THE CHAIRMAN OF PERSONAL DATA PROTECTION

Warsaw, on 21

of August

2020

DECISION

ZSOŚS.421.25.2019

Based on Article. 104 § 1 of the Act of 14 June 1960 Code of Administrative Procedure (Journal of Laws of 2020, item 256), art. 7 sec. 1, art. 60, art. 102 paragraph 1 and sec. 3 of the Personal Data Protection Act of May 10, 2018 (Journal of Laws of 2019, item 1781) and art. 57 sec. 1 lit. a, art. 58 sec. 2 lit. d and lit. and in connection with Art. 5 sec. 1 lit. e and lit. f, art. 5 sec. 2, art. 24 sec. 1, art. 25 sec. 1, art. 32 sec. 1 lit. b. and lit. d, art. 32 sec. 2, art. 38 sec. 1, art. 39 sec. 1 lit. b and art. 39 sec. 2, art. 30 sec. 1 lit. d, as well as art. 83 sec. 1 - 3, art. 83 sec. 4 letter 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 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 the Warsaw University of Life Sciences, at ul. Nowoursynowska 166, President of the Personal Data Protection Office,

1) finding a violation by the Warsaw University of Life Sciences, at ul. Nowoursynowska 166, the provisions of art. 5 sec. 1 lit. e, art. 5 sec. 1 lit. f, art. 5 sec. 2, art. 25 sec. 1, art. 32 sec. 1 lit. b, art. 32 sec. 1 lit. d, art. 32 sec. 2, art. 38 sec. 1, art. 39 sec. 1 lit. b and art. 39 sec. 2 of the Regulation of the European Parliament and of the EU Council 2016/679 of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46 / EC (general regulation on data protection) (Journal of Laws UE L 119 of 04/05/2016, page 1, as amended), hereinafter: "Regulation 2016/679", imposes a fine on the Warsaw University of Life Sciences in Warsaw in the amount of PLN 50,000 (fifty thousand) ;

2) in the remaining scope, the proceedings are discontinued.

JUSTIFICATION

Warsaw University of Life Sciences (SGGW) or the "University") notified the President of the Personal Data Protection Office

(hereinafter also referred to as the "President of the Personal Data Protection Office") of a breach of personal data protection of candidates for studies at SGGW, which was registered under with the reference number ZWAD.405.5471.2019.

From [...] to [...] November 2019, pursuant to Art. 78, art. 79 sec. 1 and art. 84 sec. 1 points 1-4 and art. 86 sec. 1 of the Act of May 10, 2018 on the Protection of Personal Data (Journal of Laws of 2019, item 1781) in connection with joke. 57 sec. 1 lit. a and lit. h, art. 58 sec. 1 lit. b, lit. e and lit. f of the Regulation 2016/679, in order to control the compliance of personal data processing with the provisions on the protection of personal data, control activities were carried out at the Warsaw University of Life Sciences, at ul. Nowoursynowska 166. The scope of the control covered the processing by the Warsaw University of Life Sciences, the personal data of persons affected by a personal data breach, notified to the President of the Personal Data Protection Office and registered under the reference number ZWAD.405.5471.2019.

In the course of the inspection, oral explanations were collected from persons employed at WULS-SGGW and persons providing services to it, and the IT system used to process personal data of candidates for studies at WULS-SGGW was inspected. The actual state of affairs was described in detail in the inspection protocol signed by the rector of WULS-SGGW.

On the basis of the evidence collected in the case, it was established that in the process of processing the personal data of candidates for studies at WULS-SGGW, the University, as the administrator, breached the provisions on the protection of personal data. The breach of the law consisted in:

1) the controller insufficiently assesses the effectiveness of technical and organizational measures to ensure the security of the processing of personal data of candidates, which constitutes a violation of Art. 5 sec. 1 lit. e, art. 5 sec. 1 letter f, art. 5 sec. 2, art. 24 sec. 1, art. 25 paragraph 1, art. 32 sec. 1 letter b, art. 32 sec. 1 lit. d, art. 32 sec. 2 and art. 38 sec. 1 of Regulation 2016/679;

2) failure by the administrator to sufficiently take into account the principles of accountability when using the system for processing personal data of candidates, which constitutes a violation of art. 5 sec. 2 of Regulation 2016/679;

3) fulfillment of tasks by the data protection officer without due consideration of the risks associated with processing operations, which constitutes a breach of art. 24 sec. 1, art. 32 sec. 1, art. 32 sec. 2, art. 38 sec. 1, art. 39 sec. 1 lit. b and art. 39 sec. 2 of Regulation 2016/679;

4) failure to include all information required by the provisions of Regulation 2016/679 in the WULS-SGGW register of personal data processing activities with regard to the processing of personal data of candidates for first-cycle, second-cycle and

long-cycle studies at WULS-SGGW, which constitutes a breach of Art. 30 sec. 1 lit. d of Regulation 2016/679.

On the basis of the collected evidence, it was established that the breach of personal data protection of applicants for studies at WULS-SGGW, which took place on [...] November 2019, was related to the theft of a private computer of an employee of WULS-SGGW - Mr. AG, who is also the secretary of the University Recruitment Committee of WULS-SGGW . The stolen laptop was used by the above-mentioned an employee for private and business purposes, including the processing of personal data of candidates for studies at WULS-SGGW for the purposes of recruitment as a secretary of the University Recruitment Committee. From the Candidate Service System used to process personal data of candidates for 1st and 2nd cycle studies and uniform master's studies (hereinafter also referred to as: "SOK"), using the functionality implemented therein, he imported sets of personal data to his private computer, including name, surname, family name, parents' names, PESEL identification number, gender, nationality, citizenship, residence address, series and number of an identity card or other identity document, including a passport, mobile and / or landline telephone number, information on previous education, information on qualifications for studies (the full list of personal data categories for individual reports available as part of the data export functionality is attached as Annex 59 to the inspection protocol). The university, being the administrator of this personal data, did not have information about this fact. This operation was also not registered in SOK. Mr. A.G. he prepared the downloaded data sets for qualification by filtering them appropriately in the spreadsheet according to the appropriate qualification criteria, which are specified for individual fields of study, and then presented at the qualifying meeting of the recruitment committee. Based on the collected sets of personal data, Mr. A.G. he also prepared final reports with statistical summaries according to selected criteria. He had a recruitment directory for a specific year on the stolen computer, in which he stored various report and base files, as well as other documents, such as replies to letters on recruitment-related matters.

This breach of personal data protection concerns candidates for studies at WULS-SGGW from the last 5 years and the calculations carried out by the University show that it covers 81 624 records (entries) in the Candidate Service System. The above number is not an exact number of people whose personal data is affected by the breach, as within 5 years the same person could have applied for a different recruitment or applied for a second degree. In the initial notification of a personal data breach to the President of the Office for Personal Data Protection [...] on November 2019, the likely number of 100,000 data subjects was indicated as the upper limit.

In connection with the above, in a letter of [...] March 2020 (reference number: ZSOŚS.421.25.2019), the President of the

Personal Data Protection Office (UODO) initiated ex officio administrative proceedings regarding the identified deficiencies, in order to determine the compliance of the processing of personal data of candidates for studies at WULS-SGGW with the provisions on protection of personal data.

In response to the notice of initiation of the administrative procedure contained in the letter of [...] April 2020 ([...]), supplementary letters of [...] June 2020 ([...]) and [...] July 2020 . ([…]) And in letters of […] December 2019 ([…]), […] January 2020 ([…] […] January 2020 ([…]) and […] January 2020 ([...]), the Rector of the Warsaw University of Life Sciences submitted explanations in which he indicated, inter alia, that:

1) The allegation of lack of reviews and updating of documentation introduced by the order of the Rector of the Warsaw University of Life Sciences 88/2013 of 03/12/2013 on the Security Policy (hereinafter: "Security Policy") and Instructions for managing the IT system used for data processing (hereinafter also referred to as : "IT system management instruction") is devoid of factual and legal grounds, and is in contradiction with the current recommendations of the President of the Office for Personal Data Protection regarding the keeping of documentation of the processes constituting the protection of personal data in the organization. In the opinion of the University, the documentation in force at WULS-SGGW is not only largely up-to-date, despite the passage of time since its implementation, but is also subject to ongoing updating works aimed at adapting it to the requirements of Regulation 2016/679.

In the opinion of the University of the above-mentioned the documents met the assumptions of the data protection strategy, although they were introduced on the basis of the regulation of the Minister of Internal Affairs and Administration of April 29, 2004 on the documentation of personal data processing and technical and organizational conditions that should be met by devices and IT systems used to process personal data (Journal .U. 2004 No. 100, item 1024). WULS-SGGW points out that the implementation of these solutions made it possible to conclude that the entity complied with the data security requirements and still meets them, although the current provisions on the protection of personal data are slightly different, as general requirements are indicated, including the requirement to conduct a risk analysis and selection of security measures. appropriate for this type of risk, and the EU legislator did not provide for the issuing of executive regulations specifying specific types of security, thanks to which WULS-SGGW, as an administrator, gained greater freedom in the selection of securities, associated with greater responsibility for their selection.

In the opinion of the University, the notice of initiation of the procedure completely ignored the fact that the policy was updated

with the obligatory elements imposed on the administrator under the regulation, such as: a register of processing activities and a register of processing activities (Article 30 of Regulation 2016/679), procedures for reporting data breaches to the supervisory authority (Article 33 (3) of Regulation 2016/679), procedures for keeping an internal register of data protection breaches referred to in Art. 33 paragraph. 5 of Regulation 2016/679. As evidence, the University indicates the e-mails of data protection inspectors - from [...] October 2019, about the need to update the register and sub-registers of processing activities (contained in the control files), from [...] May 2019 about the need to keep a register (sub-registers) of processing activities (attachment to the response to the initiation of proceedings) and of [...] September 2019 on the need to keep a register of infringements (attachment to the response to the initiation of proceedings). It was also indicated that the WULS-SGGW established rules guaranteeing safe work in mobile computing (the procedure of using portable computers) and extensive activities aimed at the implementation of a comprehensive personal data protection policy in the wording corresponding to the content of Regulation 2016/679 and replacing the currently applicable policy safety.

2) It is incorrect to say that the administrator has failed to demonstrate that the procedures applicable at WULS-SGGW are monitored on an ongoing basis and adjusted to the data processing processes. The university indicates that from the beginning of 2018 it versioned and implemented appropriate documentation adapted to the content of the 2016/679 regulation. In addition, the University does not agree with the fact that data protection inspectors did not carry out audits of units, because, according to the explanations and documentation, data protection inspectors held regular meetings in organizational units of the administrator - including at the Student Affairs Office. During meetings with employees of the units, the most urgent needs and doubts related to the processing of personal data were discussed. In addition, the current documentation related to the processing of personal data and procedures were analyzed, and recommendations were also issued. According to the records of meetings of the data protection officer - [...], during the 5 months of his function, he made several visits to individual organizational units of the University. WULS-SGGW also points to the activities of two previous employees holding the function of a data protection officer, including: organizing trainings with University employees, meetings with representatives of units, preparing and implementing versioned documents. One of the documents indicating this is the attachment to the letter of [...] July 2020 entitled "Dates of consultations / training in specific areas" concerning the work of one of the previous data protection officers - Mr. A.G. In addition, the University's assessment should take into account the appointment of a task force chaired by [...], which aims to implement changes resulting from the audit task entitled "Optimization of IT Resources" and

educational activities of the IT Center of the Warsaw University of Life Sciences, including: on informing about good practices in the field of security, developing, together with the Data Protection and Information Security Inspectorate, messages related to the correct conduct in the field of personal data security addressed to employees of university organizational units, as well as providing a tab on the Intranet for employees regarding the protection of personal data which is constantly expanded.

In addition, the University mentioned the activities it had carried out in the IT area before the control activities, i.e. the creation of a new server room in the IT Center (including [...] implemented), user authentication as part of the extensive university-wide wireless network, approval, implementation and application of the "Broadcasting Procedure" / modification / revoking of authorizations to the IT system ”and providing employees with secure shared disk resources without the need to save information on computers and portable devices.

In recent months, as indicated by the University, in the IT area, among others, the following actions: limiting copying of data to external drives for administration employees with access to the most important IT systems in which personal data are processed; permanent removal of data from media when transferring computers between organizational units using dedicated software and updating the "Standard for computer workstation configuration" introducing the obligation to apply additional security.

WULS-SGGW also presented the activities that are underway, i.e. the implementation of solutions on computers (especially portable) enabling the encryption of computer drives and external media, implementation of a common domain of the entire University and adding to it all computers used by University employees, which through central and unified management is to increase the security of users and digital assets.

In addition, the University indicated that intensive activities were launched to evaluate the University's IT systems, within which personal data are processed. As part of the actions taken, a table was sent to all organizational units of the University (letter No. [...] of [...] November 2019 supplemented by letter No. [...] of [...] January 2020) with specific requirements for data processing systems personal data, enabling the assessment of the compliance of these systems with: the Security Policy, the IT System Management Manual and Regulation 2016/679. Based on the feedback collected from the University's organizational units, an analysis was carried out, as a result of which the Rector of the University, in a letter of [...] February 2020 (attachment to the response to the initiation of the procedure), presented the conclusions resulting from the analysis and proposed actions to improve IT security. These activities were developed, presented to the Rector in a letter of [...] April 2020

and were approved by him for implementation (Annex to the letter of [...] June 2020).

In addition, the University, as part of the plans adopted by the University Senate (resolution of the Senate of the Warsaw University of Life Sciences of [...] February 2020), secured funds in 2020 for the implementation of planned activities increasing the level of IT security, i.e. construction and implementation of a new system to support the recruitment of candidates , audit of IT systems in the field of architecture, security and performance, adaptation of central IT systems to the requirements of Regulation 2016/679, development of the ICT incident management process, implementation of business continuity procedures and plans, development of an ICT security policy.

