THE CHAIRMAN OF PERSONAL DATA PROTECTION

Warsaw, on 05

January

2021

DECISION

DKN.5131.6.2020

Based on Article. 104 § 1 of the Act of June 14, 1960 Code of Administrative Procedure (Journal of Laws of 2020, item 256, as amended), art. 7 sec. 1, art. 60 and art. 102 paragraph 1 point 1 and sec. 3 of the Act of May 10, 2018 on the Protection of Personal Data (Journal of Laws of 2019, item 1781), as well as Art. 57 sec. 1 lit. a), art. 58 sec. 2 lit. e) and lit. i), art. 83 sec. 1-3 and art. 83 sec. 4 lit. a) in connection with art. 33 paragraph 1 and art. 34 sec. 1, 2 and 4 of Regulation 2016/679 of the European Parliament and of the Council 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 May 4, 2016, p. 1 and Journal of Laws UE L 127 of May 23, 2018, p. 2), hereinafter also referred to as "Regulation 2016/679", after administrative proceedings regarding the failure to notify the personal data breach to the President of the Personal Data Protection Office and the failure to notify about the breach of personal data protection of the affected persons by the Medical University of Silesia in Katowice at ul. Księcia Józefa Poniatowskiego 15, President of the Office for Personal Data Protection, finding a violation by the Medical University of Silesia in Katowice at ul. Księcia Józefa Poniatowskiego 15 recipes:

a) Art. 33 paragraph 1 of Regulation 2016/679, consisting in not reporting the breach of personal data protection to the President of the Personal Data Protection Office without undue delay, no later than 72 hours after the breach has been found,

b) art. 34 sec. 1 of Regulation 2016/679, consisting in not notifying about a breach of personal data protection, without undue delay of data subjects,

1) imposes on the Medical University of Silesia in Katowice at ul. Księcia Józefa Poniatowskiego 15, a fine of PLN 25,000 (in words: twenty-five thousand zlotys),

2) orders to notify data subjects of a breach of personal data protection in order to provide them with the information required in accordance with art. 34 sec. 2 of the Regulation 2016/679, i.e .:

a) description of the nature of the personal data breach;

(b) the name and contact details of the data protection officer or designation of another contact point from which more information can be obtained;

c) a description of the possible consequences of a breach of personal data protection;

d) description of measures taken or proposed by the administrator to remedy the breach - including measures to minimize its possible negative effects,

within 3 days from the date on which this decision becomes final.

Justification

The President of the Personal Data Protection Office, hereinafter also referred to as the "President of the Personal Data Protection Office", received information from a dozen or so people about a breach of personal data protection - including, inter alia, on [...] July 2020 from a person who filed a related complaint. According to the information provided by that person, the infringement consisted of making available on the platform [...] (where 237 people were registered as of [...]. in Katowice (hereinafter referred to as the "Administrator"), which took place on three dates: [...] .05.2020, [...] .05.2020 and [...] .05.2020, with most of the participants taking the exam in it, the students were identified with a student ID or ID card. The information (in which the Administrator is also referred to as "AOD") also shows that "On [...]. 06.2020 one of the students informed the starosts of the groups that on the above-mentioned The platform featured recordings of all sections examined from the beginning of the exams, which we did not expect, as we had not been informed that the recording would be made available to a wider group of people after the examination. Due to the fact that the recording was open to the public, information about the recording was shared among students, and the alarmed students began to check whether their data from their ID cards was clearly visible. Many people logged in to the platform or sent each other links to the recordings. From AOD's side, there was no reaction, we didn't get any information about improper processing of our personal data, so in fear of deleting the recording to conceal the security breach incident, to secure evidence of AOD's malfunction, we decided to secure the file. In order to secure the evidence supporting the validity of our report, photos of the computer screen were also taken, with paused recordings and visible ID cards of our colleagues. When checking the links, it turned out that it was possible to view the recording after obtaining the link to [...] without logging in, which proved that our personal data visible in the films was insecure. The starościna of the semester made a phone call to (...) the exercise manager to inform about the situation and ask for reporting this fact to

the Personal Data Protection Office, because the students reported their ID cards as reserved in banks and other institutions after the incident. After some time, we received information from the Head of the Department (...) that we, students, had stolen personal data that had leaked out through our fault and that the person who downloaded the file would face criminal liability ". Moreover, the information stated that "It is not true that only the users of the e-learning platform assigned to the course - students and authorized employees of the University - had access to the recordings before they were hidden, because they had access to the recordings for a period of at least a few days (respectively from [...]. 05.2020, [...] .05.2020 or [...] .05.2020) were also owned by other people - all students of groups 1-7 of the 6th year, people doing their homework, students from the Faculty [...], as well as every person with a link under which a recording has been placed. (...) We do not know the full circle of people who could have access to our personal data, as well as the scope of personal data relating to specific persons whose data was shared, because the DPO, questioning its responsibility for the breach of security of their processing, did not cooperate with us for the purpose of a detailed explanation of the circumstances of the incident. (...) It is completely untrue to say that only 26 people had access to the tapes. In the letter of [...] .06.2020, an analysis of the evidence obtained was cited, which would indicate limited access of only 26 people. This information is so unreliable that it raises our doubts as to the reliability of the AOD in the case - which, after all, is an entity with an interest in not disclosing the fact of the breach committed by its employees. At this point, I would like to explain that each academic group consists of 26 people, while the disseminated recordings concerned the exams of at least 6 groups from our semester. Moreover, the recordings could also be viewed by students from the Faculty [...] and homeworkers (approx. 200 people) ". In addition, the information provided by this person shows that "The fact is that [...] they activated the" data leakage "mechanism, i.e. they reported the information provided by students about the breach of personal data security to the Dean and Rector, but finally appointed by the IODO Administrator and the Rector (which is "a decision-making unit" as the DPO put it) expressed the position that the incident of 200 people viewing the identity cards of some 100-150 other people is not a leak of personal data. "

