of personal data. However, this issue should be considered in relation to the controller's obligation to maintain the ability to quickly and effectively identify any breaches to ensure that appropriate action can be taken. In some cases, it may take time to determine whether personal information has been disclosed. Considering the circumstances in which the Administrator learned about the breach (information from a third party) and the collected evidence and the facts established on its basis, it cannot be concluded that the administrator has implemented appropriate technical and organizational measures allowing for quick detection and investigation of the incident in in order to determine whether and how a breach of personal data protection occurred, and if so - take remedial action and, if necessary, report the breach and notify data subjects of the breach of personal data protection. Even the conclusion that the administrator would not have made a finding of a breach without a signal from a third party seems

legitimate, and some of the findings made in the Pre-intrusion analysis would be impossible, for example by not analyzing the legitimacy of a 4-week storage of logs (event logs) in a virtual machine. Only after the violation, as a result of the recommendation contained in the above-mentioned analysis, the controller changed the current practice and extended the log storage period to [...] weeks. In connection with the above, the President of the Personal Data Protection Office finds that the University violates Art. 5 sec. 1 lit. f), art. 5 sec. 2, art. 24 sec. 1, art. 25 sec. 1, art. 32 sec. 1 and art. 32 sec. 2 of Regulation 2016/679.

Pursuant to the wording of Art. 34 sec. 1 of Regulation 2016/679, if the breach of personal data protection may result in a high risk of violation of the rights or freedoms of natural persons, the controller shall notify the data subject of such a breach without undue delay.

Again, the Guidelines on Notification of Breaches, which indicate that when notifying individuals about a data breach, the controller should be transparent on this matter and provide information in an efficient and timely manner. When analyzing the meaning of the term "without undue delay" under this provision, it should be assumed that the beginning of the time limit for notifying data subjects is the moment of finding the infringement. In the case being the subject of this decision, the Administrator, immediately after finding the violation, notified the data subjects about it, providing them with all the information referred to in art. 34 sec. 2 of Regulation 2016/679.

As a result, the President of the Personal Data Protection Office (UODO) discontinued the administrative proceedings regarding the violation of Art. 34 sec. 1 of Regulation 2016/679.

Bearing in mind the above findings, the President of the Personal Data Protection Office, exercising his powers specified in art. 58 sec. 2 lit. i) Regulation 2016/679, pursuant to which each supervisory authority has the power to apply, in addition to or instead of other remedial measures provided for in Art. 58 sec. 2 lit. a-h and lit. (j) of that Regulation, an administrative fine pursuant to Article 83 of the Regulation 2016/679, having regard to the circumstances established in the present proceedings, stated that in the case under consideration there were premises justifying the imposition of an administrative fine.

When deciding to impose an administrative fine on the Warsaw University of Technology, as well as determining its amount, the President of the Personal Data Protection Office - pursuant to Art. 83 sec. 2 lit. a-k of the regulation 2016/679 - took into account the following circumstances of the case, aggravating and affecting the size of the imposed financial penalty: 1. The nature and gravity of the infringement taking into account the number of people injured (Article 83 (2) (a) of Regulation

2016/679) - when imposing the penalty, it was important that the number of people affected by the infringement was 5,013. resulting from the nature of the data, a large number of data subjects, possibly the ill will of the person who has obtained unauthorized access to them, as well as a large-scale processing. Violation of confidentiality of the telephone number, e-mail address or PESEL number of the above-mentioned persons may result in entry into the private life of those affected. In relation to the above-mentioned of persons, there is still a high risk of unlawful use of their personal data, as the purpose for which a person or unauthorized persons may take unlawful actions is unknown. Data subjects may therefore suffer material damage, and the very breach of data confidentiality is also non-pecuniary damage (harm). This is because data subjects may, at the very least, feel the fear of losing control of their personal data, of identity theft or identity fraud, and finally of financial loss. In summary, the breaches found in the present case are of a significant and serious nature and are likely to adversely affect the data subjects. 2. Duration of the infringement (Article 83 (2) (a) of Regulation 2016/679) - the President of UODO considers the long duration of the infringement of the provisions of the General Data Protection Regulation to be an aggravating circumstance. From the information obtained by the supervisory authority in the course of the administrative proceedings, it appears that the above-mentioned the infringement of the regulations continued uninterruptedly from May 25, 2018, i.e. from the date of application of Regulation 2016/679, until the end of the incident, i.e. until [...] May 2020, when the server and the software were disconnected from the network.3 . High degree of responsibility of the controller (Article 83 (2) (d) of Regulation 2016/679). Considering that it is the controller who is responsible for assessing the security measures at every stage of processing, especially with regard to technological solutions created without the support of professional external entities, and only on the basis of its own human resources and technological knowledge, implemented in the University's organization by its employees over a period of about 10 years, it should be stated that the Warsaw University of Technology has not implemented appropriate technical and organizational measures to ensure the security of personal data processing. 4. Categories of personal data affected by a breach of personal data protection (Article 83 (2) (g) of Regulation 2016/679) - personal data accessed by an unknown and unauthorized third party does not belong to special categories of personal data for which referred to in Art. 9 of Regulation 2016/679, however, their wide scope (name and surname, parents' names, date of birth, address of residence or stay, PESEL number, e-mail address, username, password, mother's maiden name, series and number of ID card, and telephone), is associated with a high risk of violating the rights or freedoms of natural persons. At this point, it should be emphasized that, in particular, unauthorized disclosure of such a data category as a PESEL number (in

combination with a first and last name) may have a real and negative impact on the protection of the rights or freedoms of natural persons. PESEL number, i.e. an eleven-digit numeric symbol, uniquely identifying a natural person, containing the date of birth, serial number, gender and a control number, and therefore closely related to the private sphere of a natural person and also subject to exceptional protection as a national identification number under Art. 87 of Regulation 2016/679 is a data of a special nature and requires such special protection. Special protection of personal data, including in particular the PESEL number, is also required from public institutions, which undoubtedly include the party to the proceedings in question.