3) WULS-SGGW does not agree with the allegation of violation of Art. 32 sec. 2 of Regulation 2016/679 by failing to perform the risk analysis related to the processing of personal data of candidates for studies at the Warsaw University of Life Sciences. The university emphasized that the risk analysis for the recruitment process dated [...] May 2019, submitted with the letter of [...] December 2019, had been carried out. In the opinion of the University, the above is confirmed by the document of the previous data protection officer, Mr. A.G. Fri "Dates of consultations / training in specific areas" (the document was attached to the letter of [...] July 2020). The methodology on the basis of which the above analysis was prepared was also attached to the letters of [...] June and [...] July 2020. In addition, in a letter of [...] June 2020, the University presented a new risk analysis for the processing of personal data in the recruitment process and the methodology on the basis of which this analysis was performed. Along with these documents, a recovery plan was presented, setting out the priorities in the administrator's activities to maximize the effectiveness of technical and organizational measures to ensure the security of personal data processing of candidates for studies at WULS-SGGW, which is to be implemented in accordance with the schedule indicated therein.

The university indicated that each of the persons holding the function of a data protection officer took steps to perform an analysis of risks related to personal data processing operations, indicated the need for their implementation or presented their methodology with risk assessment related to personal data processing operations. This is to prove that there are no grounds to question the performance of the analysis on the date indicated thereon, i.e. [...] May 2019. It was also emphasized that Regulation 2016/679 does not indicate a specific method of conducting and documenting the risk management process, but it is important that the methodology used gives a reliable and objective risk assessment. In addition, the University indicated that, in accordance with the accountability principle, Regulation 2016/679 requires the risk assessment process to be carried out

and documented - in order to demonstrate that the risk has been assessed and appropriate protection measures have been implemented. The university indicated that in practice, the risk assessment is in most cases performed in an electronic version, not requiring a signature or even a date (indicating the use of a spreadsheet or external dedicated tools).

With regard to the allegation of errors and omissions in the content of the risk analysis itself and its result, she pointed out that the risk analysis sheet is not an independent document, but correlated mainly with the Security Policy in force at the Warsaw University of Life Sciences. The university emphasizes that although there are some inaccuracies in the analysis, and the risk assessment itself is evaluable, it did it.

Explaining examples of inaccuracies in the risk analysis indicated in the notice of initiation of the procedure, WULS-SGGW argued that in point 3.3.9, one of the threats was indicated as "failure to control compliance with data protection policy and procedures (no audits)", the probability of which was assessed at the level of 1 (low probability), while the impact on the rights and freedoms of the data subject was rated at level 4 (medium impact). As a remedy, updating the data protection policy was indicated, which resulted in determining the impact on the rights and freedoms of data subjects at a negligible level. In the same paragraph referring to this point, WULS-SGGW indicated that, in its opinion, it was impossible to agree with the conclusion that the update of the Security Policy was not carried out, because the updates of the binding documents constituting the Security Policy were carried out by versioning the aforementioned individual documentation. incl. authorizations, regulations, registers. In the administrator's opinion, at this point the assessment was carried out correctly - the negligible probability was due to the ongoing work on versioning the documentation that make up the personal data protection policy at the University. In the remaining scope, i.e. in point 3.3.16, 3.3.19 above analysis, the University indicated that the analysis clearly stated that the measures had been implemented, but require updating, as well as the planned measure is the need to narrow the scope of personal data processing depending on the needs, and to prevent the system from being opened outside the areas specified in the Rector's Order No. 88 / 2013, i.e. preventing logging into the system outside the SGGW network. Thus, in the University's assessment, the risk was correctly identified in the final conclusions, and the recommendations clearly defined the scope of the proposed technical safety measures to minimize the probability.

In addition, the University indicated that, since December 2018, extensive work has been carried out by a designated task force on the optimization of IT systems and the operation of the Candidate Service System has been improved, in accordance with the recommendations resulting from the risk analysis, e.g. by limiting the functionality in the form of logging in and data

import.

4) WULS-SGGW does not agree with the allegation that appropriate organizational measures have not been implemented. Attention was paid to the content of the IT system management manual, according to which on page 17, in point 7 entitled: "Storage of information media containing personal data", in point 7.5 it is indicated that "personal data should not be taken out in the form of printouts and on portable media outside the processing area without just cause ". It was emphasized that this applies to all printouts and carriers, regardless of the type of their property (private / business WULS-SGGW) and it proves the implementation of appropriate organizational solutions aimed at securing the processed personal data.

The university indicated that Mr. A.G. he was not authorized to process personal data on a private medium, thus his operation was inconsistent with the regulations in force at the University. The University has in place the "Procedure for the use of portable computers", which is an attachment to the Instructions for managing the IT system used for data processing, specifying the methods of dealing with portable computers used to process personal data, in order to ensure security against theft and access by unauthorized persons, and data processing personal data outside the processing areas specified in the Security Policy may only take place in special cases and with the consent of the administrator. Moreover, it was noted that Mr. A.G. he did not inform that he was carrying out activities on a private computer, and he did not apply for a laptop business computer despite such a possibility (which was confirmed in the inspection report - in the explanations provided by [...] and [...]).

In the opinion of the University, procedures that expressly prohibit the use of private equipment for the processing of personal data constitute a security measure provided for in Art. 32 of Regulation 2016/679, i.e. an organizational measure. At the same time, the University indicated that, in accordance with the Security Policy, common organizational measures have been introduced in its area, which are updated and versioned over time to meet the requirements of the regulation, including the Security Policy has been developed and implemented (it is updated); users must be authorized in writing to process personal data (new authorization templates have been developed); records of persons authorized to process personal data are kept (the obligation is imposed on the data protection officers and on the ABI / IOD as the supervising person) on the terms specified in the IT system management manual; each user is obliged in the form of a written statement constituting Annex 2 to the IT system management manual and on the terms set out in point 3.2 of this manual to keep secret personal data and information about their security; a data protection officer has been appointed; the person acting as the personal data protection officer is

obliged to define the area of personal data processing, using the recommendations resulting from Annex 1 to the Security Policy, in particular by developing the "List of rooms constituting the data processing area together with a description of the security applied" which is with Annex No. la to the Security Policy - on page No. 3 of Annex No. 1 to the Security Policy, the area of personal data processing for the set of "applicants for studies" is specified at Nowoursynowska 166, 02-787 Warsaw. In addition, it was indicated that WULS-SGGW undertakes additional measures to update organizational measures aimed at increasing the security of personal data processed, including: establishing, from [...] December 2019, cooperation with an external entity specializing in data protection which currently performs a number of activities supporting the University in the area of personal data protection and information security. Moreover, work on the above-mentioned procedures (including risk analysis) and public procurement procedures for the IT infrastructure.

5) The university indicated that it is currently at an advanced stage of updating the documents used at WULS-SGGW to the current legal status by: clarifying the procedure for reporting data protection breaches to the supervisory authority (Article 33 (3) of Regulation 2016/679), the procedure for assessing and notifying security breaches personal data (Article 34 of Regulation 2016/679), procedures for keeping an internal register of data protection violations (Article 33 of Regulation 2016/679) and a register of processing activities and the scope of the register of categories of processing activities (Article 30 of Regulation 2016/679), procedures in terms of creating new processing processes and taking into account data protection by default (Article 25 of Regulation 2016/679), risk assessment and impact assessment procedures for the protection of personal data (Articles 24, 32, 35 of Regulation 2016/679), as well as a compliance plan and conducting internal audits, including the principles of monitoring and auditing internal procedures, the manner of their implementation and the procedures for selecting a provider processing personal data along with a register of processing entities. WULS-SGGW also indicated that currently a specialized external entity with which the University has signed a contract, performs an order for the comprehensive preparation of a draft personal data protection policy along with procedures at WULS-SGGW, which is confirmed by the schedule attached to the response to the initiation of the procedure.

6) Referring to the statement that WULS-SGGW has not implemented adequate technical and organizational measures to ensure adequate security of candidates' personal data in the recruitment process at WULS-SGGW, including protection against unauthorized or unlawful processing and accidental loss, destruction or damage, because the candidates' personal data from the last 5 years of recruitment were processed on the private computer of Mr. AG, [...], in particular due to the lack of

protection of this computer against unauthorized access and lack of protection of files with personal data of candidates for studies, the University indicated that the above does not constitute a violation by the administrator of the principle of storage limitation specified in art. 5 sec. 1 lit. e of the Regulation 2016/679. In the opinion of WULS-SGGW, it does not follow from the fact that personal data are processed (without appropriate security) on a private computer that WULS-SGGW has not implemented adequate measures. This fact only shows that the employee processed the data on a private computer located outside the jurisdiction, without the consent of the administrator and contrary to the procedures in force at WULS-SGGW. The university reiterated that Mr. A.G. he did not inform about this fact and he was not authorized to process personal data on a private medium.

The university raised that the statement of the supervisory authority that the storage of candidates' personal data from 5 years ago on a private computer shows that the administrator violated the principle of limiting storage, is not consistent with the facts. In the opinion of the University, WULS-SGGW has analyzed and determined the appropriate period of data storage of candidates for studies (3 months). This means that the controller complies with the principle of Art. 5 sec. 1 lit. e of the Regulation 2016/679. However, in every organization there is a human factor that is unreliable. Hence, the argument presented in the notification seems, in the University's opinion, to be inconsistent and harmful to the administrator. In addition, she emphasized that in order to reduce errors in the operation of the human factor, both before the date of the inspection and now, she constantly trains the University employees in the field of personal data processing, including on-line training for all employees.

7) Referring to the allegation of violation of the principle of accountability in the IT system used to process personal data of candidates for studies, the University indicated that during the inspection it took steps to introduce measures consistent with this principle, which were introduced in the recruitment process of candidates for second-cycle studies commencing from the summer semester 2019/2020. For this purpose, on [...] November 2019, a contract was concluded (and [...] January 2020 updated) with Mr. processing in accordance with the existing conditions (the document is contained in the inspection files and attachments to the response to the initiation of the procedure). As a result of the above, the following technical and organizational changes for the Candidate Service System:

- access to the content of the "[...]" tab is possible only after granting appropriate permissions by the head of the Student Affairs Office, and the data export itself is possible only in the functionally justified scope of data processing specified by the

head of the Student Affairs Office,

- the fact of downloading data from the tab is recorded in system logs and it is possible to download a report on data export containing information: who, when and what report (data export) was downloaded,

- restriction of access to the Candidate Service System for the University and Faculty Admissions Committees only to the area of building No. [...] and No. [...] - technical / system restriction to a separate subnet,

- entering an individual identification number (DOID) as the candidate's ID at SOK,

- enabling the members of the Recruitment Committee to use SOK only with computers prepared to handle recruitment by the IT Center of the Warsaw University of Life Sciences,

- limiting the content of reports used by the Recruitment Committees only to the information necessary to make qualification decisions,

- separation of a special resource in order to provide secure information to be transferred from the Candidate Service System to the Virtual Dean's Office of the Warsaw University of Life Sciences without the need to send it by e-mail.

In addition, the University indicated that in order to limit the transfer of files between the SOK and the "Virtual Dean's Office" system via e-mail, a separate resource was created to which transfer files are transferred. Any correspondence with faculty admission committees - if necessary - containing personal data of persons admitted to studies, is carried out using encrypted files.

8) The university indicated that it does not fully agree with the allegation that the data protection inspectors, in particular Mr. A.G, did not monitor the provisions of the regulation at all and did not provide support to the administrator in fulfilling the obligations arising from Regulation 2016/679. The university emphasized that the inspector's error or omission by the data protection officer cannot be tantamount to improper supervision of the administrator over the observance of data security. She also indicated that, with due diligence, she chose an entity specializing in the protection of personal data in a comprehensive manner and the delegation of duties / tasks to a professional entity is the only aspect within which the administrator can have a real impact on the fulfillment of the obligations under Regulation 2016/679. The university also indicated that over the years 2018-2020 new models of entrustment agreements, dedicated information clauses, data subject consents, a procedure for reporting violations and their notification and recording, a new model authorization to process personal data, etc. have been developed and implemented. the scope of individual documents and regulations that, in the administrator's opinion, needed to

be updated in the first place - be it due to legal or organizational changes. Among other things, the procedure for the circulation of correspondence in the correspondence circulation system (EZD), the anti-mobbing procedure, the Regulations of the Company Social Benefits Fund, the Regulations of the Student Dormitories, and the provisions on video monitoring (update of the information obligation) were made.

The university also argued that it is inappropriate to formulate conclusions only in relation to the person currently holding the function of an inspector (from June 2019, i.e. for a period of less than 5 months before the occurrence of the controlled event). She noted that the previous inspectors - Mr. W.K and Mr. M.K. - take steps to update the Security Policy in force at the University. On […] August 2018, the Data Protection Officer […] submitted a new version of the comprehensive data protection policy, which was processed internally by the controller. From 2018, each of the persons acting as an inspector conducted constant observation and control of the compliance of data processing processes with the provisions on the protection of personal data, as indicated by e-mails sent by data protection inspectors, which are included in the inspection files and attached to the response to the initiation proceedings. The university noted that the data protection inspector [...] conducted extensive educational activities for employees, as indicated by the inspector's meeting calendar (attachment to the response to the initiation of the procedure) and explanations of the Manager [...] submitted during the inspection. Educational activities are also conducted by an employee of the Data Protection and Information Security Inspectorate of Warsaw University of Life Sciences - [...].

The explanations provided by [...] show that during the meetings of the University authorities with heads of institutes and deans of faculties, which took place on [...] September and [...] October 2019, trainings were conducted by [...] and the data protection officer [...] in the field of personal data protection rules, in particular in matters related to the principles of safe personal data processing, incl. the need to password protect documents sent in electronic form containing personal data, apply the principles of a clean desk, be particularly careful when using USB storage devices and in relation to attachments received in e-mail. The Data Protection Officer [...] held meetings with individual units, including the Office of Student Affairs, during his 5-month term in office. During the meetings, an audit of the current functioning of individual units was carried out and the documentation of personal data processing was adjusted to the content of Regulation 2016/679. The above-mentioned activities, in the opinion of the University, certainly prove that the data protection officer fulfills the tasks in the field of control of units where personal data is processed. As confirmation of the above, the University attached appropriate e-mails to the response to the initiation of

the procedure.