In connection with the receipt of the above information on the breach of confidentiality of personal data of the majority of students participating in these exams, with regard to the data contained in the student ID or ID card, on [...] July 2020, the President of the Office for Personal Data Protection, pursuant to Art. 58 sec. 1 lit. a) and e) of Regulation 2016/679, asked the Administrator to clarify whether the incident was analyzed in terms of the risk of violating the rights and freedoms of natural persons, necessary to assess whether there was a breach of data protection resulting in the need to notify the President

UODO and persons affected by the violation. In the letter, the President of the Personal Data Protection Office indicated to the Administrator how to report the violation and called for explanations within 7 days from the date of receipt of the letter.

The response to the above, which the Administrator provided in a letter of [...] August 2020, shows that a breach of personal data protection consisting in disclosing personal data to unauthorized recipients took place. The letter also shows that the Administrator assessed the event in terms of the risk of violating the rights or freedoms of natural persons. The administrator indicated that "The logs and information about the people who downloaded the recordings were secured (...). The findings show that the security mechanisms of the e-learning platform have not been broken and the so-called data leakage. In addition, on the basis of analyzes made by the Administrator of the e-learning Platform and the Department for [...], it was found that the recording was downloaded by 26 people known to the University by name and surname - members of the University community, i.e. (examined students of a given field and academic teachers), who bear individual responsibility for not disseminating them. Due to the scope of making the recordings available, limited only to the participants of the exam and the low probability of violating the rights and freedoms of data subjects, the University waived the obligation to report the violation to the Office for Personal Data Protection, referred to in art. 33 paragraph 1 of the GDPR Regulation ". In this letter, the administrator also stated that "the Dean of the Faculty [...] was instructed that in the event of becoming aware of the unethical use of data by students or employees, there are grounds for implementing the disciplinary proceedings referred to in Art. 275 and art. 307 of the Act of July 20, 2018, Law on Higher Education and Science (i.e. Journal of Laws of 2020, item 85, as amended) ". Moreover, the explanations contained in this letter show that "The administrator of the e-learning platform has developed a proprietary amendment to the system [...] which makes it impossible for students to download videos. Downloading movies is a normal functionality of the system (it does not count as hacking activities or system vulnerabilities) for logged in students and is recorded - the created virtual room is available only to the examined group and only these people have access to the recorded recordings. The teacher's mistake consisted in not switching off the room and access to it after the exam. " As can be seen from the above, the Administrator stated that it is unlikely that the breach would result in a risk of violating the rights or freedoms of data subjects.

In connection with the above-mentioned in a letter - due to the risk assessment of violation of the rights or freedoms of data subjects, the President of the Personal Data Protection Office in a letter of [...] September 2020 informed the Administrator that pursuant to Art. 33 paragraph 1 of Regulation 2016/679, in the event of a breach of personal data protection, the data

controller shall, without undue delay - if possible, no later than 72 hours after finding the breach - notify the competent supervisory authority pursuant to art. 55, unless the breach is unlikely to result in a risk of violation of the rights or freedoms of natural persons and that the notification submitted to the supervisory authority after 72 hours is accompanied by an explanation of the reasons for the delay. In addition, he indicated to the Administrator that "When assessing whether the violation results in a risk of violating the rights or freedoms of natural persons, one should take into account, inter alia, the content of recitals 75 and 85 of the above-mentioned regulation. In addition, the Article 29 Working Party in the Guidelines on reporting personal data breaches in accordance with Regulation 2016/679 (WP250rev.01) indicated that the controller, when assessing the risk to individuals resulting from the breach, should take into account the specific circumstances of the breach, including the importance of the potential impact and the probability of of its occurrence and recommended that the criteria indicated in these Guidelines should be taken into account during the assessment. In the above-mentioned The guidelines also clarify that when assessing the risks that may arise from a breach, the controller should collectively consider the severity of the potential impact on the rights and freedoms of natural persons and the likelihood of their occurrence. Of course, the risk increases when the consequences of a breach are more severe and also when the probability of their occurrence increases. In case of any doubts, the controller should report the violation, even if such caution could turn out to be excessive. It should be noted that the above-mentioned recordings show, among others, identity cards and student IDs, hence it is necessary to assess what data has been made available to unauthorized persons and, consequently, what is the risk of violating the rights or freedoms of natural persons ". At the same time, the President of the Personal Data Protection Office called the Administrator, pursuant to art. 58 sec. 1 lit. a) and e) of Regulation 2016/679, to provide, within 7 days from the date of delivery of the letter, information whether the incident has been re-analyzed in terms of the risk of violating the rights and freedoms of natural persons, necessary to assess whether there has been a violation data protection resulting in the need to notify the President of the Personal Data Protection Office and the persons affected by the breach, and if so, whether the results of the re-analysis are identical to the results of the previously conducted assessment by the administrator of the above-mentioned events.

