THE CHAIRMAN OF PERSONAL DATA PROTECTION

Warsaw, day 13

July

2021

DECISION

DKN.5131.22.2021

Based on Article. 104 § 1 of the Act of 14 June 1960 Code of Administrative Procedure (Journal of Laws of 2021, item 735), art. 7 sec. 1, art. 60, art. 102 paragraph 1 point 1 and sec. 3 of the Act of May 10, 2018 on the Protection of Personal Data (Journal of Laws of 2019, item 1781) and Art. 57 sec. 1 lit. a) and h), art. 58 sec. 2 lit. i), art. 83 sec. 1 - 3, art. 83 sec. 4 lit. a), art. 83 sec. 5 lit. a) in connection with Art. 5 sec. 1 lit. f), art. 24 sec. 1, art. 25 sec. 1, art. 32 sec. 1 lit. b) and d) and art. 32 sec. 2 of Regulation (EU) 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 the protection of data) (Official Journal of the European Union L 119 of 04/05/2016, p. 1, Official Journal of the European Union L 127 of 23/05/2018, p. 2 and the Official Journal of the European Union L 74 of 04/03/2021, p. 35)), after conducting administrative proceedings initiated ex officio on the processing of personal data by the President of the District Court in Zgierz (Zgierz, ul. Sokołowska 6), the President of the Office for Personal Data Protection

finding that the President of the District Court in Zgierz infringed the provisions of Art. 5 sec. 1 lit. f), art. 24 sec. 1 Art. 25 sec. 1, art. 32 sec. 1 lit. b) and d) and art. 32 sec. 2 of Regulation (EU) 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 the protection of data) (Journal of Laws UE L 119 of May 4, 2016, p. 1, Journal of Laws UE L 127 of May 23, 2018, p. 2 and Journal of Laws UE L 74 of March 4, 2021, p. 35)) (hereinafter: Regulation 2016/679), consisting in failure to implement by the President of the District Court in Zgierz appropriate technical and organizational measures ensuring a level of security corresponding to the risk of data processing using external portable memory, ensuring the security of personal data stored there, including protection against unauthorized or unlawful processing and accidental loss, destruction or damage, which resulted in the loss of external portable memory with personal data stored on it in a way seized, imposes on the President of the District Court in Zgierz for violation of Art. 5 sec. 1 lit. f), art.

25 sec. 1, art. 32 sec. 1 lit. b) and d) and art. 32 sec. 2 of Regulation 2016/679, an administrative fine in the amount of PLN 10,000 (in words: ten thousand zlotys).

JUSTIFICATION

The Office for Personal Data Protection on [...] February 2020 received a notification of a personal data breach signed by the President of the District Court in Zgierz (hereinafter: the President of the Court or the administrator), registered under the reference number [...], informing about the breach of personal data protection of 400 people , subject to probation officer supervision and covered by the community interview by the probation officer, in terms of names and surnames, dates of birth, addresses of residence or stay, PESEL registration numbers, data on earnings and / or property, series and numbers of identity cards, telephone numbers, data concerning health and data on criminal convictions. The reported incident took place on [...] February 2020 and consisted in the loss of an unencrypted USB flash drive by a probation officer. In section 2A of the application form, the District Court in Zgierz was indicated as the data controller.

Due to the scope of disclosed personal data, the indicated breach resulted in a high risk of violating the rights or freedoms of natural persons. The administrator therefore informed that on [...] February 2020, he published on the website of the District Court in Zgierz, hereinafter referred to as the "Court", a notice of the violation, indicating that "it is possible that someone will try to use the data stored there". He also asked for "vigilance, and in the event of obtaining information about any attempts to use the data available to the Court - for immediate notification of law enforcement agencies and contact with the District Court in Zgierz."

By letters of [...] May and [...] July 2020, the President of the Office for Personal Data Protection (hereinafter also the President of the Office), requested another, correct notification of natural persons, because the message addressed to the data subjects did not meet the conditions specified in Regulation 2016/679 in terms of the description of the possible consequences of a breach of personal data protection and a description of the measures taken or proposed by the controller to remedy the breach - including, where applicable - measures to minimize its possible negative effects.

In addition, by letters of [...] May and [...] July 2020, the President of the Office requested additional explanations, including: 1. Whether and how probation officers were recommended to secure data stored on external storage media. 2. Has the personal data controller developed and implemented procedures for using external storage media and for securing personal data processed on external media outside the controller's seat. 3. Whether the lost storage medium was handed over to the

curator by the administrator, or did it belong to the curator. 4. If the lost medium was the property of the probation officer, do the data controller's procedures allow for such a possibility and how is the control over such processing of personal data exercised?