Moreover, WULS-SGGW disagrees with the statement that the activities of the data protection officer mainly consisted in educational activities in the field of personal data protection, i.e. conducting trainings, sending recommendations in the form of messages to University employees, and providing ongoing answers to questions related to the protection of personal data. and that the educational activities were mainly aimed at presenting the basic principles of personal data processing resulting from the content of Regulation 2016/679, without taking into account the specificity of the functioning of individual organizational units of the University and the tasks performed by them in these activities. Taking into account all the evidence collected in the case, WULS-SGGW indicated that the trainings conducted by the data protection officer [...] were fully individualized to the nature of the unit, e.g. the training conducted on [...] November 2019, in addition to the training presentation and the classic lecture on the general principles of data protection, also included a discussion panel with the heads of individual organizational units, during which the specification of the work of individual units and the processing operations performed by these units were discussed. During training and meetings in individual units, the individualized specificity of work for specific resources was discussed, including: protection of students 'personal data, protection of employees' personal data, the issue of destroying and archiving diploma theses, clauses and consents during the organization of scientific and student / doctoral conferences, providing answers to the Social Insurance Institution and the Tax Office, the issue of the legal basis for providing documentation, the issue of concluding entrustment agreements based on specific examples, data security in relation to security policy, sending e-mails, reporting violations and what the violation is - examples adapted to the specificity of academic teachers' work. Training sessions and meetings on the protection of personal data took place in the form of discussion panels, during which each of those present had the right to ask specific questions tailored to the processing operations that he performs as part of the entrusted tasks. In addition to stationary training, the University indicated that at the moment, an e-learning training was conducted, in which all university employees had the opportunity to participate, and nearly 1,500 university employees were trained.

9) The University does not agree with the allegation that the administrator did not ensure the fulfillment of obligations under Art. 24 sec. 1 and art. 32 of Regulation 2016/679 by failing to take effective measures to ensure the training of Mr. A.G. WULS-SGGW indicated that he had a real opportunity to participate in each of the available training dates and was obliged to do so, however, he did not participate in them voluntarily. She also emphasized that training and instructional e-mails were

sent to research workers in the field of compulsory training at faculties. The last e-mail before the breach, dated [...] November 2019 (developed by the IT Center in cooperation with a specialist for personal data protection and information security), was sent before the incident on [...] October 2019 by the IT Center to all employees, including Mr. AG At the same time, the University indicated that on the WULS-SGGW Intranet on the website of the IT Center there is an instruction on passwording files containing personal data, and employees, in accordance with the applicable procedures, may not process personal data outside the WULS-SGGW on any medium. In addition, members of the Recruitment Committee, including Mr. A.G., were each time informed about the security rules for the processing of personal data by the chairman of the University Admissions Committee and the Head of the Student Affairs Office, which, in the University's opinion, should also be treated as training.

10) In connection with the allegation of violation by the University of Art. 30 sec. 1 lit. d of Regulation 2016/679, it was explained that the administrator, in connection with the request received from the data protection officer on [...] October 2019, for verification by individual units of the University of the register of data processing activities, within the scope of its competence (sub-registers), in terms of their compliance with the facts, verified the sub-register of the Student Affairs Office in the above-described scope and updated it (the update of the register of processing activities in the scope of the enrollment process is attached to the letter of the Rector of the Warsaw University of Life Sciences of [...] June 2020).

Supplementing the above, the University, in a letter of [...] January 2020, provided, inter alia, e-mail correspondence of the head of the Internal Control Team, Mr.T.S. with a member of the selection committee, Mr. G.M. The committee member indicated that during the training on the use of the SOK system, which took place [...] in July 2019, probably [...], he indicated that the members of the committee downloading student data from the SOK system to determine the so-called the threshold from which candidates for admission to a given field of study will be qualified, they must delete all data except the data necessary for recruitment, i.e. information on: enrollment fee, student status, number of points in the Matura exam and language certificate.

In addition, the University, in response to the initiation of the procedure, indicated that in all currently undertaken activities, it takes overriding account of the nature, scope, context and purposes of processing as well as the risk of violating the rights or freedoms of natural persons. The actions taken, in the opinion of WULS-SGGW, guarantee that the implementation of the above objectives will not be of a one-off nature, as these measures in the scope of the recruitment system (current or future) will be subject to regular reviews and will be updated on the basis of activities undertaken as part of the implementation of the

results of the current cooperation. with a specialized external entity with which the University has signed an appropriate agreement.

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

In the opinion of the President of UODO, the University did not sufficiently assess the effectiveness of technical and organizational measures to ensure the security of personal data processing of candidates for studies, which constitutes a violation of Art. 5 sec. 1 lit. e, art. 5 sec. 1 lit. f, art. 5 sec. 2, art. 24 sec. 1, art. 25 sec. 1, art. 32 sec. 1 lit. b, art. 32 sec. 1 lit. d, art. 32 sec. 2 and art. 38 sec. 1 of Regulation 2016/679, including failure to sufficiently take into account the principle of accountability by using the IT system used to process personal data of candidates for studies, which is a violation of art. 5 sec. 2 of Regulation 2016/679.

Article 5 of Regulation 2016/679 lays down the rules for 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"). According to Art. 5 sec. 1 lit. e of Regulation 2016/679, personal data must be stored in a form that permits identification of the data subject for no longer than is necessary for the purposes for which the data are processed; personal data may be stored for a longer period as long as they are processed exclusively for archiving purposes in the public interest, for scientific or historical research purposes or for statistical purposes pursuant to Art. 89 paragraph. 1, subject to the implementation of the appropriate technical and organizational measures required by this Regulation to protect the rights and freedoms of data subjects ("storage limitation").

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 seriousness, the controller implements appropriate technical and organizational measures to ensure that the processing is carried out in accordance with this Regulation and to be able to demonstrate it . These measures are reviewed and updated as necessary. This means that the controller, when assessing the proportionality of the safeguards, should take into account the factors and

circumstances relating to the processing (e.g. type, method of data processing) and the related risks. 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 the Regulation 2016/679. The implementation of technical and organizational measures should rely on the administrator implementing relevant provisions and rules for the processing of personal data in a given organization, but also regular reviews of these measures, and, if necessary, updating previously adopted safeguards.

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

Pursuant to the wording of Art. 32 (2) of Regulation 2016/679, when assessing whether the level of security is appropriate, 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.

In addition, to ensure effective protection of personal data and compliance with the provisions of Regulation 2016/679, Art. 25 sec. 1 obliges the controller to implement appropriate technical and organizational measures - both when determining the method of processing and during the processing itself, taking into account the same criteria that are contained in art. 32 sec. 1 of Regulation 2016/679, i.e. the state of technical knowledge, the cost of implementation, nature, scope, context and purposes

of processing as well as the risk of violating the rights or freedoms of natural persons with a different probability and severity of the risk resulting from processing.

In the mentioned Art. 24 of Regulation 2016/679, the legislator also established an additional requirement addressed to the controller, who should be able to demonstrate compliance with the data security requirements and compliance with the provisions of Regulation 2016/679. This may be achieved by documenting the risk analysis performed and other measures taken to ensure compliance with the provisions of the regulation. Such a structure refers to the general obligation of accountability referred to in the provision of art. 5 sec. 2 of Regulation 2016/679, laying down general principles for data processing (Fajgielski Paweł, Commentary to Regulation 2016/679 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Directive 96/46 / EC [general Data Protection Regulation], in: General Data Protection Regulation. Personal Data Protection Act. Comment).

The WULS-SGGW currently has a Security Policy and Instructions for the management of the IT system used for data processing, introduced by the order of the Rector of the Warsaw University of Life Sciences No. 88/2013 on the Security Policy and Instructions for the management of the IT system used for data processing. This documentation has not been comprehensively updated so far. The concept of "data protection policy" is included in Art. 24 sec. 2 of Regulation 2016/679 and is understood as a data protection strategy, an action plan aimed at achieving the goal of effective data protection. In this sense, data protection policy means a general document indicating the basic assumptions and goals, as well as a set of detailed procedures and tools related to technical and organizational data security measures, which clarify and develop the adopted general goals and principles. Taking into account the assumptions of the EU reform consisting in the continuation and improvement of the existing solutions and the evidence collected during the inspection, the President of the Personal Data Protection Office took into account that the University has implemented procedures for keeping a register of processing activities (Article 30 (1) of Regulation 2016/679), in what is important from the point of view of the subject of control, the register of processing activities in the field of personal data processing of candidates for first-cycle, second-cycle and long-cycle studies, procedures for keeping an internal register of data protection violations (Article 33 of Regulation 2016/679), procedures for reporting data breaches to the supervisory authority (Article 33 (3) of Regulation 2016/679) and other documents, such as entrustment agreements, model authorizations, consents, etc., which were presented during the inspection. The President of the Personal Data Protection Office, accusing an insufficient assessment of the technical and

organizational measures applied, including the processing of personal data of candidates for studies at SGGW, followed the principle resulting from Art. 24 (1) of Regulation 2016/679 which is the controller's control over the processing of personal data. Improper taking of measures resulting, inter alia, from joke. 32 sec. 1 affect the procedures and documents adopted by the administrator. The initiation of the administrative procedure indicated that it is recommended that the internal documentation, taking into account the organizational structure of the University, comprehensively regulate all areas of personal data protection referred to in Regulation 2016/679. This is to ensure the protection of personal data not only on a formal but also practical level. This means that the procedures must not only be introduced but also applied, otherwise it will not comply with Regulation 2016/679.

The university indicated that the adopted Security Policy and IT System Management Instruction met the assumptions of the data protection strategy, although it was introduced on the basis of the Regulation of the Minister of the Interior and Administration of April 29, 2004 on personal data processing documentation and technical and organizational conditions that should be met by devices and IT systems used to process personal data (Journal of Laws of 2004, No. 100, item 1024). She also pointed out that the implementation of these solutions made it possible to conclude that the entity met the requirements for data protection and still meets them, although the current provisions on the protection of personal data are slightly different, as general requirements are indicated, including the requirement to conduct a risk analysis and selection of security measures. appropriate for this type of risk, and the EU legislator did not provide for the issuing of executive regulations specifying specific types of security, thanks to which WULS-SGGW, as an administrator, gained greater freedom in the selection of securities, associated with greater responsibility for their selection.

While one should agree with the University's statement that the current provisions on the protection of personal data do not impose on the administrators specific types of security that they should apply, in the opinion of the President of the Personal Data Protection Office, one cannot agree with the position that compliance with The provisions of the aforementioned regulation of the Minister of Interior and Administration of 2004 allow to state that the entity met and still meets the requirements for the protection of personal data, and only the responsibility for the selection of appropriate measures is now greater. Taking into account the fact that the personal data processed on the private computer of the University employee used for business purposes covers a period of 5 years, it should be clearly emphasized that the personal data protection model based on the assumption that the measures taken by administrators should be adapted to the risks and nature of processed

data is not new. Such an approach is based on the existing, nearly forty-year-old legislative and jurisprudence achievements developed in Europe. Art. 17 sec. 1, repealed by Regulation 2016/679 of Directive 95/46 / EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, indicates examples of threats that may occur during operations processing of personal data and requires the adoption of such safeguards that will ensure a level of security appropriate to the risks that may occur during data processing and appropriate to the nature of the data protected. In Poland, until the application of Regulation 2016/679, the obligation to carry out a risk assessment and properly select technical and organizational measures appropriate to the threats and categories of data covered by protection resulted from Art. 36 sec. 1 of the Act of August 29, 1997 on the Protection of Personal Data (Journal of Laws of 2016, item 922). As indicated in the case law (judgment of the Provincial Administrative Court in Warsaw, file no. II SA / Wa 2016/78), the above provision did not indicate what specific measures are to be applied by the data controller, and his obligations result from the tasks assigned to him, which are very broadly defined. and in general: the administrator is to ensure the protection of personal data processed. The obligation formulated in this way is then specified in such a way that the most important tasks are indicated, consisting in securing the data against: disclosure to unauthorized persons, removal by an unauthorized person, damage, destruction, alteration, loss, processing in violation of the Act. Moreover, as pointed out by the court in the cited judgment, the literature on the subject indicates that the effectiveness of the measures used should be tested, and when using safeguards, one should also take into account the changing conditions and technical (IT) progress, which may result in the need to change or modernize the introduced measures. previously by the security systems administrator.

The concept of accepting and monitoring the applied technical and organizational measures adequate to the risks, as well as to protect against processing in violation of the provisions on the protection of personal data, is continued by Regulation 2016/679, inter alia, in art. 32 of Regulation 2016/679. Pursuant to this provision, the adoption and monitoring of these measures should be preceded by an analysis taking into account relevant criteria, i.e. the 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 of the threat. Therefore, the implemented measure should be appropriate to the already identified threats and non-compliance. The failure to comply with this rule and the lack of supervision by the administrator of the compliance by an employee of WULS-SGGW with the rules of data processing in force at the University is evidenced by the use by an employee of

WULS-SGGW of a private device to process the data of candidates for studies at WULS-SGGW from the last 5 years, lack of the administrator's knowledge of this fact, the possibility of downloading the data of these persons from the SOK system without registering this process in this IT system and collecting them by an employee outside the processing area, contrary to the adopted procedures. Moreover, it should be noted that Mr A.G. he undertook these activities outside the scope of the authorization, because each time the authorization covered personal data included in the recruitment for studies for a given academic year, both those processed on paper carriers and those processed in the SOK system. WULS-SGGW also points out that the authorization in question did not include saving and storing personal data on a private computer and taking them outside the WULS-SGGW premises. At the same time, according to the material collected in the course of the inspection, the University received a statement from the employee about keeping personal data secret and about getting acquainted with the personal data protection system in force at the University. WULS-SGGW also points out that Mr. A.G. he did not report the need to have a company computer, which, in the opinion of the President of the Personal Data Protection Office, cannot be a mitigating circumstance, and even more so, it may mean removing the administrator from the responsibility for control over the processing of personal data in connection with the official activities performed by the employee. It is the controller who is obliged to verify the areas of personal data processing in the organization and implement appropriate technical and organizational measures to ensure their security.