In response of [...] September 2020, the Administrator informed the President of the Personal Data Protection Office that "(...) from the date of submitting the first explanations (...) until today, the University has not received any additional information that would have a direct impact on the factors determining the need to re-analyze incident risk, the possible escalation of which has

been promptly, effectively and technically stopped. In addition, I would like to explain that the recordings of the course of the exam were available to students of the marked year of one field of study and lecturers, where they mutually have access to such information in terms of knowing the identity of the data subjects. However, it is undisputed that the scope of data that can be downloaded by the above-mentioned the group of people was wider, but effective measures were taken to block this violation along with the proprietary IT reprogramming of the e-learning platform functionality. Due to the fact that the recordings could be downloaded by the above-described group being a separate part of the academic community, the risk of violating the rights of freedom of data subjects was assessed to a small extent ". Attached to the explanations was a letter in which the then Rector instructed the Dean of the Faculty to provide all students with, inter alia, information that "5. If students are aware of the circumstances of unethical use of personal data by students or employees, I kindly ask for such information to be provided to me in writing together with a proof of its support. In the event of confirmation of the above-mentioned information about a breach of security, I kindly ask you to apply to the relevant disciplinary officer to initiate an investigation, and if it is justified, the subsequent disciplinary procedure with all sanctions provided for by law, including removal from the list of students or termination of employment, including legal obligations The university, in particular, notifying the competent law enforcement authorities ". The above-mentioned letter of the Administrator also shows that "The University has not received any information with regard to point 5 of the letter cited, which could be relevant to the case and imply the need for a new analysis. Importantly, it should be emphasized that every student of the Medical University of Silesia in Katowice is obliged to respect the dignity of every human being, and in particular, within the academic community. Such an obligation is known to students and expressed in the Study Regulations of the Medical University of Silesia in Katowice and is confirmed by the signature of each student. Moreover, students are obliged by the University Statute to comply with the internal regulations in force at the University (norms, rules of coexistence and academic customs), including, in particular, those relating to the protection of privacy. Considering the above obligations of students and other members of the academic community in the field of reporting incidents related to information security, no information was received by the University that could affect the risk level or required other technical and organizational measures to expand the catalog of actions taken. "

Moreover, on [...] September 2020, the Administrator sent a letter to the President of the Personal Data Protection Office regarding the complaints submitted to the Office for Personal Data Protection against the Administrator in connection with the incident, in which he informed that "The analysis of complaints (...) shows that the standardized blanco the content of the

complaint and, importantly, the attachments presented therein (including those containing correspondence, screenshots) were shared by the initiator (s) of individual complaints, or were made available by the author of the content of the standardized complaints to an unmarked group of students, which makes him / her in the light of the above-mentioned . the context responsible for disseminating information in an uncontrolled manner (blank pattern with attachments). Therefore, such blame cannot be attributed to the Medical University of Silesia in Katowice, which has taken all available and possible effective measures (...) to block this violation along with the proprietary IT reprogramming of the e-learning platform functionality. The above makes the administrator of the blank complaint form the sole owner of the risk of violating the rights and freedoms of persons whose data in the attachments are related, because, as the explanations submitted by the University show, only 26 people known to the University by name and surname had access to the recordings made available within the group of students. the essential list of persons, which I submit in the appendix to this letter, does not correlate with the personal data of the complainants. As a result, applicants not appearing on the attached list could not obtain a recording of the examination process directly from the University's e-learning system, but if it did, they were likely to be a victim of manipulation secondarily ".

In the absence of notification of a personal data breach to the President of the Personal Data Protection Office and no notification of the breach of personal data protection of persons affected by the breach, on [...] October 2020, the President of the Personal Data Protection Office initiated administrative proceedings against the Administrator (letter reference: [...]) .

In response to the above, in a letter of [...] October 2020, the Administrator explained that it considered that "it is unlikely that the breach in question would result in a risk of violating the rights and freedoms of natural persons for the following reasons:

1. (…) the recordings were accidentally made available on the e-learning platform of the Medical University of Silesia as a result of an incident related to information security, which consisted in not closing the videoconference room in which the examination was conducted due to an employee's error […]. Failure to close the videoconference room in which the course of the exam was recorded meant that after the rendering by the e-learning platform was finished, the system automatically published a file with the recording of the exam in this room (available to logged in users). As part of the actions taken, the platform administrator developed an author's amendment to the system [...], which makes it technically impossible to repeat the situation that has arisen.

2. To the above-mentioned Only the logged-in students of a specific field and year of study had access to the file with the

course of the exam - the analysis of system logs shows that it was 240 people (...)

3. The file with the exam was downloaded by 26 people, which is the actual scope of access. Among the above-mentioned 26 people there are 2 academic teachers and one e-learning platform administrator. (...)

4. The analysis of the recordings of the course of the exams shows that the ID cards were presented by the Students sporadically and only the first page with a photo was presented (which concerns a possible wider scope of data disclosed by the Student than the data processed during the exam: image, voice, name, surname, information about the group, year of study, field of study, subject and the answers given during the exam).

5. Most importantly, many of the documents presented, due to the quality of the students' link, were completely illegible, and in other cases, the quality can be defined on the verge of legibility (...)

6. In addition, I would like to inform you that the generated recording, which could be accessed by students through the online stream player built into the web browser, also when reading, due to the quality of the recipient's link, could have been of lower quality than that described in the preceding point - most likely completely blurred and unreadable.

7. The context of the processing is also worth mentioning, because in the case of conducting the oral examination in a traditional form, a given student group would have access or could view the same scope of the examined Student's data. The difference is only in the form of remote learning and the incident, the occurrence of which made it possible to play the recording of the above-mentioned 26 people logged in to the e-learning platform - members of the academic community ”.