In response to the request, on [...] August 2020, the Administrator informed about the posting of a supplemented message on the breach of personal data protection, and by a letter of [...] August 2020, it indicated that:

1. Probation officers were recommended to comply with the data protection regulations in the Court and data protection procedures in individual interviews and during training meetings. 2. He has developed and implemented procedures for the use of external storage media and the protection of personal data processed on external media outside his seat, and this procedure is part of the Information System Management Instruction at the District Court in Zgierz. 3. The lost storage medium was handed over to the probation officer by the Court, while the Data Protection Regulations for the Court prohibit the use of private data carriers for the processing of official data.

In connection with the presented explanations, in a letter of [...] September 2020, the President of the Office initiated administrative proceedings ex officio, due to the possibility of a breach by the District Court in Zgierz, as the data controller, of the obligations arising from Regulation 2016/679, i.e. Art. 5 sec. 1 lit. f), art. 24 sec. 1, art. 25 sec. 1 and art. 32 sec. 1 and 2, in connection with the breach of personal data protection (ref. [...]). Moreover, the President of the Office called on the Court to present further explanations and documentation concerning:

1. Indication whether, before the breach in question, the data controller defined the rules for the processing of personal data and the security measures applied using flash drives, and if so, what steps were taken by the administrator to ensure the effectiveness of the introduced solutions, and in particular whether and how the was the verification of their compliance by persons with access to personal data, including probation officers. 2. Determining whether, and if so, how the lost medium has been protected against access to personal data processed using it. 3. Indication whether the security measures were implemented by the administrator before the medium was released for use, or whether the curator was obliged to apply them personally. 4. Provide information whether probation officers were acquainted with the implemented procedures and solutions before the violation in question occurred. 5. Indication of whether, prior to the occurrence of the personal data breach in question, the controller performed an analysis of the risk of a possible breach in this respect. 6. Provide information on whether, and if so, when and how, the controller regularly tested, measured and assessed the effectiveness of technical and

organizational measures to ensure the security of the processed personal data concerned by the breach.

In response, the Administrator, in a letter of [...] October 2020, explained that before the infringement occurred, he had implemented a personal data protection system in the form of rules for the processing of personal data, which were set out in the Security Policy of the District Court in Zgierz and the IT System Management Instruction for data processing personal data at the District Court in Zgierz. This system has been operating in the administrator's structure since [...] November 2017, and the implemented documentation is constantly updated and audited by a data protection officer appointed for this purpose. According to the appendix No. 4 attached to the letter, "Rules for the protection of data carriers after the update of [...] May 2018", "it is forbidden to use and process business data with the use of private information media (including flash memory, CDs, USB flash drives). and external drives) ". In order to ensure the effectiveness of the implemented solutions, the Court undertook activities in the form of stationary and e-learning training courses for employees of the Court (including probation officers), regarding the protection of personal data and records of the implemented documentation, duties performed by the data protection officer at the controller's seat, on- line and ad hoc controls carried out by the data protection officer during office hours.

As further pointed out by the Administrator, in accordance with the content of the IT System Management Instruction, the obligation to secure the medium rests on the user who has secured it by storing it in a lockable bag, while after the violation in question, the procedure for issuing data carriers was updated by introducing recording, encryption and password protection on media. All employees of the Court, including probation officers, undergo training in the field of data protection and rules for dealing with data processed in the District Court in Zgierz. Trainings are conducted by an e-learning platform, after completing such training, the employee must pass the knowledge test, only after passing the test, the system generates a certificate and authorization to process personal data, an integral part of which is a declaration of reading the documentation, as well as in a traditional form, conducted by the data protection officer. The administrator also carried out a risk analysis of the possibility of this type of breach in the form of loss of equipment or media, defining the risk at an average level and indicating the need to reduce this risk, adopted as a sufficient measure limiting the possibility of this risk materializing in the form of training for staff on potential threats.

In terms of regular testing, measuring and assessing the effectiveness of technical and organizational measures to ensure the security of personal data processed, in the context of the implementation of obligations resulting, inter alia, joke. 32 sec. 1 lit.

d) of Regulation 2016/679, the Administrator indicated that the data protection officer, in consultation with the Director of the Court, carries out ad hoc checks in individual court divisions during visits in accordance with the duty schedule. In special cases, the check is made at the request of the head of the department, while the testing, measurement and evaluation of system security and their effectiveness is carried out by the IT department. However, he did not provide documentation confirming the performance of any testing, measurement and evaluation of the effectiveness of the implemented technical and organizational measures.