Thus, from the evidence collected during the inspection and the above explanations submitted in the course of administrative proceedings, it does not appear that the University assessed the risk of violating the principle of confidentiality of personal data (Article 5 (1) (f) of Regulation 2016/679) or rules for limiting data storage (Article 5 (1) (e) of Regulation 2016/679), resulting from the risk of exporting a wide range of personal data categories from the SOK system to an external medium. In the opinion of the President of the Personal Data Protection Office, the controller stopped at the above-mentioned documents signed by the employee and the implementation of organizational measures in the form of the Security Policy, Information System Management Instructions for data processing (paying attention to the content of section 7.5, which prohibits taking personal data in the form of printouts and on portable media outside the processing area without justifiable reason) and the Procedure use of portable computers (including only business computers entrusted to employees by the University), which are insufficient in the context of ensuring adequate security of personal data against unauthorized or unlawful processing and accidental loss, destruction or damage, as they additionally require the administrator (Article 24 (1) of Regulation 2016/679) and the data

protection officer (Article 39 (1) (b) of Regulation 2016/679) to review, supervise the principles set out in these documents and, if necessary, adjust organizational measures technical and technical characteristics to the identified threats and non-conformities.

In connection with the above, it is justified to charge the University of violating Art. 24 sec. 1, art. 25 sec. 1, art. 32 sec. 1 lit. b and lit. d and art. 32 sec. 2 of Regulation 2016/679 by implementing insufficiently technical and organizational measures, which should be regularly reviewed and updated, taking into account the factors and circumstances relating to the processing of personal data indicated in this provision. The implementation of appropriate measures is aimed at the implementation of one of the general principles of data processing - the principle of integrity and confidentiality, as defined in art. 5 sec. 1 lit. f of the Regulation 2016/679, which was consequently also breached by the controller. Moreover, with Art. 24 sec. 1 of Regulation 2016/679 results in the obligation to demonstrate compliance with the requirements for data security and compliance with the provisions of the Regulation, which is reflected in documenting actions taken to ensure compliance with the provisions of the Regulation and refers to the principle of accountability specified in Art. 5 sec. 2 of Regulation 2016/679. In the material collected in the proceedings, there is no evidence that the administrator supervised the compliance by an employee of the Warsaw University of Life Sciences, Mr. A.G. the rules for the processing of personal data specified in the documents in force at the University and the Regulation 2016/679, therefore the allegation of violation of Art. 5 sec. 2 of Regulation 2016/679.

Therefore, in the content of the notification on the initiation of administrative proceedings, the President of UODO emphasized that an important document constituting the data protection policy is the compliance maintenance plan and internal audits, including rules for monitoring and auditing internal procedures. Monitoring the policy in the field of personal data protection is the responsibility of the controller, as well as the data protection officer, who is responsible for supporting the controller in complying with the provisions on the protection of personal data.

Moreover, on the basis of the evidence collected in the course of the inspection, the President of the Personal Data Protection Office states that no internal audit covering individual organizational units of WULS-SGGW was carried out and that the data protection officer, Mr. A.G., did not conduct a risk analysis related to the processing of personal data of candidates for studies at WULS-SGGW. He also did not inform about the necessity to prepare it by the rector of the Warsaw University of Life Sciences or the head of the Student Affairs Office, which according to the organizational structure of the University is responsible for the recruitment process for studies at the Warsaw University of Life Sciences.

In its explanations, the University claims that it does not agree with the above statements because the collected evidence shows that data protection inspectors held regular meetings at organizational units of the Warsaw University of Life Sciences, including at the Student Affairs Office, responsible for processing activities, including the recruitment process for studies at WULS-SGGW, the subject of which was the clarification of important issues related to the processing of personal data, issued appropriate recommendations in this regard, organized training for employees, as well as implemented and versioned documents. In addition, as indicated by the University, the analysis covered documentation related to the processing of personal data, and the current data protection officer, Mr. A.G. during the 5 months he was in office, he held meetings with individual units of the University. WULS-SGGW emphasized that during these meetings, as part of educational activities in the field of personal data protection, an audit of the current functioning of these units was carried out and the documentation of personal data processing was adjusted to the content of Regulation 2016/679.

It should be pointed out that the control of compliance with data protection regulations and procedures contained in policies, including audits related to processing operations, is a multi-stage activity, which includes collecting information, analyzing and checking compliance of processing, informing, advising and recommending specific solutions. Therefore, first of all, it is important to collect information about the entity and the data processing processes used in it, including identification of data processing activities, determination of assets used for data processing, i.e. IT systems, documents, data carriers and determination of the scope of data that are processed along with their categorization. Secondly, it is important to analyze and evaluate processing activities in terms of compliance with the provisions of Regulation 2016/679, both in terms of formal and legal aspects and compliance of IT systems. Third, it is reasonable to develop a report and recommendations. The audit report is the basis for the implementation of the procedures set out in Regulation 2016/679.

Bearing in mind the above, in the opinion of the President of the Personal Data Protection Office (UODO), the actions taken by data protection inspectors, resulting from the material collected during the inspection activities, as well as the University's explanations contained, inter alia, in a letter of [...] April 2020, consisting, inter alia, of organizing trainings, formulating recommendations, holding meetings with employees, or preparing documentation (including entrustment agreements, information clauses or data subjects' consents), only exhaust at most one of the elements (stages) of the audit. Therefore, it cannot be considered that they conducted audits related to processing operations in a comprehensive manner. The above is also evidenced by the lack of evidence of the preparation of reports on the control of compliance with data protection

regulations, in particular in the Student Affairs Office and the University Admissions Committee, which were specified as mandatory in point 3 of Annex 7 to the Security Policy entitled "Scope of obligations with regard to protection personal data ". It should also be noted that the data protection officer himself, Mr. A.G. in his explanations, he confirmed that he had not carried out any audits or risk analysis because, as he pointed out, the contract with […] did not cover the provision of such activities and that, to his knowledge, an audit at WULS-SGGW had not been carried out. This is contrary to the University's explanations contained in the letter of [...] April 2020, indicating that Mr. A.G. audit of the current functioning of WULS-SGGW units as part of educational activities in the field of personal data protection and the contract for the provision of data protection officer services (No. [...] concluded [...] May 2019 with [...] based in [...]). Paragraph 3 point 2 lit. c of this agreement and the content of Art. 39 sec. 1 lit. b of the Regulation 2016/679 oblige the inspector, inter alia, to monitor compliance with the provisions on the protection of personal data and policies adopted by the administrator, including audits related to data processing operations. In addition, Annex 7 entitled "scope of obligations with regard to the protection of personal data" to the Security Policy, in point 3 obliges the information security administrator (currently the data protection officer) to internal control of compliance with data protection regulations and procedures contained in the Security Policy and Management Manual and to present reports on their implementation to the authorities of the Warsaw University of Life Sciences. These activities should include collecting information to identify processing processes, analyzing and checking compliance of processing, advising and recommending specific activities.

At the same time, there is no evidence that data protection inspectors took actions in the field of, inter alia, analyzing, checking the compliance of processing with the provisions of Regulation 2016/679, as well as recommending specific solutions or recommendations for the SOK system. All modifications and new functionalities of the SOK system, as it results from the collected evidence, were introduced as a result of meetings of the administrator of this IT system - Mr. S.L. with Mr. Z.W. - head of the Student Affairs Office. Moreover, as is clear from point 10.1.4 Security policies, the task of the information security administrator (currently the data protection officer) is to analyze whether the policy in question and the IT system management manual and other related documents are adequate to changes in the structure of the IT system, organizational changes at the University, changes in almost and other changes that may affect the security of personal data. Also, the provision in point 3 of the above-mentioned Annex 7 to the Security Policy imposes on the information security administrator (currently the data protection officer) the obligation to cooperate with the IT system administrator in the field of IT security of personal data. Due to

the scale of the breach of personal data protection and the established facts, it is reasonable to conclude that data protection inspectors did not conduct such analyzes and reviews in the context of the processing of personal data of candidates for studies in the SOK system and outside it, in particular as part of recruitment activities carried out by members of the University Admissions Committee, including its secretary. Moreover, as indicated in his explanations, the data protection officer, Mr. A.G., was not involved by the controller in the process of developing a draft personal data protection policy at the Warsaw University of Life Sciences. It should be emphasized here that Art. 38 of Regulation 2016/679 imposes an absolute obligation on the controller to properly and immediately involve the data protection officer in all matters related to the protection of personal data. The data protection officer should be involved in the decision-making process involving the processing of personal data by providing him with the opportunity to express his position in the context of the adopted technical, organizational and legal solutions. Involving the inspector in matters concerning personal data is part of the concept of data protection at the design stage expressed in art. 25 sec. 1 of Regulation 2016/679, which obliges the controller to implement appropriate technical and organizational measures - both when determining the method of processing and during the processing itself. It should be additionally emphasized that Mr. A.G. on the basis of the authorization granted to him to process personal data (each time including a set of data on recruitment for studies in a given academic year), he was authorized to access the IT system in which the data of candidates for studies at SGGW are processed. From the material collected during the inspection, as well as from the explanations provided by the University in the course of the proceedings, it does not appear that WULS-SGGW assessed on what medium, under what conditions and for what period of storage personal data, which can be exported to such a wide extent for thanks to the implemented functionality of the IT system, to which Mr. AG had access and which he used to perform official duties (indicated in the annex to the application for a special allowance in connection with the performance of tasks related to a given recruitment). Such actions were not taken despite the awareness of the Student Affairs Office about the need to remove (from the set of data exported in the form of a spreadsheet) data that was not necessary to determine the so-called the threshold from which candidates for admission to a given field of study will be qualified (which is confirmed by e-mail correspondence of the head of the Internal Control Team, Mr. T.S. with a member of the recruitment committee, Mr. G.M. attached to the University's letter of [...] January 2020).

In connection with the above, the allegation of violation of Art. 24 sec. 1, art. 32 sec. 1 lit. b and lit. d, art. 32 sec. 2, and art. 39 sec. 1 lit. b of the Regulation 2016/679 in connection with art. 5 sec. 2 of Regulation 2016/679. In the context of the above, the

allegation of infringement of Art. 38 sec. 1 of Regulation 2016/679 - due to the lack of inclusion of the data protection officer in matters concerning the protection of personal data in the scope of the adopted technical solutions as part of the SOK system operation and its subsequent modifications, and the allegation of violation of Art. 25 sec. 1 of Regulation 2016/679 by not taking into account data protection during the processing of data in the SOK system and outside it, and by adopting appropriate procedures in this regard.

The university, refuting the allegation of breach of the obligation to perform a risk analysis and check the compliance of processing with the provisions of Regulation 2016/679, indicates that in the letter of [...] December 2019, along with the signed inspection protocol, it provided a document entitled "Risk assessment sheet" regarding the recruitment of candidates for studies, dated [...] May 2019, to be provided by the controller while the audit was still ongoing. In initiating the administrative procedure, the President of the Personal Data Protection Office indicated that the presented risk analysis raises doubts as to the correctness of its preparation (the reliability of the data contained therein), does not contain the methodology for its implementation, does not allow for an unequivocal statement that it was performed on the indicated date and that it does not appear from it, who specifically and on whose order has carried out and prepared the analysis in question and by whom it has been approved. The answers to these doubts did not bring any explanations provided by the University after the initiation of the procedure, including the document entitled "Risk assessment methodology" provided with the letter of [...] June and [...] July 2020. From the material collected during the inspection and from the explanations provided by the University in the course of the procedure, neither the risk analysis dated to [...] in May 2019, as well as the methodology submitted to the proceedings, was presented and known to the head of the Student Affairs Office, who is responsible for the processing of personal data of candidates for studies. The above also applies to the data protection officer, Mr M.K., who, as he explained, did not carry out a risk analysis because, as he pointed out, the contract with […] did not cover the provision of such activities and that, to his knowledge, an audit at WULS-SGGW was not carried out.

In response to the initiation of the procedure, the university indicated that the risk analysis sheet is not an independent document, but correlated mainly with the Security Policy in force at the Warsaw University of Life Sciences. In the opinion of the President of the Personal Data Protection Office, it is difficult to agree with this position, because the presented methodology on the basis of which the discussed document was prepared differs from other documents and procedures presented by the University during the inspection and during the administrative procedure. The analysis of the risk assessment

methodology adopted by the University shows that this document is a diagram that is only the basis for the implementation of a proper risk analysis method in the organization (the document contains empty items, e.g. to indicate the place where individual processing processes are subject to analysis, or to indicate who is responsible for supervision of the validity of this document). In addition, from the above-mentioned the document does not indicate when the methodology in question is in force and is used at the University. Regulation 2016/679 leaves room for the choice of methodology, however, the administrator must be able to demonstrate that it provides a reliable risk assessment and analysis in the organization.

The presented methodology shows that the risk assessment is each time the responsibility of the business owner of the data processing process to be assessed, in the case at hand it is the Student Affairs Office. In addition, if the data protection officer or managers of the IT or legal department submit comments on the worksheet, the business owner of the process must respond in writing. If the risk is accepted by the business owner of the process, these risks are monitored and reviewed, and the current risk assessment questionnaire is kept by the owner of the assessed process. From the material collected during the inspection and from the explanations submitted by the University after the initiation of the procedure, it does not appear that the above provisions were respected and implemented, taking into account also the explanations of the head of the Student Affairs Office indicating that he was not included in the risk analysis process. Moreover, the methodology provided does not indicate who is responsible for the process of monitoring the accepted risks.