When determining the amount of the administrative fine, the President of the Personal Data Protection Office also took into account the mitigating circumstances affecting the final penalty, i.e. 1. Unintentional nature of the breach (Article 83 (2) (b) of Regulation 2016/679) - no intentional actions of the controller aimed at violating the provisions on the protection of personal data were found at any stage of the proceedings. 2. Actions taken by the controller to minimize the damage suffered by data subjects (Article 83 (2) (c) of Regulation 2016/679) - Warsaw University of Technology has taken additional measures, going beyond the legal obligation, to mitigate or remunerate harm suffered by persons affected by the violation, i.e. "The University finances the costs of securing personal data in a standard service for a period of 12 months", as well as "[...] all affected persons may apply for reimbursement of basic costs incurred to secure their personal data. The basis for the return is confirmation of the status of the person whose personal data has been disclosed "(supplementary notification of [...] May 2020 and explanations of [...] June 2020) 3. All relevant previous violations by the administrator (Article 83 (2) (e) of Regulation 2016/679) - no previous violations of the provisions of Regulation 2016/679 by the University were found.

The other, specified in Art. 83 sec. 2 of Regulation 2016/679, the circumstances: 1. The degree of cooperation with the supervisory body in order to remove the violation and mitigate its possible negative effects (Article 83 (2) (f) of Regulation 2016/679) - the University has independently taken a number of actions to remove the violation and mitigate its possible negative effects. Above the activities were autonomous and were not subject to any consultation with the supervisory authority. 2. The way in which the supervisory body learned about the breach (Article 83 (2) (h) of Regulation 2016/679) - the breach of personal data protection was reported to the President of the Personal Data Protection Office by the Warsaw University of Technology, which is the fulfillment of the obligation imposed on it by the Warsaw University of Technology, referred to in Art. 33 of the Regulation 2016/679. The Article 29 Working Party in the Guidelines on the application and setting of administrative fines for the purposes of Regulation 2016/679 (WP 253 17 / PL) emphasizes that “Pursuant to the Regulation, the controller is

required to notify the supervisory authority of a breach of personal data protection. Mere compliance with this obligation by an administrator cannot be interpreted as a weakening / mitigating factor ". 3. In the same case, the measures referred to in Art. 58 sec. 2 of Regulation 2016/679 (Article 83 (2) (i) of Regulation 2016/679). The Warsaw University of Technology does not apply the approved codes of conduct pursuant to Art. 40 of the Regulation 2016/679 or approved certification mechanisms pursuant to Art. 42 of the Regulation 2016/679 (Article 83 (2) (j) of the Regulation 2016/679). 5. It was not found that the Administrator obtained financial benefits or avoided the losses referred to in art. 83 sec. 2 lit. k of Regulation 2016/679.

Referring to the amount of the administrative fine imposed on the University, the President of the Office for Personal Data Protection decided that in the established circumstances of this case - i.e. in the event of a violation of the provisions of Art. 5 sec. 1 lit. f), art. 5 sec. 2, art. 25 sec. 1 and art. 32 sec. 1 and 2 of Regulation 2016/679 and the fact that the University is a body of a public finance sector unit - Art. 102 of May 10, 2018 on the protection of personal data (Journal of Laws of 2019, item 1781), which results in the limitation of the amount (up to PLN 100,000) of an administrative fine that may be imposed on a public finance sector entity.

Taking into account all the above-mentioned circumstances, the President of the Office for Personal Data Protection decided that the imposition of an administrative fine in the amount of PLN 45,000 (forty-five thousand PLN) on the Warsaw University of Technology is necessary and justified by the weight, nature and scope of the violations made by the Warsaw University of Technology. At this point, it should be emphasized that the application to the University of any other remedy provided for in Art. 58 sec. 2 of Regulation 2016/679, and in particular stopping at an admonition (Article 58 (2) (b)), would not be proportionate to the identified irregularities in the processing of personal data and would not guarantee that the University will not commit further negligence in the future.

In the opinion of the President of the Personal Data Protection Office, the administrative fine applied performs the functions referred to in Art. 83 sec. 1 of Regulation 2016/679, i.e. it is effective, proportionate and dissuasive in this individual case. The administrative fine will perform a repressive function in these specific circumstances, as it will be a response to the violation by the Warsaw University of Technology of the provisions of Regulation 2016/679, but also preventive, i.e. preventing violations of the provisions on the protection of personal data in the future by both the Warsaw University of Technology and other administrators data.

The purpose of the imposed penalty is to ensure that the Warsaw University of Technology performs its duties properly, in

particular in Art. 5 sec. 1 lit. f), art. 5 sec. 2, art. 24 sec. 1, art. 25 sec. 1, art. 32 sec. 1 and 2 of Regulation 2016/679, and consequently to conduct data processing processes in accordance with applicable law.

Bearing in mind the above, the President of the Personal Data Protection Office resolved as in the operative part of this decision.

2022-01-11