The administrator also indicated that after the violation in question, in accordance with the order no. [...] of the President of the District Court in Zgierz of [...] February 2020, all removable memories were secured with an encryption application.

In connection with the above, on [...] March 2021, the President of the Office called on the Court to provide further explanations, in the form of an indication of the provisions constituting the legal basis for appointing a probation officer in relation to each of the cases granted to him to conduct cases in which personal data were processed on a lost storage medium.

In a reply sent to the supervisory authority on [...] April 2021, the Administrator indicated that the duties and powers of probation officers as well as the legal conditions for this function are specified in the Act of July 21, 2001. on probation officers (Journal of Laws of 2020, item 167), hereinafter referred to as the "Act on probation officers". After the amendment of February 21, 2019 and the addition of Art. 9a - probation officers are fully legitimized to collect and process information necessary in the cases entrusted to them. Supervisions were ordered under § 2 of the Regulation of the Minister of Justice of 12 June 2003 on the detailed manner of exercising the rights and obligations of professional probation officers (Journal of Laws of 2014, item 795), while environmental interviews were commissioned to the probation officer in the following types of cases:

- in matrimonial matters (Article 434 of the Act of November 17, 1964, Code of Civil Procedure (Journal of Laws of 2020, item 1575), hereinafter referred to as "the Code of Civil Procedure", in connection with Article 56 § 2, 58 § 1 and 61¹ § 2 of the Act of February 25, 1964, the Family and Guardianship Code (Journal of Laws of 2020, item 1359) - in cases for adjudication in important family matters (Art. 565¹ of the Code of Civil Procedure); - in custody of minors (Art. 570¹ of the Code of Civil Procedure); - in matters relating to the establishment of guardianship or guardianship and to the enforcement proceedings conducted in order to determine the possibility or manner of exercising custody or guardianship and the living conditions of the person concerned (Art. 570¹ᵃ of the Code of Civil Procedure)); - in matters concerning the adoption of a child (Article 9 of the

European Convention on the Adoption of Children); - in the investigation and examination proceedings in juvenile cases (Article 24 of the Act of October 26, 1982 on juvenile delinquency proceedings (Journal of Laws No. of 2018, item 969); - to determine the circumstances indicating abuse alcohol by the person concerned and disturbing the peace or public order, as well as their relationship in the family, behavior towards minors and work relationship (art. 30a of the Act of October 26, 1982 on Upbringing in Sobriety and Counteracting Alcoholism (Journal of Laws of 2019, item 2277); - in order to determine the living conditions of the person concerned and its functioning in the environment (Art. 42a of the Mental Health Protection Act of August 19, 1994 (Journal of Laws of 2020, item 685); - control interviews conducted by professional probation officers in the supervision of social probation officers and other authorized persons (art. point 4 of the Act on probation officers and § 5 point 2 of the Regulation of the Council of Ministers of June 12, 2003 on the detailed manner of exercising the powers and duties of probation officers (Journal of Laws of 2014, item 989).

The Administrator further explained that the procedure for conducting interviews by a family probation officer was specified in § 6-8 of the Regulation of the Minister of Justice on the detailed manner of exercising the powers and duties of probation officers and in the Regulation of the Minister of Justice of August 16, 2001 on detailed rules and procedure for conducting probation officers. environmental interviews about minors (Journal of Laws of 2001, No. 90, item 1010). In addition, he indicated that the provisions of § 1 para. 1 and 2, § 2, § 3, § 4 and § 7 of the Regulation of the Minister of Justice of June 11, 2003 on the regulations of activities in the field of conducting an environmental interview and the model questionnaire for this interview (Journal of Laws of 2003, No. 108., item 1018).

Pursuant to Art. 9b of the Act on probation officers, the administrator of data processed in order to perform tasks or duties by the probation officer is the president of the court in which the probation officer performs official duties.

As is clear from the findings, the breach of personal data protection reported to the President of the Office and registered under reference number [...], consisted in the loss by the probation officer of an unencrypted portable flash drive, which was used to process the personal data of 400 people who were subject to probation and covered by an environmental interview by the probation officer, in terms of names and surnames, dates of birth, addresses of residence or stay, PESEL registration numbers, data on earnings and / or property, series and numbers of ID cards, telephone numbers, health data and data on criminal convictions. Thus, pursuant to the above-mentioned provision of the Act on probation officers, the administrator of data processed by the probation officer on a lost medium is the President of the District Court in Zgierz, and not the Court.