The content of the document "Risk assessment sheet" also allows to conclude that the University, despite being aware of the existence of a processing operation in the processing of personal data of candidates for studies, consisting in exporting personal data to an external medium from the IT system, ignored this operation. For the threat "3.2.22 disclosure of personal data to employees and associates of the administrator or processor without an instruction to process the data", it was indicated that there was no such threat. This is in contradiction with the University's explanations that Mr. A.G. He did not have the authorization to process personal data on a private medium and outside the premises of the Warsaw University of Life Sciences and the findings of the inspection, i.e. the technical possibility of such processing due to the functionality enabling uncontrolled export of a wide range of personal data from the SOK system and awareness in this regard of the Student Affairs Office. In addition, for example, for threats "3.3.10 Data stored in an unencrypted form (or no key management policy)", "3.3.16 Inability to ensure traceability / no logs (no registers / logs of operations taking place in IT systems supporting data processing)", " 3.3.19 Redundant data processing (in particular, lack of measures to reduce redundant data - filtering, deletion,

conversion to less sensitive data, limiting the identifying aspect of the data) ”indicated the same level of risk both before and after the proposed measures. This indicates that the administrator accepted the identified risks, which, in turn, based on the material collected during the inspection and the University's explanations submitted in the course of the administrative procedure, were not monitored by the administrator, which cannot constitute the basis for finding that the controller has performed a risk analysis in accordance with the provisions of Regulation 2016/679.

In addition, the University emphasized that in the context of risk assessment, the actions taken by previous inspectors, i.e. Mr. W.K. and Mr. M.K., who took steps to perform an analysis of risks related to personal data processing operations, indicated the need for their implementation or presented their methodology. To confirm the risk analysis, the University submitted a document entitled "Dates for consultation / training in specific areas" by one of the previous DPO […], which indicates that […] a student recruitment meeting was held […] in which the audit sheets were provided. In addition, an e-mail of the data protection officer of [...] August 2018 was also sent, which, in addition to the draft personal data protection policy, contained proposals for risk analysis procedures, including data protection impact assessments and data protection by design assessment (privacy by design assessment). From the material collected during the inspection, as well as from the explanations submitted during the administrative procedure, it does not appear that the administrator implemented these proposals.

In response to the initiation of the procedure, WULS-SGGW indicates that, in line with the accountability principle, Regulation 2016/679 requires the risk assessment process to be carried out and documented - in order to demonstrate that the risk has been assessed and appropriate protection measures have been implemented. At the same time, he points out that the risk assessment in practice, in most cases, is performed in an electronic version, not requiring a signature or even a date, and the Regulation 2016/679 itself does not indicate a specific method of conducting and documenting the risk management process, but it is important that the methodology used is it gave a reliable and objective risk assessment. Moreover, she pointed out that although some inaccuracies in the analysis may be accused, and the risk assessment itself is evaluable, she did it.

While one should agree with the statement that Regulation 2016/679 does not specify how to conduct a risk assessment and document the risk management process, as the University itself indicates, the administrator is required to demonstrate that the risk has been assessed in a reliable and objective manner, and appropriate protection measures have been put in place. This may be achieved by documenting the risk analysis performed and other measures taken to ensure compliance with the

provisions of the regulation. When documenting the actions taken, it should be expected that the administrator will undertake them in an organized manner by implementing appropriate organizational and technical measures, as indicated in Art. 24 sec. 1 and art. 32 sec. 1 of Regulation 2016/679.

The above explanations of the University indicate that individual data protection inspectors undertook actions independently of each other that were not analyzed and continued by their successors (subject to further proceedings). Undoubtedly, this has an impact on the quality of verifying the compliance of processing with the provisions of Regulation 2016/679 and the control over data processing processes in the organization. Despite the fact that the University itself indicates in its explanations that the risk is to be assessed reliably and objectively, and the analysis is to show that appropriate protection measures have been introduced, in the opinion of the President of UODO, the University did not comply with these criteria. The above is evidenced by the existence in the IT system used to process personal data of candidates for studies, a functionality enabling the export of personal data to an external medium, which the University was aware of, the lack of evidence of verification of this processing operation, as well as the fact that the employee is processing personal data. Universities from the last 5 years of recruitment for studies at SGGW on a private computer without the administrator's knowledge.

With the above in mind, it should be emphasized that the risk assessment, as indicated by the presented methodology, should be a continuous process and should be carried out cyclically, taking into account the changing circumstances and the existing and possible future vulnerabilities and threats to the rights and freedoms of natural persons. , which is the implementation of obligations under Art. 24 sec. 1 and art. 32 sec. 1 of Regulation 2016/679. At the same time, the administrator should document and be able to demonstrate activities undertaken as part of this process, in accordance with the principle expressed in art. 5 sec. 2 of Regulation 2016/679. In view of the above, the circumstance raised by the University that there is no need to put a date or signature on a document constituting a risk analysis exposes the administrator to the accusation of failure to demonstrate risk assessment cyclically or on specified dates, permanently or periodically, which in consequence constitutes a breach of the obligations under Art. 24 sec. 1 and art. 32 sec. 1 in connection with Art. 5 sec. 2 of the Regulation 2016/679 laying down the principle of accountability.

The collected evidence allows for the conclusion that the University has not taken steps to ensure the monitoring of the level of threats and accountability in this respect, as well as the adequacy of the introduced safeguards. Therefore, the allegation that WULS-SGGW infringed Art. 24 sec. 1, 32 sec. 1 lit. d and art. 32 sec. 2 of the Regulation 2016/679 in connection with Art. 5

sec. 2 of Regulation 2016/679.

In response to the initiation of administrative proceedings, the University indicated that it had taken increased steps to update organizational measures aimed at increasing the security of personal data processed, including: starting from [...] December 2019, cooperation with an external entity specializing in in the protection of personal data, which currently performs a number of activities supporting the University in the field of personal data protection and information security. In addition, work on the above-mentioned procedures (including risk analysis). In a letter of [...] June 2020, it submitted a risk analysis for the processing of personal data in the recruitment process along with the methodology for this risk analysis. In the presented risk analysis, the administrator indicated, inter alia, at the risk of data loss in the form of generating a file (report) containing a full list of candidates along with the full scope of data. For the indicated risk, measures to reduce the level of the primary risk have been proposed, including in the form of limiting to the necessary minimum the right to generate a full list of candidates containing all personal data and only on devices located at the University in building No. [...].

In response to the notice of initiation of the procedure, contained in the letter of [...] April 2020, the University raised that the processing of personal data (without appropriate security) on the private computer of Mr. AG, [...] does not indicate that SGGW does not implemented adequate technical and organizational measures to ensure adequate security of candidates' personal data in the recruitment process at SGGW, including protection against unauthorized or unlawful processing and accidental loss, destruction or damage. In the opinion of the University, this fact only shows that the employee processed data on a private computer outside the jurisdiction, without the consent of the administrator and contrary to the procedures in force at WULS-SGGW. In doing so, she pointed out again that the supervisory authority had ignored the fact that Mr. A.G. he was not authorized to process personal data on a private medium, thus his operation was inconsistent with the regulations in force at the University.

In response to the initiation of the procedure, also in the context of the allegation of violation of the principle of restriction of storage, the University emphasized that WULS-SGGW had analyzed and specified the appropriate period of data storage of applicants for studies (3 months) and that there is an unreliable human factor in each organization. Hence, in the opinion of the University, the argumentation presented in the notification seems to be inconsistent and harmful to the administrator.

In the opinion of the President of the Personal Data Protection Office, the human factor is one of the sources of risk which in the process of personal data processing, in accordance with Art. 24 sec. 1 and art. 32 sec. 1 of Regulation 2016/679, is a basic

element reflecting the inherent essence of the personal data protection system, which is the controller's control over the processing of personal data. The risk of violating the principle of limiting data storage (Article 5 (1) (e) of Regulation 2016/679) in the course of performing official duties or violating the principle of data confidentiality (Article 5 (1) (f) of Regulation 2016/679) as a result of failure by employees to comply with The university's procedures implemented in the organization cannot constitute mitigating circumstances, and even more so, remove the responsibility from the administrator for the consequences of their materialization. On the contrary, the controller is obliged to apply such technical and organizational measures that will be adequate to the threats and comply with the provisions of Regulation 2016/679. When assessing the effectiveness of these measures, the university should, inter alia, examine the circulation of personal data in the organization. When processing personal data in the IT system that allows their uncontrolled export, it should determine whether it is not at risk of, inter alia, for the violation of the two above-mentioned basic principles of personal data protection. Moreover, as it results from the material collected during the inspection, and what the University itself repeatedly emphasizes in its explanations, employees, in accordance with the applicable procedures, cannot process personal data outside WULS-SGGW on any medium (the IT system management manual in point 7.5 prohibits taking personal data in the form of printouts and on portable media outside the processing area without just cause). Also in Annex 1 to the Security Policy, which is a list of areas in which personal data are processed, the processing area for the collection "Candidates for studies" includes only the seat of the University, i.e. ul. Nowoursynowska 166, 02-787 Warsaw. Contrary to another set (ie "Students"), this item is not provided with information indicating that the data can be processed from anywhere due to the access to the IT system via a web browser. This is in contradiction with the implemented technical measure, which is the possibility of exporting a wide range of personal data from SOK to a medium, including private, for each study program, without supervision over this process. The fact of the possibility of accessing the IT system from anywhere was stated in the risk analysis dated [...] May 2019, which the University presented, however, until the end of the inspection, the stated recommendation to limit access had not been implemented. In the opinion of the President of the Personal Data Protection Office, such a functioning data processing process proves the lack of control of the administrator over this process and insufficient assessment of the effectiveness of technical and organizational measures to ensure the security of personal data processing of candidates for studies.

The above and, as the University emphasized in its letter of [...] April 2020, the fact that these activities were performed by Mr. A.G. undertaken outside the scope of authorization to process personal data, testify to the lack of implementation by the

administrator of mechanisms for monitoring, verification and control over the manner and scope of processing of personal data of candidates for studies at WULS-SGGW by the secretary of the University Admissions Committee and constitutes a violation of Art. 32 sec. 1 lit. b in connection with Art. 5 sec. 1 lit. f of Regulation 2016/679, i.e. the administrator's failure to implement appropriate technical and organizational measures to ensure an appropriate level of security of personal data processing of candidates for studies at WULS-SGGW in terms of the ability to continuously ensure the confidentiality of processing. Personal data should be processed in a manner ensuring their security and confidentiality, including protection against unauthorized access to data and equipment used for their processing and against unauthorized use of this data and this equipment.

In addition, the storage by an employee of the University, Mr. AG, of personal data of candidates for studies at WULS-SGGW, from the last 5 years of recruitment, as a result of performed official activities, is inconsistent with the prescribed period for storing personal data of candidates for studies, which was specified at WULS-SGGW for 3 months. from the end of recruitment. The above constitutes a breach by the administrator of art. 25 sec. 1 of Regulation 2016/679 in connection with Art. 5 sec. 1 lit. e of the Regulation 2016/679, i.e. by failing to take into account appropriate technical and organizational measures in order to effectively implement the principle of limiting storage, also known as the principle of temporary limitation of data processing. Pursuant to this principle, personal data should be kept in a form which permits the identification of the data subject for no longer than is necessary for the purposes for which the data are processed. This means that after achieving the purposes of processing, in this case, after the recruitment process is completed or the deadline for appealing against the decision on admission to studies, the data should be deleted or made anonymous.

It should also be pointed out that it does not follow from the above, taking into account the processing of personal data from the last 5 years of recruitment and collected in the course of material control, that WULS-SGGW regularly test, measure and evaluate the effectiveness of technical and organizational measures to ensure the security of processing personal data of candidates for studies in the SOK system, which constitutes a violation of Art. 32 sec. 1 lit. d in connection with Art. 5 sec. 2 of Regulation 2016/679, i.e. the accountability principle.

The President of the Personal Data Protection Office accused the University of not taking sufficient account of the accountability principle specified in Art. 5 sec. 2 of Regulation 2016/679 also in connection with the use of the functionality of the system for processing personal data - Candidate Service System.

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 specified 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 the events should be recorded in order to maintain the compliance of data processing in the organization with data protection regulations. personal. 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 and with regard to which data were 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 administrator 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 evidence collected in the course of the inspection shows that the SOK system enables the collection of candidate data (e.g. in a spreadsheet format) according to the criteria adopted in the system (the scope of data categories for both views, according to selected criteria, is indicated in Annex 59 to inspection report). The Candidate Service System as part of one of the modules did not have an implemented function of recording events related to downloading the database of candidates within the selected field of study. Due to the scope of the categories of data obtained through this functionality and their scale, it is a breach that prevents the accountability of a person having access to personal data, especially in connection with the duties performed by members of the University Recruitment Committee, including its secretary.

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 requires 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 violating the rights and freedoms of natural persons with varying probability and severity. Considering the above, the allegation of a violation of this article is well founded. The failure of the University to sufficiently take into account this principle

in the process of using the IT system used to process personal data of candidates for studies has become one of the factors that led to a breach of personal data protection.

In response to the initiation of administrative proceedings, the University indicated that after finding the above-mentioned shortcomings, on the basis of a new contract concluded with the IT system administrator, Mr. S.L., a number of changes were implemented in the Candidate Service System, including access to the content of the tab [...] is possible only after being granted the appropriate rights by the head of the Student Affairs Office, and the data export itself is possible only in the functionally justified scope of data processing specified by the head of the Student Affairs Office, the fact of downloading data from the tab is recorded in system logs and it is possible to download a data export report containing information: who, when and what report (data export) downloaded. In addition, access to the Candidate Service System for the University and Faculty Admissions Committees was limited only to the area of building No. [...] and No. [...] - technical / system restriction to a separate subnet, an individual identification number (DOID) was introduced as a candidate identifier at SOK, Recruitment Committees use of the SOK system only with computers prepared for recruitment by the IT Center of the Warsaw University of Life Sciences, the content of reports used by Recruitment Committees only to the information necessary to make qualification decisions (none of the above reports contains the PESEL number, ID document numbers - passport / Pole's card, address, date of birth, index number, etc.).