In this letter, the Administrator also explained that "(...) the University, in accordance with Art. 76a of the Act of July 20, 2018 - Law on Higher Education and Science (Journal of Laws of 2018, item 1668, as amended), which was added by the Act of April 16, 2020 (Journal of Laws of 2020, item 695), from [...] .04.2020, could organize the verification of the learning outcomes specified in the study program, in particular, conduct credits and examinations at the end of specific classes and diploma examinations, outside the seat of the university or outside its branch with the use of information technologies ensuring control of their course and registration. In connection with the above-mentioned the legal basis and the changed method of examination, the academic teacher had to verify the identity of the examination participant in order to ensure the proper conduct of the examination ”. It was also emphasized that "(...) the University launched a number of information channels through which students could, individually or anonymously, obtain information about the incident, which, however, the applicants did not use (...). Above Of course, news channels do not replace the obligations set out in Art. 34 GDPR, however,

allow the student to provide additional information, notifications, concerns and other circumstances that could cause a change in the assessment of the risk of violating the rights and freedoms of data subjects, and therefore imply the Administrator's taking information measures both towards students and the Data Protection Office Personal data within the time limit stipulated in the regulations. "

After reviewing all the evidence collected in the case, the President of the Office for Personal Data Protection considered the following:

Pursuant to Art. 4 point 12 of Regulation 2016/679 "breach of personal data protection" means a breach of security leading to accidental or unlawful destruction, loss, modification, unauthorized disclosure or unauthorized access to personal data transmitted, stored or otherwise processed.

Art. 33 sec. 1 and 3 of Regulation 2016/679 provide that in the event of a breach of personal data protection, the data controller shall, without undue delay - if possible, no later than 72 hours after finding the breach - report it to the competent supervisory authority pursuant to Art. 55, unless it is unlikely that the breach would result in a risk of violation of the rights or freedoms of natural persons. The notification submitted to the supervisory authority after 72 hours shall be accompanied by an explanation of the reasons for the delay. The notification referred to in para. 1, must at least: a) describe the nature of the personal data breach, including, if possible, the categories and approximate number of data subjects, as well as the categories and approximate number of personal data entries affected by the breach; (b) include the name and contact details of the data protection officer or the designation of another contact point from which more information can be obtained; c) describe the possible consequences of the breach of personal data protection; (d) describe the measures taken or proposed by the controller to address the personal data breach, including, where appropriate, measures to minimize its possible negative effects.

In turn, art. 34 sec. 1 of Regulation 2016/679 indicates that in a situation where a breach of personal data protection may result in a high risk of violation of the rights or freedoms of natural persons, the controller is obliged to notify the data subject of such a breach without undue delay. Pursuant to Art. 34 sec. 2 of Regulation 2016/679, the correct notification should:

1. describe the nature of the personal data breach in clear and simple language;

2. contain at least the information and measures referred to in Art. 33 paragraph 3 lit. b), c) and d) of Regulation 2016/679, i.e .:

a.name and contact details of the data protection officer or designation of another contact point from which more information can be obtained;

b. a description of the possible consequences of a breach of personal data protection;

c. a description of the measures taken or proposed by the controller to address the personal data breach, including, where appropriate, measures to minimize its possible negative effects.

In the case at hand, there was a breach of personal data protection consisting in making available on the platform [...] of recordings showing the course of practical exams, during which most of the participants - students were identified with a student ID or ID card. The administrator did not question that such a situation had taken place - he even indicated in the explanations he submitted that the following quotation was: "(...) the academic teacher had to verify the identity of the examination participant in order to ensure the proper conduct of the examination." The administrator argued, however, that: "(...) ID cards were presented by the Students sporadically and only the first page with a photo was presented (which concerns a possible wider scope of data disclosed by the Student than the data processed during the exam: image, voice, name, surname , information about the group, year of study, field of study, subject and the answers given during the examination) ".

Responding to the above, it should be noted that the data visible on the first page of the ID card (depending on the time of its issuance, as there are currently ID cards issued according to three models in circulation), except for: photo, first name, surname, date of birth and gender, additionally include:

1) in the case of evidence issued before March 1, 2015: maiden name, parents' names, signature, ID card number and its expiry date,

2) in the case of identity cards issued from March 1, 2015 to March 3, 2019: maiden name, parents' names,

3) for identity cards issued after March 4, 2019: citizenship, identity card number and its expiry date.

In addition, the Administrator did not refer to the issue of data visible on student ID cards, which students presented in connection with taking the exam. According to:

1) Regulation of the Minister of Science and Higher Education of September 14, 2011 on the documentation of the course of studies (Journal of Laws of 2011, item 201, No. 1188, as amended - applicable from October 1, 2011, repealed) on October 1, 2016),

2) Regulation of the Minister of Science and Higher Education of September 16, 2016 on the documentation of the course of

studies (Journal of Laws of 2016, item 1554, as amended - applicable from October 1, 2016, repealed on 1 October 2018), which define the model of the electronic student ID card, the ID card shows: a color photo of the ID card holder, university name, name, address, date of issue, album number, PESEL number (and in the case of foreigners: date of birth, respectively). On the other hand, according to the current regulation of the Minister of Science and Higher Education of September 27, 2018 on studies (Journal of Laws of 2018, item 1861, as amended - in force from October 1, 2018), such a card is contains all the above-mentioned data, except for the student's address.