In view of the above, in the letter of [...] May 2021, the President of the Office initiated ex officio administrative proceedings against the violation by the President of the District Court in Zgierz, as the data controller, of the obligations arising from Regulation 2016/679, i.e. Art. 5 sec. 1 lit. f), art. 24 sec. 1, art. 25 sec. 1 and art. 32 sec. 1 and 2, in connection with the above-mentioned breach of personal data protection (ref. DKN.5131.22.2021). Moreover, pursuant to Art. 123 § 1 and art. 75 § 1 of the Code of Civil Procedure in connection with joke. 7 sec. 1 of the Act on the Protection of Personal Data, the President of the Office issued [...] in May 2021 a decision on the preparation of certified copies of the files of the proceedings with reference number [...], i.e. a notice of the initiation of administrative proceedings against the District Court in Zgierz on [...] September 2020 , replies of [...] October 2020, requests for clarification of [...] February 2021, replies of [...] March 2021, requests for clarification of [...] March 2021 and the replies of [...] April 2021, in order to include them in the procedure under reference DKN.5131.22.2021.

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

Article 5 of Regulation 2016/679 indicates the rules for the processing of personal data that must be respected by all administrators, i.e. entities designated by EU law or the law of a Member State and 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 ("integrity and confidentiality ").

Pursuant to Art. 24 sec. 1 of Regulation 2016/679, taking into account the nature, scope, context and purposes of processing as well as the risk of violating the rights or freedoms of natural persons of varying probability and seriousness, the controller implements appropriate technical and organizational measures to ensure that the processing is carried out in accordance with this Regulation and to be able to demonstrate it . These measures are reviewed and updated as necessary.

The provision of art. 24 sec. 1 of Regulation 2016/679 specifies the basic and main duties of the administrator, who is charged with the implementation of appropriate technical and organizational measures to ensure the compliance of processing with the requirements of Regulation 2016/679. This is, in particular, about the implementation of the principles set out in Art. 5 sec. 1 of Regulation 2016/679.

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

Pursuant to Art. 32 sec. 1 of Regulation 2016/679, taking into account the state of technical knowledge, the cost of implementation and the nature, scope, context and purposes of processing as well as the risk of violating the rights or freedoms of natural persons with different probabilities and severity, the controller and the processor implement appropriate technical and organizational measures to ensure the level of security corresponding to this risk, including, inter alia, the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services (point b), as appropriate, and regular testing, measurement and evaluation of the effectiveness of technical and organizational measures to ensure the security of processing (letter d).

Pursuant to Art. 32 sec. 2 of Regulation 2016/679, the controller, when assessing whether the level of security is appropriate, takes into account in particular the risk associated with the processing, in particular resulting from accidental or unlawful destruction, loss, modification, unauthorized disclosure or unauthorized access to personal data sent, stored or otherwise processed.

The provisions of Art. 25 sec. 1 and art. 32 sec. 1 and 2 of Regulation 2016/679, along with art. 24 sec. 1 above of the regulation, thus constitute a specification of the provisions referred to in Art. 5 sec. 1 lit. f) Regulation 2016/679, the principles of integrity and confidentiality.

Data confidentiality is a property that ensures, in particular, that data will not be disclosed to unauthorized entities, obtained, inter alia, through the use of technical and organizational measures, adequate to the scope of the data, the context of processing and identified risks. The indicated principle, as results from the established facts, was violated by the President of the Court by issuing for official use to probation officers an unsecured portable storage medium and obliging them to implement security measures for this storage on their own, which as a result of the loss of such a medium by the probation

officer resulted in the possibility of unauthorized access to personal data processed on this medium. As it was established, the only security used by the probation officer was storing the medium in a closed service bag.

As indicated by the Provincial Administrative Court in Warsaw in the judgment of 3 September 2020, file number II SA / Wa 2559/19, "Regulation 2016/679 introduced an approach in which risk management is the foundation of activities related to the protection of personal data and is a continuous process. . Entities processing personal data are obliged not only to ensure compliance with the guidelines of the above-mentioned of the regulation through one-off implementation of organizational and technical security measures, but also to ensure the continuity of monitoring the level of threats and ensuring accountability in terms of the level and adequacy of the introduced security. This means that it becomes necessary to prove to the supervisory authority that the implemented solutions aimed at ensuring the security of personal data are adequate to the level of risk, as well as taking into account the nature of the organization and the personal data processing mechanisms used. The administrator is to independently conduct a detailed analysis of the data processing processes carried out and assess the risk, and then apply such measures and procedures that will be adequate to the assessed risk.