The WULS-SGGW has a Procedure for the Use of Portable Computers, which constitutes an appendix to the IT System Management Instruction, however, as explained by Mr. R.B. (the protocol of oral explanations is attached as Annex 20 to the control protocol) and the analysis of its content, it includes computers that have been entrusted to users by the University. Therefore, the above procedure cannot constitute a reference point for assessing the activities of the secretary of the University Admissions Committee in this case, because the computer used by him and used to process the personal data of candidates for studies at WULS-SGGW was a private computer.

On the basis of the above-mentioned justification of the allegation, insufficient assessment of the effectiveness of technical and organizational measures to ensure the security of personal data processing of candidates for studies at SGGW, the President of the Personal Data Protection Office states that at the time of the breach of personal data protection and the inspection carried out in the period from [...] November to [...] November 2019, the obligations under Regulation 2016/679 were not properly implemented. The university only after the occurrence of a breach of personal data protection, during and after the

inspection, has shown that it has taken a number of actions that ensure compliance with Regulation 2016/679 and guarantees that the implementation of these obligations will not be of a one-off nature and measures in the scope of the recruitment process will be subject to regularly reviewed and updated based on the actions taken as part of proper risk analysis. While this circumstance is of an attenuating nature for the final decision, in the opinion of the President of the Personal Data Protection Office, it does not affect the final allegation of infringement of the provisions of Regulation 2016/679 indicated in the conclusion of the decision.

The evidence gathered in the case gives the basis, in the opinion of the President of the Personal Data Protection Office, to conclude that the data protection officer performed his tasks without due consideration of the risk related to processing operations, which constitutes a breach by the administrator of Art. 24 sec. 1, art. 32 sec. 1, art. 32 sec. 2, art. 38 sec. 1, art. 39 sec. 1 lit. b and art. 39 sec. 2 of Regulation 2016/679.

Pursuant to the wording of Art. 37 sec. 1 lit. and Regulation 2016/679, the administrator appoints a data protection officer, whenever the processing is carried out, inter alia, by public entity. In turn, art. 37 sec. 6 of Regulation 2016/679, the data protection officer may be a member of the administrator's staff or perform tasks under a service contract. During the inspection, it was found that the data protection officer at WULS-SGGW was appointed and performs his tasks in connection with contract No. [...] concluded [...] on May 2019 between the Warsaw University of Life Sciences and [...] with its seat in [...] on providing services related to the implementation of tasks assigned to the Data Protection Inspector. From [...] June 2019, Mr. M.K. acts as the Data Protection Officer at the Warsaw University of Life Sciences.

Pursuant to art. 39 sec. 1 lit. b of Regulation 2016/679, the data protection officer should monitor compliance with the provisions on the protection of personal data and data protection policies adopted by the administrator, including audits related to personal data processing operations. The obligation in this regard was also imposed in point 10.1.4. Security policy of the Warsaw University of Life Sciences, in particular with regard to organizational changes at the University.

In response to the initiation of the procedure, the university indicates that it does not agree with the allegation that data protection inspectors, in particular Mr. M.K, did not monitor the provisions of the regulation at all and did not support the administrator in fulfilling the obligations arising from Regulation 2016/679. It also argued that the security inspector concerned, Mr M.K. he conducted extensive educational activities for employees, which results from the calendar of his meetings attached to the explanations. In the opinion of the University, this proves that the inspector is fulfilling his tasks. Taking into account the

material collected in the course of the inspection, the President of the Personal Data Protection Office indicates that in the content of the notification on the initiation of administrative proceedings, he did not make any allegations that no actions were taken to fulfill his tasks by the data protection officer. The President of the Personal Data Protection Office took into account that data protection inspectors took steps to ensure the proper performance of their tasks and monitor compliance with the provisions on the protection of personal data, however, these activities were undertaken in an insufficient and ineffective manner by performing tasks without due consideration of the risks associated with processing operations, which is inherently important in the process of controlling the processing of personal data.

The above is evidenced by the fact that an employee of the Warsaw University of Life Sciences, Mr. A.G. had the option of downloading from the SOK system and storing personal data of candidates for studies at WULS-SGGW from the last 5 years of recruitment without the administrator's knowledge from the SOK system and storing them on this medium, outside the designated processing area, against accepted procedures. Pursuant to Art. 38 sec. 1 of Regulation 2016/679, the controller ensures that the data protection officer is properly and immediately involved in all matters related to the protection of personal data. As already indicated by the President of the Personal Data Protection Office, the personal data protection inspector was not involved in the recruitment process for studies covering the functioning of the IT system intended for this process. The inclusion of the inspector in the processing process in question could reduce the risks associated with the processing operations involving the enrollment process.

According to Art. 39 sec. 2 of Regulation 2016/679, the data protection officer performs his tasks with due regard to the risks associated with processing operations, taking into account the nature, scope, context and purposes of the processing. This provision requires the inspector to set priorities in his work, which should consist in individual and independent determination of means and methods of operation and adapting them to the specificity of a particular administrator. In this context, it is important to identify the risks associated with the processing of personal data in advance and on this basis to determine effective solutions, both technical and organizational. This selective and pragmatic approach, i.e. focusing on the aspects with higher personal data protection risk, should make it easier for the DPO to advise the controller which methodology to use when carrying out a DPIA, which areas should be subject to internal or external data protection. audit, what internal trainings to plan and conduct for employees or managers responsible for data processing, and for which processing operations to allocate more time and resources. Taking into account the risk related to the processing of personal data is also, inter alia, one of the criteria

to be taken into account when assessing whether the degree of safety is adequate, as referred to in Art. 32 sec. 2 of Regulation 2016/679, in particular the risk resulting from accidental or unlawful destruction, loss, modification, unauthorized disclosure or unauthorized access to personal data transmitted, stored or otherwise processed.

Moreover, the material collected during the inspection and the period from which the data of applicants for studies at WULS-SGGW came from the infringement, allow us to conclude that the functionality enabling the collection of personal data without recording this fact in the IT system has existed in the SOK system for at least 5 years. Therefore, it can be concluded that both the administrator and the data protection inspectors did not properly monitor the process of processing the data of candidates for studies during this period, so they had no knowledge of the fact that the personal data of candidates were stored on the employee's private computer from an IT system that did not register the fact. downloading sets of personal data, and as a consequence, they did not properly monitor the threats to the personal data of candidates for studies, despite the fact that, as indicated by the University in response to the initiation of the procedure, during cyclical visits of data protection inspectors in organizational units, patterns of conduct were analyzed and recommendations were issued.

When assessing the correctness of the allegation, the President of the Personal Data Protection Office took into account that a public university such as SGGW, as part of its statutory provisions (Act of July 20, 2018, Law on Higher Education and Science - Journal of Laws 2018.1669) and its statutory activities processes m .in. personal data of candidates for studies. The university, as a data administrator, due to the specificity of operation, scale and scope of the categories of personal data obtained, should pay special attention to processing activities related to the recruitment process. In these activities, the University should be actively supported by the data protection officer. As part of each recruitment, averaging the numbers in Annex 29 to the control protocol, the University has about 16,000 entries in the IT system regarding candidates in the Candidate Service System (while during registration for studies, the candidate fills in up to 91 fields with data categories - a printout of the study presenting the list of information fields available in the Candidate Service System is attached as Annex 67 to the inspection report). It should also be noted that the period during which the data protection officer, Mr M.K. performed his function, including the period of recruitment for studies, which, in the opinion of the President of the Personal Data Protection Office, should be even more an area of his particular interest, manifested in taking specific actions.

From the material collected during the inspection, as well as from the explanations provided by the University during the proceedings, it does not appear that both the risk analysis dated [...] May 2019 and the methodology submitted to the

proceedings files were known to the data protection officer, Mr. MK which, as he explained, did not carry out a risk analysis because, as he pointed out, the contract with […] did not cover the provision of such activities and that, to his knowledge, an audit at WULS-SGGW was not carried out. Consequently, it is appropriate to conclude that the work and activities undertaken by previous inspectors were not continued by the data protection officer, M.K.

In connection with the above, it is justified to charge the University of violating Art. 39 sec. 1 lit. b and art. 39 sec. 2 of Regulation 2016/679.

The evidence collected in the case shows that one of the persons involved in the processing of personal data at the University during the recruitment of candidates for studies is Mr. A.G. (copies of the scope of activities of the secretary of the University Recruitment Committee, Mr. A.G. related to recruitment for the academic year 2017/2018, 2018/2019 and 2019/2020, constitute Appendix 18 to the inspection report). Based on the protocol for the acceptance of an oral explanation by Ms A.P. (Appendix No. 12 to the inspection protocol), an example of the attendance list from the training in the field of personal data protection conducted for employees of the Department [...] on [...] March 2019 (Appendix No. 90 to the inspection protocol), explanations contained in the letter from [...] January 2020, lists of employees of the Department [...] participating in the training scheduled for [...] March 2019 and [...] March 2019, the President of UODO determined that Mr. AG he did not participate in the training at any of the set dates, as he was on a sabbatical leave from [...] March 2019. He also did not participate in the training after returning from the above-mentioned leave. In the context of the above, the President of the Personal Data Protection Office indicated that the undertaken educational activities should be monitored and verified in terms of their effectiveness. The administrator should be able to demonstrate monitoring of the training process, including confirmation of training completion. In the absence of Mr. A.G. during trainings dedicated to the employees of the Faculty [...], the administrator should take effective measures to ensure that this person is trained in the planned scope by selecting the appropriate form of education. Bearing in mind the above and the content of art. 24 sec. 1 and art. 32 sec. 1 and 2 of Regulation 2016/679, obliging the administrator to implement appropriate organizational and technical measures, the President of the Personal Data Protection Office stated in the notification on the initiation of administrative proceedings that the administrator did not fulfill this obligation properly by not adjusting the form of training to the specificity of the work of research workers and ensuring sufficient accountability in the field of training conducted for employees, which undoubtedly has an impact on the security and personal data protection system in the organization.

In a letter of [...] January 2020 and a reply to the notice of initiation of the procedure, contained in the letter of [...] April 2020, the University explained that in the field of training conducted at faculties where attendance is mandatory, research workers were training and instructional e-mails sent, including immediately before the breach, an e-mail was sent [...] October 2019, one of the addressees of which was also Mr. AG Moreover, on the WULS-SGGW Intranet, on the website of the IT Center, there is an instruction on password for files containing personal data. As the University indicates, employees, in accordance with the applicable procedures, cannot process personal data outside of WULS-SGGW on any medium. In addition, members of the Recruitment Committee, including Mr. A.G., were each time informed about the security rules for the processing of personal data by the Chairperson of the Committee and the Head of the Student Affairs Office, which should also be treated as training in the University's opinion. WULS-SGGW emphasized that Mr. A.G. had the opportunity to participate in each of the available training dates, but did not voluntarily participate in them. In addition, it indicated that in order to reduce errors in the operation of the human factor, both before the date of the inspection and now, the administrator conducts ongoing training of the University employees in the field of personal data processing, including online training for all employees.

In the context of the above, it should be noted that building data security awareness in the organization and focusing employees' attention on related issues reduces the risk of personal data processing. Therefore, it is in the interest of the controller to properly train persons authorized to process personal data, in particular personal data, the processing of which, due to the scale, scope and context, is burdened with greater risk. It should be emphasized that the administrator, as an employer, has legal instruments based on the applicable regulations that enable the employee to be mobilized to participate in training, especially as it is related to his / her professional duties. The above also applies to Mr. A.G., who is an employee of the Warsaw University of Life Sciences.

Moreover, pursuant to Art. 39 sec. 1 of Regulation 2016/679, monitoring compliance with the provisions, including activities aimed at increasing awareness in the field of personal data protection and training of employees participating in data processing operations, are the tasks of the data protection officer, who implements them taking into account the risk to the rights and freedoms of persons physical. It does not appear from the material collected in the course of inspection activities that the administrator had a confirmation of training completion by Mr. A.G. against infringement, which confirms that educational activities were not monitored and verified by the administrator and the data protection officer, and were not adapted to the specificity of the work of research workers related to, inter alia, with the use of study leaves.

Therefore, the allegation that the controller has not duly fulfilled the obligations under Art. 24 sec. 1 and art. 32 sec. 1 and 2 of Regulation 2016/679 by failing to implement appropriate organizational and technical measures in this regard and not ensuring sufficient accountability in the scope of training conducted for employees. Moreover, the allegation of violation of Art. 39 sec. 1 lit. b of the Regulation 2016/679 by not taking into account the fact that Mr. A.G. in planned trainings and art. 39 sec. 2 of Regulation 2016/679 by not treating this circumstance as a factor indicating the need to verify whether, as a result, Mr. A.G. correctly and in accordance with the procedures adopted at the University, he processes personal data as part of his official duties, taking into account his special function - [...] and the scope of duties entrusted to him in this connection.