In the submitted explanations, the Administrator indicated that the data recorded on the recordings contained in the above-mentioned documents may remain illegible or only partially legible. The above statement may raise doubts in the context of the purpose for which these documents were presented, i.e. verification of the identity of the person taking the exam. Moreover, the fact that the data could be partially legible does not exclude the possibility of reading it by an unauthorized person. Finally, the existence of programs which make it possible to process photos or recordings in an appropriate way in such a way that the data can be read cannot be ignored. All these circumstances, as important, should be taken into account by the Administrator when assessing whether there has been a breach of personal data protection, what was its scale and whether it was potentially associated with the risk of violating the rights or freedoms of data subjects, and whether this risk is high. Meanwhile, as is clear from the explanations provided, the Administrator did not do it.

It should also be emphasized that in the present case, it is not important whether an unauthorized recipient actually came into possession and familiarized himself with the personal data of other persons, but that there was such a risk, and consequently also a potential risk of violating the rights or freedoms of data subjects. . In his explanations, the administrator emphasized that he had not received any information indicating unauthorized use of personal data provided as a result of the breach in question. Therefore, it concluded that the violation did not involve the risk of violating the rights or freedoms of those affected.

It is worth emphasizing that the administrator, however, foresaw that the breach may involve such a risk - this is evidenced by the fact that he requests the transmission of signals about possible unauthorized use of the personal data provided and threatens with the consequences that such use of data may entail (disciplinary proceedings , removal from the list of students, termination of employment, notification of law enforcement agencies). Making the reaction to a breach dependent on the fulfillment of its potential consequences is contrary to the principle according to which the controller is to counteract the consequences of a breach or minimize its negative effects (in a situation where it is no longer justified to apply measures to

prevent them). It should be emphasized that the possible consequences of the event that occurred do not have to materialize - in the content of Art. 33 paragraph 1 of Regulation 2016/679, it was indicated that the mere occurrence of a breach of personal data protection, which involves the risk of violating the rights or freedoms of natural persons, implies an obligation to notify the breach to the competent supervisory authority. Therefore, the fact raised by the Administrator that the quotation: "no information has been received by the University that could have an impact on the change of the risk level or requiring taking other technical and organizational measures extending the catalog of actions taken" is not relevant for determining the Administrator's obligation to report the violation in question protection of personal data to the President of the Personal Data Protection Office, in accordance with art. 33 paragraph 1 of Regulation 2016/679.

In the case at hand, there was a risk of unauthorized possession of personal data by as many people as they had potential access to. This is at least as many people as were registered on the platform, because the information received by the local Office shows that it was possible to "view the recording after obtaining a link to [...] without logging in". The explanations submitted by the Administrator on [...] September 2020 also indicate that the access to the recordings in question was granted to a wider group of people than assumed by the Administrator. It should also be emphasized that the possible opening of the file containing the recording by anyone, its downloading or further sharing, leads to an increase in the scale of the breach and thus the risk of violating the rights or freedoms of data subjects.

In view of the above, it should be considered that as a result of the event in question there was a breach of the confidentiality of the data of those persons who, when taking the exams, had student ID cards or ID cards visible on the subject recording - in terms of data contained in these documents - that is, a breach security leading to accidental, unauthorized disclosure of the data of these persons, which clearly determines that there has been a breach of personal data protection. It is also worth noting that as a result of the incident, unauthorized recipients were made available to unauthorized recipients, in addition to the data on the documents presented by them, also information about the student: about the group, year of study, field of study, subject and the answers given during the exam.

It should be emphasized that the breach of confidentiality of data that occurred in the case in question, in connection with the breach of personal data protection consisting in making available on the platform [...] recordings showing the course of practical exams, during which most of the students participating in them were identified with a student ID or ID card, as a result of which the confidentiality of these students' data was breached with regard to the data on the student ID card or ID card,

poses a high risk of violating the rights or freedoms of natural persons. As the Article 29 Working Party points out in the guidelines on reporting personal data breaches in accordance with Regulation 2016/679, hereinafter also referred to as "guidelines": people whose data has been breached. Examples of such damage include discrimination, identity theft or fraud, financial loss and damage to reputation. " There is no doubt that the examples of damage cited in the guidelines may occur in the case of persons whose personal data - in some cases together with the PESEL identification number or the series and number of the ID card - were recorded on the shared recordings. Another important factor for such an assessment is the possibility of easy identification of persons whose data was affected by the breach, based on the disclosed data. In the case at hand, there was a disclosure of recordings with images and voices of students who, when taking the exams, showed student IDs or ID cards with the above-mentioned personal data to verify their identity - in some cases also the PESEL identification number or series and number of the identity card in combination with other data. Moreover, by making these recordings available to unauthorized persons, other data were disclosed, such as: "(...) information about the group, year of study, major, subject and the answers given during the exam." As a consequence, this means that there is a high risk of violation of the rights or freedoms of persons covered by the violation in question, which in turn results in the Administrator being obliged to notify the breach of personal data protection to the supervisory authority, in accordance with art. 33 paragraph. 1 of the Regulation 2016/679, which must contain the information specified in art. 33 paragraph. 3 of this regulation and to notify these persons of the infringement pursuant to Art. 34 sec. 1 of the Regulation 2016/679, which must contain the information specified in art. 34 sec. 2 of this regulation.