The consequence of such an orientation is the resignation from the lists of security requirements imposed by the legislator, in favor of the independent selection of security measures based on the analysis of threats. Administrators are not informed about specific security measures and procedures. The administrator is to independently carry out a detailed analysis of the data processing processes carried out and assess the risk, and then apply such measures and procedures that will be adequate to the assessed risk. "

In the context of the judgment cited, it should be noted that the risk analysis carried out by the personal data administrator should be documented and justified on the basis of, first of all, the determination of the actual state of affairs at the time of its performance. The characteristics of the ongoing processes, assets, vulnerabilities, threats and existing safeguards as part of the ongoing processes of personal data processing should be taken into account in particular. The scope and nature of personal data processed in the course of activities carried out by the data controller cannot be overlooked during this process, because depending on the scope and nature of the disclosed data, the potential negative consequences for a natural person in the event of a breach of personal data protection will depend.

The term asset is used to indicate anything of value to the data controller. Some assets will be worth more than others and should also be assessed and secured from this perspective. The interrelationships of existing assets are also very important,

e.g. the confidentiality of assets (personal data) will depend on the type and method of processing these data. Establishing the value of assets is necessary to estimate the effects of a possible incident (personal data breach). It is obvious that a wide range of personal data or the processing of personal data referred to in Art. 9 or article. 10 of Regulation 2016/679, may cause (in the event of a breach of personal data protection) far-reaching negative effects for data subjects, so they should be assessed as high-value assets, and thus the level of their protection should be adequately high.

It is necessary, inter alia, for this purpose, so as not to duplicate existing or used safeguards to be specified. It is also essential to check the effectiveness of these security measures, because the existence of an unchecked security may, firstly, eliminate its value, and secondly, it may give a false sense of security and may result in omitting (not detecting) a critical vulnerability, which, if used, will have very negative consequences, including in particular it may lead to a breach of personal data protection.

Vulnerability is commonly defined as a weakness or a security gap which, when exploited by a given threat, may interfere with functioning, and may also lead to incidents or violations of personal data protection. Identifying threats consists in determining what threats and from what direction (reason) may appear.

The method of conducting a risk analysis is, for example, defining the risk level as the product of the probability and the effects of the occurrence of a given incident. Typically, a risk matrix is used to visualize the levels of risk, representing the levels of risk for which the organization defines the relevant activities.

In order for the risk analysis to be carried out properly, there should be a definition of threats that may occur in data processing for each of the assets.

Moreover, in order to fulfill the requirement of art. 32 sec. 1 lit. d) of Regulation 2016/679, indicated, moreover, in the above-mentioned of the judgment of the Provincial Administrative Court in Warsaw as an obligation to ensure the continuity of monitoring the level of threats and ensuring accountability in terms of the level and adequacy of the implemented security measures, the personal data administrator should regularly test, measure and evaluate the effectiveness of technical and organizational measures to ensure the security of processing.

Risk management (conducting a risk analysis and, on that basis, implementing appropriate safeguards) is one of the basic elements of the personal data protection system, and, as the judgment cited above also indicates, is a continuous process. Therefore, periodic verification of both the adequacy and the effectiveness of the applied security measures should take place.

The risk analysis presented by the Administrator in the course of the administrative procedure, carried out before the violation in question, shows a score of 6 for the risk of "Losing equipment, carriers". According to the presented documentation, this is a medium level of risk, resulting in the need to implement security measures in order to reduce it to a low level (considered as an acceptable level), and as a response to the risk, measures to mitigate this risk have been adopted and applied only in the form of "Training for personnel on potential threats ". Of course, training on this type of subject is necessary and necessary, because it can, for example, increase the awareness of the staff. However, with regard to the scope and nature of the personal data processed in this case using this type of device, the training is not an organizational measure that will allow to reduce to a low level or eliminate the risk of losing the medium. It will also not replace technical solutions that have not been provided for. On the other hand, according to the table presenting the result of risk assessment and the response to risk, depending on its amount, for the "Risk response" defined as "O - mitigation", the data controller provides for "Training, additional technical or organizational security", but in this case itself is limited only to training, while the actual securing of the carrier is left to its user, without indicating any examples, defined by the President of the Court as adequate safeguards that the employee may apply. Therefore, actions of this type cannot be considered as the implementation of appropriate technical or organizational measures in the context of Art. 24 sec. 1, art. 25 sec. 1 and art. 32 sec. 1 of Regulation 2016/679 (in particular to ensure the ability to ensure the confidentiality of data on an ongoing basis), because the employee, above all, cannot replace the data controller in the performance of his tasks under these provisions. In addition, the employee may not have the appropriate knowledge in this regard, ignore the need to secure the carrier (as was the case here - the court probation officer secured the carrier only by storing it in a closed bag, which does not protect the carrier itself) or implement a protection inadequate to the scope and nature of the data and the risks involved in this data processing. It should be emphasized that such an organized process of determining and implementing security measures for the processed personal data results in depriving the controller of basic information necessary to properly conduct a risk analysis and on this basis to build an effective data protection system, necessary to ensure continuous data confidentiality, in accordance with the requirement resulting from in particular with Art. 32 sec. 1 lit. b) of Regulation 2016/679, because he will not have knowledge of what safeguards exist in his organization, to what extent and for what threats they will be effective, and he will be deprived of information and the possibility of reacting to the implementation of security inadequate to the threats. In addition, one should also take into account the possibility of a new, previously unknown risk or threat that may materialize or arise during the implementation of a new security, in particular if such

implementation took place incorrectly.