It should also be noted that the University, as the administrator of personal data, is fully responsible for the implementation of the principles and processes resulting from the provisions on the protection of personal data, including supervision over them, even in a situation where a personal data protection officer has been appointed. At the same time, it should be emphasized that Regulation 2016/679 and the currently applicable Act of 10 May 2018 on the protection of personal data do not constitute a special responsibility of the data protection officer. The inspector, in connection with the performance of his tasks, is responsible directly to the entity that appointed him, and therefore to the data controller or processor. In the present case, due to the performance of duties by an inspector under a contract for the provision of services, his liability towards the data controller - WULS-SGGW will be subject to general regulations contained in the Civil Code. It is the controller who is responsible for the activities of the data protection officer, as he is responsible for designating him on the basis of professional qualifications, in particular expertise in data protection law and practices, and the ability to fulfill the tasks referred to in Art. 39 of the Regulation 2016/679. According to Art. 83 sec. 4 lit. and Regulation 2016/679, an administrative fine may be imposed on the controller for violation of the provisions of the Regulation regarding obligations related to the activities of the data protection officer. Considering the above, it should be considered an incorrect position of the University contained in the letter of [...] April 2020 that the inspector's error cannot be tantamount to improper supervision of the administrator over the observance of data security and assigning full responsibility to the administrator.

The evidence collected in the course of these proceedings was the basis for stating that the personal data processing activities conducted at WULS-SGGW, in the scope of personal data processing of candidates for first-cycle, second-cycle and long-cycle studies at WULS-SGGW did not include all the information required by the provisions of Regulation 2016/679. , which is in breach of Art. 30 sec. 1 lit. d of Regulation 2016/679.

In the course of the inspection it was found that the WULS-SGGW maintains a register of processing activities. Individual organizational units of WULS-SGGW keep registers of processing activities within the scope of their competence. The head of the Student Affairs Office of the Warsaw University of Life Sciences - Mr. Z.W., keeps a register of personal data processing activities of candidates for first-cycle, second-cycle and long-cycle studies.

Art. 30 sec. 1 of Regulation 2016/679 specifies the scope of information that should be included in the register of processing activities kept by the data controller. One of the types of information that should be entered in the register are the categories of recipients to whom the personal data have been or will be disclosed, including recipients in third countries or in international organizations. The concept of the recipient has been defined in Art. 4 point 9 of Regulation 2016/679 and means a natural or legal person, public authority, entity or other entity to which personal data is disclosed, regardless of whether it is a third party. In other words, it is any entity to which the administrator discloses personal data, with the exception of public entities that obtain data as part of proceedings conducted on the basis of legal provisions. In this context, the data recipient within the meaning of the commented provision should also be considered an entity that processes data at the request of the administrator to whom the administrator discloses personal data.

The evidence collected in the course of the inspection shows that WULS-SGGW concluded civil law contracts regarding IT support for the Candidate Service System and contracts for entrusting data processing with Mr. S.L. (contractor), on the basis of which WULS-SGGW discloses to the contractor (by providing access to the system in which personal data of candidates for studies are processed) personal data of candidates for studies at WULS-SGGW processed in the Candidate Service System in order to perform the obligations arising from these contracts. Therefore, information about the recipient, who is the contractor, should be disclosed in the register of processing activities. In addition, the risk assessment sheet for recruiting candidates for studies attached to the letter of [...] December 2019, carried out on [...] May 2019, section 1.1.8, shows that the data processor is the system administrator - Mr. SL, with whom as indicated above, WULS-SGGW concluded contracts for IT support for SOK. The university [...] in May 2019 concluded an agreement No. [...] with [...] based in [...] on the provision of services related to the implementation of tasks assigned to the Data Protection Officer. On its basis, WULS-SGGW entrusts "in the scope of viewing all personal data sets (...) to which the Contractor will gain access during the performance of the subject of the Agreement". Therefore, information about the recipient, who is the contractor, should be disclosed in the register of processing activities. In addition, on [...] May 2019, by e-mail and on the University's Intranet, the procedure for reporting personal data

breaches was provided, under which other representatives of the company were indicated [...] and their contact details, to whom information about incidents should be provided if there is no possibility making contact with the data protection officer. Therefore, on the basis of the collected evidence, it was found that the register of processing activities in the scope of the processing of personal data of candidates for first-cycle, second-cycle and long-cycle studies in column 10 does not contain information on the categories of recipients to whom the administrator disclosed personal data, which constitutes an infringement of art. 30 sec. 1 lit. d of Regulation 2016/679.

In response to the notification of initiation of the procedure, contained in the letter of [...] April 2020, it was explained that the University verified the register for compliance with the facts, so that it met the requirements of Art. 30 sec. 1 lit. d of Regulation 2016/679. The updated register of processing activities related to the processing of candidates' personal data was attached to the letter of [...] June 2020, confirming the above explanations. It follows from the above that WULS-SGGW introduced the already required solutions correcting the existing provisions of the contract with Mr. S.L. and […] established in […]. Consequently, the breach in this respect has been removed. During the inspection and administrative procedure, it was not found that failure to take into account all the information required by the provisions of Regulation 2016/679 had an impact on the occurrence of a breach of personal data protection. As a result, the President of the Personal Data Protection Office (UODO) discontinued the administrative proceedings in this respect, and thus the breach found does not constitute the basis for the administration of a fine.

The university, supplementing its explanations, in response to the initiation of the administrative procedure, i.e. in the letter of [...] April 2020 and in the letter of [...] June 2020, indicated to the supervisory authority that when issuing the decision ending the procedure, one should take into account the specific and special situation faced by the University after the application of Regulation 2016/679 in May 2018, as it coincided with the reform of higher education introduced by the Act of July 20, 2018 Law on Higher Education and Science (Journal of Laws . of 2020, item 85), which forced very large organizational changes at WULS-SGGW both in 2018 and 2019. Moreover, the University emphasized that the implementation of technological solutions at the University is a continuous, complicated and long-lasting process due to the size of the organization and requires prior development of a strategy and compliance with generally applicable laws, incl. public procurement law, which is related to the fact that the activity of the University as a public entity is financed from public funds. With the above in mind, the President of the Personal Data Protection Office indicates that any legal and organizational changes affecting the processing of personal

data are circumstances to which the administrator should pay special attention in the process of building a data protection system, and any significant changes in this respect should be preceded by an appropriate analysis, because the context of processing is one of the factors that the controller is obliged to take into account in this process, in particular from the point of view of art. 24 sec. 1, 25 sec. 1, 32 sec. 1 or 39 sec. 2 of Regulation 2016/679. The context of the processing is a factor that the controller must address in the process of determining the likelihood and severity of the risk of violating the rights or freedoms of natural persons (recital 78 of Regulation 2016/679). The basic factor indicated in the aforementioned regulations, that is, the risk of violating rights or freedoms. Moreover, Art. 99 of Regulation 2016/679 delimits the dates of entry into force of this legal act and its application. The entry into force of this legal act took place on May 24, 2016, and it became applicable on May 25, 2018. In recital 171 of Regulation 2016/679, the EU legislator indicates that the processing, which is already underway on the date of application of this regulation, should within two years from entry into force of this Regulation be brought into line with its provisions. The two-year adjustment period was a signal, also for the University, that during this period it should re-analyze technical and organizational measures. It should also be emphasized that the entity is responsible for creating structures and resources enabling the fulfillment of obligations under Regulation 2016/679, adequate to the nature and complexity of its activities, regardless of the source of its financing.

Bearing in mind the above findings, the President of the Office for Personal Data Protection, exercising his powers specified in art. 58 sec. 2 lit. and Regulation 2016/679, according to which each supervisory authority has the right 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 this regulation, an administrative fine under Art. 83 of Regulation 2016/679, having regard to the circumstances established in the proceedings in question, stated that in the case under consideration there were premises justifying the imposition of an administrative fine on the University.

When deciding to impose an administrative fine on WULS-SGGW, 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) Severity and nature of the violations - when imposing the penalty, it was important that the personal data protection violation applies to candidates for studies at WULS-SGGW from the last 5 years and that the number of people affected by the violation is 100,000 as the upper limit (initial notification of a personal data violation addressed to the President of the Personal Data Protection Office of [...] November 2019), and the number of records (entries) in the SOK system includes 81,624. Moreover,

the President of the Personal Data Protection Office took into account that the data protection breach was the result of an employee using an unsecured private laptop computer for private and business purposes, including the processing of personal data of candidates for studies at WULS-SGGW for the purposes of recruitment as a secretary at the University Recruitment Committee, with the administrator not knowing about this fact and not controlling this process also in the SOK system due to the lack of registration download operations the processing of personal data from this IT system. The above circumstances proving a breach of the principle of confidentiality (Article 5 (1) (f) of Regulation 2016/679) and accountability (Article 5 (2) of Regulation 2016/679) have a significant impact on the amount of the fine imposed. It should be emphasized that the failure of the University to sufficiently take into account the principle of accountability specified in Art. 5 sec. 2 of Regulation 2016/679 in the process of using the IT system used to process personal data of candidates for studies has become one of the factors that led to a breach of personal data protection. The collection of data was not recorded, which is confirmed by the collected evidence. Taking into account the scope of the categories of data obtained through this functionality and their scale, it constitutes a fault that prevents the accountability of the person having access to the data, especially in connection with the duties performed by members of the University Recruitment Committee.

2) Categories of personal data affected by the breach of personal data protection - the Candidate Service System, due to the functionality implemented in this system, enabled the import to a private computer, used by the secretary of the University Recruitment Committee and also used to perform official duties, a set of data of candidates for 1st and 2nd degree studies and uniform master's studies at WULS-SGGW including: name, surname, family name, parents' names, PESEL identification number, sex, nationality, citizenship, address of residence, series and number of an identity card or other identity document, including a passport, mobile and / or landline telephone number and other categories of data regarding the course of education to date: i.e. information about completed secondary school, data of secondary school including city, year of graduation from secondary school, number and date of secondary school leaving certificate, authority issuing the certificate, year of the matura exam and d matriculation certificate, authority issuing the matriculation certificate, results obtained on the matriculation examination, completed studies, completed university, completed field of study, grade on the diploma, average grade in studies, field of study for which the candidate is applying, information about qualifying for studies, points qualification of the candidate, the coincidence of the field of study completed with the one for which the candidate is applying (the full list of personal data categories for individual reports available as part of the functionality enabling data export is attached as Annex

59 to the inspection protocol). Considering the above, it should be stated that a wide range of personal data of candidates for studies at WULS-SGGW has undoubtedly been breached, which is a significant circumstance affecting the amount of the administrative penalty.

3) Duration of violations - personal data of applicants for studies at WULS-SGGW, in a form that allows the identification of the data subject, was stored for a longer period than is necessary for the purposes for which the data is processed. Mr. A.G. - [...] stored the personal data of candidates for studies at WULS-SGGW from the last 5 years of recruitment on a portable private computer, which was inconsistent with the prescribed period for storing personal data of candidates for studies, which was specified at WULS-SGGW for 3 months from the end of recruitment . After the purposes of processing have been achieved, in this case, after the recruitment process has been completed or the deadline for appealing against the decision on admission to studies, the data should be deleted or made anonymous, which in this case was not fully performed. The above constitutes a violation by the administrator of the principle of limitation of storage, also known as the principle of temporary limitation of data processing, specified in art. 5 sec. 1 lit. e of the Regulation 2016/679, which also had a significant impact on the amount of the fine imposed by the President of the Personal Data Protection Office.

4) The high degree of administrator's responsibility - the arrangements made by the President of the Personal Data Protection Office allow for the conclusion that the University has not implemented appropriate technical and organizational measures to ensure the security of processing of personal data of candidates for studies, which should be regularly reviewed and updated, in particular failure to sufficiently to assess the effectiveness of these measures. The lack of mechanisms for monitoring, verification and control over the method, scope and timing of the processing of personal data of candidates for studies at WULS-SGGW by the secretary of the University Admissions Committee made it possible for an employee of WULS-SGGW to use Mr. A.G. private equipment for processing the data of candidates for studies at WULS-SGGW, the ability to download data of candidates for studies from the SOK system and take them on this medium outside the processing area in violation of the implemented procedures and provisions of Regulation 2016/679, as well as the authorization granted to the processing of personal data. In addition, the administrator's lack of proper monitoring of policies and documents related to it, including the lack of supervision of compliance with the rules set out in these documents, as well as the lack of audits of organizational units of the Warsaw University of Life Sciences, including the Student Affairs Office, and the University Admissions Committee, with no documentation at the same time. taking these actions resulted in the fact that the administrator did not have full knowledge

about the flow of personal data at the University.

Taking into account the period from which the personal data subject to the breach of personal data protection originate and the findings made by the President of the Personal Data Protection Office allow the conclusion that from the beginning of the application of Regulation 2016/679, as part of the processing of personal data of candidates for studies at WULS-SGGW, the administrator did not comply with: Art. 32 sec. 1 lit. b and lit. d, art. 32 sec. 2 and art. 39 sec. 1 lit. b of the Regulation 2016/679 in connection with art. 5 sec. 2 of Regulation 2016/679 - through improper monitoring of organizational measures in the processing of personal data of candidates for studies at WULS-SGGW, art. 38 sec. 1 of Regulation 2016/679 - by not involving the data protection officer in matters relating to the protection of personal data in the field of technical solutions adopted as part of the SOK system and its subsequent modifications, to art. 25 sec. 1 of Regulation 2016/679 by not taking into account data protection during the processing of data in the SOK system and the adoption of appropriate procedures in this regard.

The principle of accountability set out in Art. 5 sec. 2 of Regulation 2016/679 has been detailed in Art. 32 sec. 1 of this regulation, which requires 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. The risk related to the lack of registers / logs of operations taking place in IT systems supporting the processing of personal data of candidates for studies has not been properly assessed, therefore, adequate technical measures have not been implemented.

As a consequence, it led to the violation by the University of Art. 32 sec. 1 lit. b in connection with Art. 5 sec. 1 lit. f by loss of confidentiality and data integrity, violation of Art. 5 sec. 2 (i.e. accountability rules), and art. 38 sec. 1, art. 39 sec. 1 lit. b and art. 25 sec. 1 of the Regulation 2016/679 having a significant impact on the amount of the penalty imposed.