For the above assessment, it does not affect whether the file containing the recording showing the course of the exams in question was downloaded by twenty-six people, the number indicated by the Administrator in the submitted explanations. There is no certainty that the file was not then made available to other unauthorized recipients, and the administrator cannot hold the persons who had access to these recordings responsible for the breach - in the case at hand, it is clear that it was the administrator's omissions that led to the breach of data protection. personal data, which is associated with the risk of violating the rights or freedoms of persons affected by it. It is worth emphasizing once again that the information received by the President of the Personal Data Protection Office in connection with the incident, shows, inter alia, that there was "the possibility of viewing the recording after obtaining a link to [...] without the need to log in". Even if it was assumed that the possibility of getting acquainted with the personal data presented in the shared recording was possible only for the above-mentioned

twenty-six people, the fact that these persons are in any relationship with the Administrator does not give any guarantees as to the intentions of these persons, and the possible consequences of using such data categories may be significant for the persons whose data was affected by the breach. In the above-mentioned of the guidelines stated: "Whether a controller knows that personal data is in the hands of persons whose intentions are unknown or who may have malicious intent may have a bearing on the level of potential risk. There may be a breach of data confidentiality consisting in an accidental disclosure of personal data to a third party, as defined in Art. 4 point 10, or to another recipient. This may be the case, for example, if personal data is inadvertently sent to the wrong department of the organization or to a vendor organization whose services are widely used. The administrator may request the recipient to return or securely destroy the data received. In both cases - due to the fact that the controller is in a permanent relationship with these entities and may know their procedures, their history and other relevant details concerning them - the recipient can be considered "trusted". In other words, the administrator can trust the recipient enough to be able to reasonably expect that the party will not read or access the data sent by mistake, and that he will follow the instructions to send them back ". In the present case, however, there are no grounds for recognizing and treating unauthorized recipients as "trusted recipients", which determines the existence of a risk of violation of rights or freedoms for persons covered by the violation in question. Moreover, the Article 29 Working Party clearly states in the guidelines that "in case of any doubts, the controller should report the breach, even if such caution could turn out to be excessive".

It is also irrelevant that "as part of the actions taken, the platform administrator developed a proprietary amendment to the system [...], which makes it technically impossible to repeat the situation that occurred." The data has been made available to unauthorized persons, which means (which should be emphasized again) that there was a security breach leading to unauthorized disclosure of personal data, and the scope of this data (including in some cases also the PESEL identification number or the series and number of the ID card) determines this that there was a high risk of violating the rights or freedoms of natural persons. The development and implementation of such an amendment should be considered as a measure taken by the controller to minimize the risk of such a breach in the future, and not as an action to minimize the risk of violating the rights or freedoms of data subjects. Also, the determination by the Administrator of who the persons who downloaded the file containing the recordings in question were, does not minimize the risk of violating the rights or freedoms of the data subjects.

At the same time, it should be emphasized that the data controller allowing the use of means of communication such as those

used to conduct examinations in the case in question, should be aware of the risks related to, for example, improper protection of recordings against unauthorized access and, in order to minimize them, take appropriate organizational and technical measures. The existence of these risks, in the absence of actions of the data controller aimed at minimizing them by implementing appropriate organizational and technical measures, directly leads to the risk of violating the rights or freedoms of natural persons.

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

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

In turn, recital 86 of the preamble to Regulation 2016/679 explains: "The controller should inform the data subject without undue delay of the breach of personal data protection, if it may result in a high risk of violating the rights or freedoms of that person, so as to enable that person to take necessary preventive actions. Such information should include a description of the nature of the personal data breach and recommendations for the individual concerned to minimize the potential adverse effects. Information should be provided to data subjects as soon as reasonably possible, in close cooperation with the supervisory authority, respecting instructions provided by that authority or other relevant authorities such as law enforcement authorities. For example, the need to minimize the immediate risk of harm will require the immediate notification of data

subjects, while the implementation of appropriate measures against the same or similar breaches of data protection may justify subsequent notification. '

By notifying the data subject without undue delay, the controller enables the person to take the necessary preventive measures to protect the rights or freedoms against the negative effects of the breach. Art. 34 sec. 1 and 2 of Regulation 2016/679 is intended not only to ensure the most effective protection of the fundamental rights or freedoms of data subjects, but also to implement the principle of transparency, which results from Art. 5 sec. 1 lit. a) Regulation 2016/679 (cf. Chomiczewski Witold [in:] GDPR. General Data Protection Regulation. Comment. ed. E. Bielak - Jomaa, D. Lubasz, Warsaw 2018). Proper fulfillment of the obligation specified in art. 34 of Regulation 2016/679 is to provide data subjects with quick and transparent information about a breach of the protection of their personal data, together with a description of the possible consequences of the breach of personal data protection and the measures that they can take to minimize its possible negative effects. Acting in accordance with the law and showing concern for the interests of data subjects, the controller should, without undue delay, provide data subjects with the best possible protection of personal data. To achieve this goal, it is necessary to at least indicate the information listed in Art. 34 sec. 2 of Regulation 2016/679, from which the administrator did not fulfill. Therefore, when deciding not to notify the supervisory authority and the data subjects of the breach, the administrator in practice deprived these persons of reliable information about the breach and the possibility of counteracting potential damage, provided without undue delay.

When applying the provisions of Regulation 2016/679, it should be borne in mind that the purpose of this regulation (expressed in Article 1 (2)) is to protect the fundamental rights and freedoms of natural persons, in particular their right to the protection of personal data, and that the protection of natural persons in connection with the processing of personal data is one of the fundamental rights (first sentence of Recital 1). In case of any doubts, e.g. as to the performance of obligations by administrators - not only in a situation where there has been a breach of personal data protection, but also when developing technical and organizational security measures to prevent them - these values should be taken into account in the first place. Consequently, it should be stated that the Administrator did not notify the personal data breach to the supervisory body in compliance with the obligation under Art. 33 paragraph 1 of the Regulation 2016/679 and did not notify the data subjects of a breach of data protection without undue delay, in accordance with art. 34 sec. 1 of the Regulation 2016/679, which means the Administrator's violation of these provisions.