New risks or threats may materialize or be revealed also spontaneously, in a manner completely independent of the administrator, and this is a fact that should also be taken into account both when building a personal data protection system and during its implementation. This, in turn, defines the need to conduct regular verification of the entire personal data protection system, both in terms of adequacy and effectiveness of the implemented organizational and technical solutions.

It should also be emphasized that the examination of the probability of a given event should not be based solely on the frequency of occurrence of events in a given organization, because the fact that an event did not occur in the past does not mean that it cannot occur in the future.

The "Guidelines for the assessment of the likelihood and consequences of a risk" presented in the course of the administrative procedure in the column "Consequences (impact) for the data subject" for each risk assessed from 1 (negligible) to 2 (low), 3 (medium), 4 (high) to 5 (very high) indicate the same consequences for a natural person in the form of: "loss of reputation, financial penalty, loss of a client, inability to provide services, legal consequences". On the other hand, in recitals 75 and 85 of the preamble to Regulation 2016/679, among the possible negative consequences for a natural person, the occurrence of physical damage, damage to property or non-property, such as: loss of control over own personal data or limitation of rights, discrimination, theft or falsification of identity, loss financial, unauthorized reversal of pseudonymisation, breach of reputation, breach of confidentiality of personal data protected by professional secrecy or any other significant economic or social harm.

Therefore, it should be stated that the presented risk analysis was not carried out properly due to the identification of consequences of a breach of personal data protection inadequate for individuals and the adoption of inappropriate security measures - exclusively organizational - with complete disregard of technical measures, e.g. in the form of encryption of flash drives, aimed at risk reduction to an acceptable level. In addition, it should be stated that the solution adopted in this respect by the data controller (only employee training) undermines the effectiveness of the implemented personal data protection system, because, as indicated above, the result of the risk analysis should be an appropriate selection of both technical and organizational measures, i.e. specific measures that will minimize the identified risks. On the other hand, leaving the selection and implementation of security measures to the person who received the unsecured portable memory for use means that the President of the Court deprived himself of the basic data and key information necessary in the context of the performance of obligations under Art. 32 sec. 2 of Regulation 2016/679.

In this context, it should be noted that the Provincial Administrative Court in Warsaw, in its judgment No. II SA / Wa 2826/19 of August 26, 2020, stated that "(...) technical and organizational activities are the responsibility of the personal data administrator, but they cannot be selected in a completely free and voluntary manner, without taking into account the degree of risk and the nature of the personal data protected. "

It should be emphasized that the President of the Court should not use unsecured portable memory devices for the proper performance of the obligations arising from the above-mentioned provisions of Regulation 2016/679. While allowing the possibility of processing personal data with their use, based on a properly conducted risk analysis, they should define and implement appropriate technical and organizational measures to ensure the security of personal data, and then regularly check the effectiveness of these measures. It should be pointed out again that pursuant to Art. 24 sec. 1, art. 25 sec. 1 and art. 32 sec. 1 and 2 of Regulation 2016/679, it is the data controller, not an employee or a person performing official tasks, is obliged to implement appropriate technical and organizational measures so that the processing takes place in accordance with the requirements of the aforementioned regulation. The breach of personal data protection of natural persons in question occurred as a result of failure to apply the protection of a portable storage medium, which made it possible to access personal data processed by unauthorized persons using it.

As indicated by the Provincial Administrative Court in Warsaw in the judgment No. II SA / Wa 2826/19 of August 26, 2020 "This provision [Art. 32 of Regulation 2016/679] does not require the data controller to implement any technical and organizational measures that are to constitute personal data protection measures, but requires the implementation of adequate measures. Such adequacy should be assessed in terms of the manner and purpose for which personal data are processed, but also the risk related to the processing of such personal data, which may vary in size, should be taken into account. (...) The adopted measures are to be effective, in specific cases some measures will have to be low risk mitigating measures, others - high risk mitigating measures, but it is important that all measures (and each individually) are adequate and proportionate to the degree of risk ".