The University's failure to undertake actions aimed at ensuring the monitoring of the level of threats and accountability in this respect, as well as the adequacy of the introduced safeguards. Failure to perform a risk assessment by the University regarding the possibility of breaching the principle of confidentiality of personal data (Article 5 (1) (f) of Regulation 2016/679) or the principle of limiting data storage (Article 5 (1) (e) of Regulation 2016/679), resulting from the risk of the possibility of exporting a wide range of personal data categories from the SOK system to an external medium. The Candidate Service System as part of one of the modules did not have an implemented function of recording events related to downloading the

database of candidates within the selected field of study, which is a breach that prevents the settlement of a person with access to personal data, especially in connection with the obligations performed by members of the University Recruitment Committee, including her secretary. Lack of implementation into the risk analysis process, including activities related to the development of risk analysis methodology, the head of the Student Affairs Office, who, in accordance with the organizational structure of the University, is responsible for the processing of personal data of candidates for studies. In connection with the above, the violation of 32 par. 1 lit. d and art. 32 sec. 2 of the Regulation 2016/679 in connection with Art. 5 sec. 2 of the Regulation 2016/679 also had an impact on the amount of the administrative fine imposed.

Failure to duly consider the risks associated with processing operations in the performance of the tasks of data protection officers. There are no grounds to believe that data protection inspectors conducted audits in individual organizational units in a comprehensive manner, in particular, there is no evidence of the preparation of reports on the control of compliance with data protection regulations, in particular in the Student Affairs Office and the University Recruitment Committee. Nor can it be concluded that the data protection officers have sufficiently monitored the data protection policies adopted by the controller and the compliance with the provisions on the protection of personal data. There is no evidence that inspectors take actions in the following areas: analyzing, checking the compliance of processing with the provisions of the regulation, as well as issuing recommendations for specific solutions in relation to the SOK system. The fact that an employee of the Warsaw University of Life Sciences, Mr. A.G. had the ability to download from the SOK system, store personal data of candidates for studies at SGGW on a private computer from the last 5 years of recruitment and take them on this medium outside the data processing area without the administrator's knowledge. The inspectors did not perform their tasks with due regard to the risks associated with the processing operations, having regard to the nature, scope, context and purposes of the processing.

Failure to involve the data protection officer in all matters relating to data protection, in particular as regards the adoption of technical solutions as part of the SOK system operation and its subsequent modification, and failure to adopt appropriate procedures in this regard (as an organizational measure referred to in Article 32 para. 1 of Regulation 2016/679), constitutes a violation of art. 38 sec. 1 and art. 25 sec. 1 of Regulation 2016/679 by not taking into account data protection during the processing of data in the SOK system and the adoption of appropriate procedures in this regard. The above circumstances and the University's breach of art. 25 sec. 1, art. 32 sec. 1, art. 32 sec. 2, art. 38 sec. 1, art. 39 sec. 1 lit. b and art. 39 sec. 2 in connection with Art. 5 sec. 2 of Regulation 2016/679, the President of the Personal Data Protection Office took into account

the amount of the administrative penalty when determining the amount of the administrative penalty.

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) WULS-SGGW taking all possible actions to remove the infringement - as it was established in the course of the proceedings, an analysis of the incident was made followed by on:

- commissioning by the Rector of WULS-SGGW to determine the circumstances of the secretary of the University Admissions Committee of WULS-SGGW having the personal data of candidates for studies at WULS-SGGW using a private computer;
- submitting a request to initiate explanatory proceedings by the disciplinary spokesman for academic teachers;
- organizing meetings with University employees regarding the violation in question, as well as meetings with representatives of the University Council of the Student Government and students;
- publishing on the website of WULS-SGGW a message on a personal data breach, which also includes information on possible ways of reducing the negative effects of the breach and the possibility of monitoring credit activity at BIK and other institutions;
- sending via e-mail notifications about a breach of personal data protection to people recruiting for studies in the 2019/2020 academic year, as well as students of the University via the IT system [...];
- sending a letter to the Minister of Science and Higher Education informing about the violation in question and about the actions taken by the University;
- sending a notification to the prosecutor's office about the suspicion of a crime committed by Mr. A.G .;
- sending information on the event to institutions granting loans (including institutions granting the so-called payday loans), telecommunications operators and all banks on the PFSA website (by electronic means), asking for extreme caution when accepting applications;

2) Actions taken as a follow-up to the breach aimed at ensuring the security of personal data processing at WULS-SGGW in the future:

- changes were implemented to the Candidate Service System program in the scope of the recruitment process for second-cycle studies starting from the summer semester in the 2019/2020 academic year:

access to the Candidate Service System for the University and Faculty Admissions Committees was limited only to the area of

building No. [...] and No. [...] - technical / system restriction to a separate subnet,

an individual identification number (DOID) was introduced as the candidate's ID at SOK,

members of the Recruitment Committee were allowed to use the SOK system only with computers prepared for recruitment by the IT Center of the Warsaw University of Life Sciences,

the content of the reports used by the Recruitment Committees has been limited only to the information necessary to make qualification decisions (none of the above reports contain the PESEL number, identity document numbers (passport / Pole's card), address, date of birth, index number, etc.),

a special resource was separated in order to provide secure information to be transferred from the Candidate Service System to the Virtual Dean's Office of the Warsaw University of Life Sciences without the need to send it by e-mail;

correspondence with faculty admission committees - if necessary - containing personal data of persons admitted to studies is carried out using encrypted files;

- copying of data to external disks for administration employees with access to the most important IT systems in which personal data is processed was limited, methods of permanent data removal from media when transferring computers between organizational units using dedicated software were introduced and the "Standard configuration of a computer workstation" was updated, introducing obligation to use additional security,

- the implementation on computers (especially portable) of a solution enabling the encryption of computer drives and external media as well as the implementation of a common domain of the entire University and the addition of all computers used by University employees to it, which through central and uniform management, will significantly increase the security of users and digital resources;

- an analysis of the compliance of the systems processing personal data with the Security Policy, IT system management manual and Regulation 2016/679 was carried out within individual organizational units of WULS-SGGW, along with conclusions and recommendations to improve IT security;

- financial resources have been secured in 2020 for the implementation of planned activities increasing the level of IT security in the field of building and implementing a new recruitment system to support the recruitment process of candidates for studies, conducting an audit of IT systems in the field of architecture, security and performance, adaptation of central IT systems to the requirements Regulation 2016/679, development of the ICT incident management process, implementation of procedures and

business continuity plans, as well as development of the ICT Security Policy (resolution of the Warsaw University of Life Sciences Senate of [...] February 2020 on adopting the IT service plan for 2020 is attached to the letter Of universities from [...] April 2020);

- as part of the university project involving the computerization of the Warsaw University of Life Sciences - SGGW, among others the expansion of approx. 11 IT systems was planned, the replacement of the postal system and tools supporting the work of teaching staff was planned, appropriate agreements were concluded with external entities, the subject of which is centralization in the scope of the [...] service, delivery of an IT Service Desk solution with the "GDPR" module, whose task is to be the possibility of keeping a register of processing activities, a register of authorizations to process personal data, submitting applications for granting a processing authorization and requests for granting / withdrawing authorizations in IT systems;

- work is underway on updating organizational measures aimed at implementing a comprehensive personal data protection policy along with the procedures for: reporting data breaches to the supervisory authority - Art. 33 paragraph. 3 of Regulation 2016/679, assessment and notification of personal data breaches - art. 34 of Regulation 2016/679, regarding the keeping of an internal register of data protection violations - art. 33 of Regulation 2016/679, and the register of processing activities and the scope of the register of categories of processing activities, art. 30 of Regulation 2016/679, in terms of creating new processing processes and taking into account data protection by default - art. 25 of Regulation 2016/679, the procedure of risk assessment and impact assessment for the protection of personal data - art. 24, 32, 35 of Regulation 2016/679, as well as a compliance plan and internal audits, including rules for monitoring and auditing internal procedures, the manner of their implementation and the procedure for selecting a provider processing personal data along with a register of processing entities. For this purpose, the University has started cooperation with an external entity, which is currently commissioning the comprehensive preparation of a draft personal data protection policy along with procedures;

- steps have been taken to update the risk analysis for the recruitment process (the risk analysis for the processing of personal data in the recruitment process along with the methodology for the analysis is attached to the University's letter of [...] June 2020);

- a recovery plan was defined, setting priorities in the administrator's activities to maximize the effectiveness of technical and organizational measures to ensure the security of personal data processing of candidates for studies at WULS-SGGW (the recovery plan is attached to the University's letter of [...] June 2020);

- a person was employed from [...] May 2020 as a personal data protection specialist reporting directly to the Rector of WULS-SGGW, whose tasks include primarily substantive support and cooperation with organizational units of the University in the field of information security and personal data processing, in particular support the recruitment process for studies (the scope of duties of the abovementioned specialist is attached to the University's letter of [...] June 2020);
- e-learning training for SGGW employees was planned, ending with a verification test and generating reports confirming the training and the result obtained.

3) Good cooperation on the part of the University, which, both during the inspection and during the administrative procedure, cooperated with the President of the Personal Data Protection Office in order to remove the breach and mitigate its possible negative effects; within the prescribed period, the University sent explanations and replied to the request of the President of the Office for Personal Data Protection, therefore the degree of this cooperation should be assessed as full.

4) There is no evidence that data subjects have suffered material damage, but the very breach of data confidentiality is a non-pecuniary damage (harm) - natural persons affected by this breach of confidentiality of personal data may, at least, feel the fear of losing control over their personal data. personal data, identity theft or identity fraud, and finally against financial loss.

5) It has not been found that the University previously violated the provisions of Regulation 2016/679, which would be significant for this procedure.

The fact that:

1) The University 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 Regulation 2016/679,

2) In the same case, the measures referred to in art. 58 sec. 2 of Regulation 2016/679,

3) There is no evidence that the University obtained financial benefits and avoids losses in connection with the violation.

In addition, the evidence attached to the University's letter of [...] April 2020 regarding the EZD system (e-mail of [...] April 2020), anti-mobbing procedure (e-mail of [...] July 2019) is irrelevant for the resolution of this case. and [...] July 2019), update of the rules of the company social benefits fund (e-mails of [...] July 2019, [...] July 2019, [...] July 2019, [...] April 2020), video monitoring (e-mail of […] July 2019 and […] July 2019 and […] April 2020), therefore they are not subject to assessment.

The University's explanations presented in the letter of [...] August 2020 are also irrelevant for the resolution in question, because in accordance with the arrangements made by the supervisory body during the inspection and administrative

procedure, the data of candidates for doctoral studies and doctoral students of the University were not on the stolen laptop.

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 on the University is necessary and justified by the weight, nature and scope of the alleged violations of the University. It should be stated that 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 proportional to the identified irregularities in the processing of personal data and would not guarantee that the University will not commit similar measures in the future as in this negligence case.

The President of the Personal Data Protection Office took into account that SGGW is a public sector entity. At this point, the content of Art. 102 of the Act on the Protection of Personal Data, which limits the penalty (up to PLN 100,000) that may be imposed on a public sector entity. In the opinion of the President of the Personal Data Protection Office, the administrative fine of PLN 50,000 applied under the established circumstances of this case 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 University 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 University and other data administrators. Moreover, the applied financial penalty meets the conditions referred to in Art. 83 sec. 1 of Regulation 2016/679 due to the seriousness of the breaches found in the context of the basic requirements and principles of Regulation 2016/679 - in particular the principle of confidentiality expressed in Art. 5 sec. 1 lit. f of the Regulation 2016/679. This is indicated by the serious nature of the breach of personal data protection, the categories of data and the group of people affected by it. Importantly, there is still a risk of unlawful use of their personal data in relation to these people, because the private laptop of an employee of the Warsaw University of Life Sciences, on which the personal data of applicants for studies was stored, has not been found (recovered).

The purpose of the penalty imposed is to ensure that the University performs the duties provided for in Art. 5 sec. 1 lit. e, art. 5 sec. 1 lit. f, art. 25 sec. 1 and art. 32 sec. 1 lit. b and d, art. 32 sec. 2, art. 38 sec. 1, art. 39 sec. 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.

The decision is final. The party has the right to lodge a complaint against the decision with the Provincial Administrative Court in Warsaw, within 30 days from the date of its delivery, via the President of the Office for Personal Data Protection (address: ul. Stawki 2, 00-193 Warsaw). A proportional fee should be filed against the complaint, in accordance with Art. 231 in connection with Art. 233 of the Act of August 30, 2002, Law on proceedings before administrative courts (Journal of Laws of 2018, item 1302, as amended). A party (natural person, legal person, other organizational unit without legal personality) has the right to apply for the right to assistance, which includes exemption from court costs and the appointment of an attorney, legal advisor, tax advisor or patent attorney. The right to assistance may be granted at the request of a party submitted prior to the initiation of the proceedings or in the course of the proceedings. The application is free of court fees.

Pursuant to Art. 105 paragraph. 1 of the Act of May 10, 2018 on the Protection of Personal Data (Journal of Laws of 2019, item 1781), the administrative fine must be paid within 14 days from the date of expiry of the deadline for lodging a complaint to the Provincial Administrative Court, or from on the day the ruling of the administrative court becomes legally binding, to the bank account of the Personal Data Protection Office at NBP O / O Warsaw no. 28 1010 1010 0028 8622 3100 0000. Moreover, pursuant to Art. 105 paragraph. 2 above of the Act, the President of the Personal Data Protection Office may, at the justified request of the punished entity, postpone the date of payment of the administrative fine or divide it into installments. In the event of postponing the payment of the administrative fine or dividing it into installments, the President of the Personal Data Protection Office shall charge interest on the unpaid amount on an annual basis, using a reduced rate of late payment interest, announced pursuant to Art. 56d of the Act of August 29, 1997 - Tax Ordinance (Journal of Laws of 2019, item 900, as amended), from the day following the date of submitting the application.

Pursuant to Art. 74 of the Act of May 10, 2018 on the Protection of Personal Data (Journal of Laws of 2019, item 1781), the submission of a complaint by a party to the administrative court suspends the execution of the decision on the administrative fine.

2020-09-07