Pursuant to Art. 34 sec. 4 of Regulation 2016/679, if the controller has not yet notified the data subject about the breach of personal data protection, the supervisory authority - taking into account the probability that this breach of personal data protection will result in a high risk - may request it or may state that that one of the conditions referred to in sec. 3. In turn, from the content of Art. 58 sec. 2 lit. e) of Regulation 2016/679 it follows that each supervisory authority has the right to remedy the need for the controller to notify the data subject about a breach of data protection.

Moreover, pursuant to Art. 58 sec. 2 lit. i) of Regulation 2016/679, each supervisory authority has the power to apply, in addition to or instead of other remedial measures provided for in Art. 58 sec. 2 of Regulation 2016/679, an administrative fine under Art. 83 of the Regulation 2016/679, depending on the circumstances of the specific case. The President of the Personal Data Protection Office states that in the case under consideration there are circumstances justifying the imposition of an administrative fine on the Administrator pursuant to Art. 83 sec. 4 lit. a) of Regulation 2016/679 stating, inter alia, that the breach of the administrator's obligations referred to in art. 33 and 34 of Regulation 2016/679 is subject to an administrative fine of up to EUR 10,000,000, and in the case of an enterprise - up to 2% of its total annual worldwide turnover from the previous financial year, with the higher amount being applicable. However, with Art. 102 paragraph 1 of the Act of May 10, 2018 on the Protection of Personal Data (Journal of Laws of 2019, item 1781), it follows that the President of the Personal Data Protection Office may impose, by way of a decision, administrative fines of up to PLN 100,000 on: units of the public finance sector, referred to in article 1. 9 points 1-12 and 14 of the Act of 27 August 2009 on public finance, a research institute or the National Bank of Poland. From the paragraph 3 of this article also shows that the administrative pecuniary penalties referred to, inter alia, in para. 1, the President of the Office shall impose on the basis and under the conditions specified in Art. 83 of the Regulation 2016/679.

Pursuant to art. 83 sec. 2 of Regulation 2016/679, administrative fines shall be imposed, depending on the circumstances of each individual case, in addition to or instead of the measures referred to in Art. 58 sec. 2 lit. a) - h) and lit. j) Regulation 2016/679. When deciding to impose an administrative fine on the Administrator, the President of the Personal Data Protection Office - pursuant to art. 83 sec. 2 lit. a) - k) of Regulation 2016/679 - took into account the following circumstances of the case, which necessitate the application of this type of sanction in the present case and which had an aggravating effect on the amount of the fine imposed:

a) The nature and gravity of the infringement (Article 83 (2) (a) of Regulation 2016/679);

The infringement found in the present case is of considerable gravity and serious nature as it is likely to cause pecuniary or non-pecuniary damage to the data breached persons and the likelihood of its occurrence is high.

b) Duration of the infringement (Article 83 (2) (a) of Regulation 2016/679);

The President of the Personal Data Protection Office recognizes the long duration of the infringement as an aggravating circumstance. Several months elapsed from the Administrator receiving information about the breach of personal data protection until the date of issuing this decision, during which the risk of violating the rights or freedoms of persons affected by the breach could be realized, and which these persons could not counteract due to the Administrator's failure to fulfill the obligation notifying them of the breach.

c) Number of injured data subjects (Article 83 (2) (a) of Regulation 2016/679);

In the present case, it was established that the infringement concerned the personal data of many people - all those 6th-year students from six student groups of 26 (according to the information provided to the President of the Office for Personal Data Protection) taking pediatric practical exams, belonging to all sections examined from the beginning of the exams. (held on the dates: […] .05.2020, […] .05.2020 and […] .05.2020) who presented a student ID or ID card when taking the examinations.

d) Intentional nature of the infringement (Article 83 (2) (b) of Regulation 2016/679);

The administrator made a conscious decision not to notify the President of the Personal Data Protection Office and data subjects about the breach, despite receiving information about the event from data subjects and the letters of the President of the Personal Data Protection Office (UODO) addressed to him indicating the possibility of a high risk of infringement of rights in this case. or the freedom of those affected by the violation. Above the Administrator's obligations under Art. 33 paragraph 1 and 3 and article. 34 sec. 1 and 2 have not been implemented. Such omission in this respect, despite the obligation to act "without undue delay", made it impossible for individuals to take action as soon as possible to protect themselves against any negative effects of the breach, which in turn has an impact on their effectiveness in the event of doing so. obligation by the Administrator.

e) The degree of cooperation with the supervisory authority in order to remove the breach and mitigate its possible negative effects (Article 83 (2) (f) of Regulation 2016/679);

In the present case, the President of the Personal Data Protection Office found the Administrator's cooperation with him unsatisfactory. This assessment concerns the Administrator's reaction to the letters of the President of the Personal Data

Protection Office indicating the possibility of a high risk of violating the rights or freedoms of the persons affected by the violation in this case. Correct, in the opinion of the President of the Personal Data Protection Office (UODO), the actions (notification of the infringement to the President of the Personal Data Protection Office and notification of the persons affected by the infringement) were not taken by the Administrator even after the President of the Personal Data Protection Office initiated the administrative procedure in the case.

f) Categories of personal data affected by the breach (Article 83 (2) (g) of Regulation 2016/679);

Personal data made available to unauthorized persons do not belong to special categories of personal data referred to in art. 9 of Regulation 2016/679, however, their wide scope is associated with a high risk of violating the rights or freedoms of natural persons. The data contained in the ID cards, apart from: photo, first name, surname, date of birth and gender, additionally include:

For evidence issued before March 1, 2015: maiden name, parents' names, signature, identity card number and validity date,

For identity cards issued from March 1, 2015 to March 3, 2019: maiden name, parents' names,

For identity cards issued after March 4, 2019: citizenship, identity card number and its expiry date.