In the order no. [...] of the President and Director of the District Court in Zgierz of [...] November 2017, adopted by the President of the Court, the Security Policy and the Instruction on the Management of the IT System for the Processing of Personal Data in the District Court in Zgierz do not indicate the regulations ensuring regular testing, measuring and assessing the effectiveness of the applied technical and organizational measures to ensure the security of data processing, which also

contributed to the occurrence of a personal data breach.

Despite the request to present documentation confirming the actions taken by the administrator, in order to ensure the effectiveness of the introduced solutions and to confirm the regular testing, measurement and evaluation of the effectiveness of technical and organizational measures to ensure the security of personal data processed, the President of the Court, in a letter of [...] October 2020, limited only to conclude that the data protection officer conducts ad hoc checks in individual court divisions in accordance with the duty schedule, and the testing, measurement and assessment of system security and their effectiveness is carried out by the IT department without presenting, despite the request, any documentation confirming that the type of action taken.

Moreover, it should be noted that conducting "ad hoc checks" does not exhaust the features of regularity. In the opinion of the President of the Office, carrying out ad hoc checks, without adopting a procedure that specifies a schedule of activities ensuring regular testing, measurement and evaluation of the effectiveness of the implemented measures, is insufficient. Moreover, ad hoc actions are usually a reaction to emerging threats, materializing risks of occurrence of adverse events or situations, or a reaction to reported or disclosed gaps in the applied personal data protection system. However, they are not the result of planned activities aimed at verifying the effectiveness of the implemented security measures. Under no circumstances can they be assigned the regularity attribute.

It should be emphasized that regular testing, measuring and evaluating the effectiveness of technical and organizational measures to ensure the security of processing is a fundamental duty of every controller and processor resulting not only from Art. 32 sec. 1 lit. d) of Regulation 2016/679, but also from the fact that during the implementation of individual processing activities, new or previously unknown risks for the security of this processing may appear or arise. The administrator is therefore obliged to verify both the selection and the level of effectiveness of the technical measures used at each stage of processing. The comprehensiveness of this verification should be assessed through the prism of adequacy to risks and proportionality in relation to the state of technical knowledge, implementation costs and the nature, scope, context and purposes of processing. On the other hand, in the present state of facts, the President of the Court did not fulfill this obligation.

Testing, measuring and evaluating the effectiveness of the adopted security measures in order to fulfill the requirement resulting from art. 32 sec. 1 lit. d) of Regulation 2016/679, must be performed on a regular basis, which means consciously planning and organizing, as well as documenting (in connection with the accountability principle referred to in Article 5 (2) of

Regulation 2016/679) of this type of activities in specific time intervals, irrespective of e.g. changes in the organization and the course of data processing processes. However, the President of the Court did not undertake such actions. It should also be emphasized that leaving the choice of the method of securing the portable storage medium used for the processing of personal data and its implementation to the person who is its user deprives the administrator of knowledge about essential elements of the personal data protection system, which in turn prevents the proper implementation of the obligation specified in art. 32 sec. 1 lit. d) Regulation 2016/679.

Therefore, the lack of a reliable risk analysis, combined with the lack of regular testing, measurement and evaluation of the effectiveness of the implemented technical and organizational measures to ensure the security of processing, and the failure to implement technical and organizational measures securing personal data processed with the use of portable storage media, led, which should be reiterated, breach of data protection data, but also prejudices the violation by the President of the Court of the obligations incumbent on the data administrator, resulting from 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, and consequently also the principle expressed in art. 5 sec. 1 lit. f) Regulation 2016/679.

It should also be emphasized that the referred to Art. 25 sec. 1 of Regulation 2016/679, despite the fact that the controller's obligation indicated therein is called "data protection at the design stage", it applies not only to the design stage, but also to the data processing stage itself. The implementation of security measures is a continuous process, not just a one-time action by an administrator. The measures mentioned therein, such as "data minimization" or "pseudonymization", are only an example of measures that should be applied in order to meet the requirement to implement data protection principles and provide processing with the necessary safeguards to meet the requirements of the regulation and protect the rights of data subjects. concern.

Therefore, it should be pointed out again that the obligation of each controller is to process data in accordance with the principles set out in Art. 5 of Regulation 2016/679, in this case in accordance with Art. 5 sec. 1 lit. f).