On student ID cards, in accordance with:

· The above. Regulation of the Minister of Science and Higher Education of September 14, 2011 on documentation of the course of studies,

· The above. Regulation of the Minister of Science and Higher Education of September 16, 2016 on documentation of the course of studies,

which define the model of the electronic student ID card, you can see: a color photo of the ID card holder, university name, name, address, date of issue, album number, PESEL number (and in the case of foreigners, respectively: date of birth). However, in accordance with the currently applicable above-mentioned Regulation of the Minister of Science and Higher Education of September 27, 2018 on studies, such a card contains all the above-mentioned data for the card, except for the student's address.

In addition, as a result of the violation in question, unauthorized persons could read other information about the students: about the group, year of study, major, subject and the answers provided during the exam.

g) The manner in which the supervisory authority became aware of the breach (Article 83 (2) (h) of Regulation 2016/679);

The President of the Personal Data Protection Office was not informed about the breach of the protection of personal data being the subject of this case, i.e. disclosure of personal data processed by the Administrator to unauthorized persons, in accordance with the procedure provided for in such situations, specified in Art. 33 of Regulation 2016/679 - this information was received from over a dozen other sources. The fact that there is no information about a breach of data protection from the controller obliged to provide such information to the President of the Personal Data Protection Office should be considered as incriminating this controller.

When determining the amount of the administrative fine, the President of the Personal Data Protection Office also took into account the actions taken by the administrator to minimize the damage suffered by the data subjects (Article 83 (2) (c) of Regulation 2016/679). The controller provided data subjects with certain information about the breach and allowed them to communicate through dedicated communication channels. He also pointed out to people who could have unauthorized access to the disclosed recordings for possible disciplinary and criminal consequences of their unlawful use. Such action of the Administrator deserves recognition and approval, however, it is in no case tantamount to the fulfillment of the obligation referred to in art. 34 of the Regulation 2016/679.

The sanctions in the form of an administrative fine, as well as its amount, were not influenced in any way by the other sanctions indicated in Art. 83 sec. 2 of Regulation 2016/679, the circumstances:

a) the degree of responsibility of the controller, taking into account technical and organizational measures implemented by him pursuant to Art. 25 and 32 (Article 83 (2) (d) of Regulation 2016/679) - the breach assessed in this proceeding (failure to notify the President of the Personal Data Protection Office of the breach of personal data protection and failure to notify about the breach of personal data protection of the data subjects) is not related to the by the administrator with technical and organizational measures;

b) relevant previous violations of the provisions of Regulation 2016/679 by the Administrator (Article 83 (2) (e) of Regulation 2016/679) - no previous violations committed by the administrator were found;

c) compliance with previously applied measures in the same case, referred to in Art. 58 sec. 2 of Regulation 2016/679 (Article 83 (2) (i) of Regulation 2016/679) - in this case, the President of the Personal Data Protection Office has not previously applied the measures referred to in the indicated provision;

(d) adherence to 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 (Article 83 (2) (j) of Regulation 2016/679) - the administrator does not apply approved codes of conduct or approved certification mechanisms;

e) financial benefits or losses avoided, directly or indirectly due to the breach (Article 83 (2) (k) of Regulation 2016/679) - the administrator was not found to obtain any benefits or avoided financial losses due to the breach.

In the opinion of the President of the Personal Data Protection Office, the administrative fine, in 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.

It should be emphasized that the penalty will be effective if its imposition will result in the Administrator fulfilling his obligations in the field of personal data protection in the future, in particular with regard to reporting a personal data breach to the President of the Personal Data Protection Office and notifying about a breach of personal data protection. affected by the infringement. The application of an administrative fine in this case is also necessary considering the fact that the Administrator ignored the fact that we are dealing with a breach of data protection both when the event occurs as a result of deliberate action and when it is caused inadvertently.

In the opinion of the President of the Personal Data Protection Office, the administrative fine will fulfill a repressive function, as it will be a response to the Administrator's breach of the provisions of Regulation 2016/679. It will also fulfill a preventive function; in the opinion of the President of the Personal Data Protection Office, he will indicate to the administrator in question and other data administrators the reprehensibility of disregarding the obligations of administrators related to the occurrence of a breach of personal data protection, and aimed at preventing its negative and often severe consequences for the persons affected by the breach, as well as removal of these effects, or at least a limitation.

In connection with the above, it should be noted that the fine in the amount of PLN 25,000 (in words: twenty-five thousand zlotys) meets the conditions referred to in Art. 83 sec. 1 of Regulation 2016/679 due to the seriousness of the breach found in the context of the basic objective of Regulation 2016/679 - the protection of fundamental rights and freedoms of natural persons, in particular the right to the protection of personal data. At the same time, the amount of the administrative fine imposed by this decision on the administrator who is a unit of the public finance sector (a public university - indicated in Art. 9 (11) of the Act of 27 August 2009 on Public Finance) is within the range specified in Art. 102 paragraph 1 of the Act of May 10, 2018 on the Protection of Personal Data (Journal of Laws of 2019, item 1781), the limit of PLN 100,000.

In this factual and legal state, the President of the Personal Data Protection Office resolved as in the sentence.

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, through 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 2019, item 2325, 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 default interest, announced pursuant to Art. 56d of the Act of August 29, 1997 - Tax Ordinance (Journal of Laws of 2020, item 1325, 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.

2021-01-19