In conclusion, despite the removal by the President of the Court of the deficiencies in the security of data processed with the use of portable storage media, including the use of encryption of these media, the lack of which resulted in the breach of the confidentiality of personal data, there were premises justifying the application of the President of the Court of powers to impose a penalty against the President of the Court administrative for breach of the principle of confidentiality of data (Article 5 (1) (f) of

Regulation 2016/679), in connection with the breach of the administrator's obligations when implementing technical and organizational measures during data processing, in order to effectively implement data protection principles (Art. 25 (1) of Regulation 2016/679), obligations to ensure confidentiality, integrity, availability and resilience of data processing systems and services (Article 32 (1) (b) of Regulation 2016/679), obligation to regularly test, measure and evaluate the effectiveness of the adopted technical measures organizational and organizational measures to ensure the security of processing (Art. 32 sec. 1 lit. d) Regulation 2016/679) and the obligation to take into account the risk related to the processing resulting from unauthorized access to the processed personal data (Article 32 (2) of Regulation 2016/679).

The exercise by the President of the Office of exercising his / her powers results primarily from the fact that the controller breached one of the basic principles of data processing, i.e. the principle of confidentiality, expressed in Art. 5 sec. 1 lit. f) Regulation 2016/679.

Based on Article. 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 lit. a) - h) and lit. (j) of that regulation, an administrative fine pursuant to Article 83 of the Regulation 2016/679, depending on the circumstances of the specific case.

When deciding to impose an administrative fine on the President of the Court, as well as determining its amount, the President of the Personal Data Protection Office - pursuant to Art. 83 sec. 2 lit. a) - k) of Regulation 2016/679 - took into account, and found it aggravating for the President of the Court, the following circumstances of the case:

a) The nature and gravity of the violation, the number of people injured (Article 83 (2) (a) of Regulation 2016/679). The violation found in the present case, which resulted in the possibility of obtaining unauthorized access to the data processed by the President of the Court by a person or unauthorized persons, and as a consequence obtaining personal data of persons against whom actions were taken by the probation officer, is of considerable importance and serious nature, creates because there is a high risk of negative legal consequences for a large number of people whose data could have been accessed by a person or unauthorized persons. The breach by the President of the Court of the obligations to apply security measures to the processed data against their disclosure to unauthorized persons entails not only the potential, but also a real possibility of using this data by third parties without the knowledge and against the will of the data subjects, contrary to the provisions of Regulation 2016 / 679, e.g. to establish legal relations or enter into obligations on behalf of the persons whose data was obtained, primarily due to the wide scope of personal data, i.e. names and surnames, dates of birth, addresses of residence or

stay, PESEL registration numbers, personal data on earnings and / or property, series and numbers of ID cards, telephone numbers, health and criminal records relating to four hundred (400) natural persons under probation officer custody. b) Duration of the infringement (Article 83 (2) letter a of the Regulation 2016/679) recognizes the long duration of the infringement, because the introduction of recording of portable data carriers and the encryption of data processed with their use took place only after the President of the District Court in Zgierz issued the order No. [...] of [...] February 2020. However, it should be emphasized at the same time, that the consequences of the violation of the provisions of Regulation 2016/679 by the data controller are still ongoing, because the lost, unsecured storage medium has not been found so far, so the unauthorized person or persons may still have access to personal data on this medium, which results in high the risk of violating the rights or freedoms of these persons. c) The extent of the damage suffered by the persons affected by the violation (Art. 83 sec. 2 lit. and Regulation 2016/679). In the present case, there is no evidence that persons accessed by an unauthorized person or persons suffered material damage. Nevertheless, the very breach of the confidentiality of their data is a non-pecuniary damage (harm) to them; natural persons whose data has been obtained in an unauthorized manner may at least feel the fear of losing control over their personal data, identity theft or fraud relating to identity, discrimination, and finally financial loss. d) Unintentional nature of the breach (Article 83 (2) (b) of the Regulation 2016/679) Unauthorized access to personal data of persons against whom the probation officer took actions became possible as a result of failure to exercise due diligence by the President of the Court and undoubtedly constitutes an unintentional nature of the infringement. Nevertheless, the President of the Court as the controller is responsible for any irregularities found in the data processing process. The fact that the President of the Court transferred the obligation to secure the carrier to the probation officer, did not verify whether the probation officer had secured it in any way, and did not carry out a test in terms of the effectiveness of this protection, deserves a negative assessment. In this state of affairs, the negligence of the President of the Court should be considered gross. E) The degree of responsibility of the President of the Court, taking into account technical and organizational measures implemented by him under Art. 25 and 32 of Regulation 2016/679 (Article 83 (2) (d) of Regulation 2016/679). In accordance with the above-mentioned provisions, it is the personal data controller that is primarily responsible for determining what technical and organizational measures will be appropriate in relation to the identified risks. violation of the rights or freedoms of natural persons, implementation of appropriate technical and organizational measures and the obligation to evaluate them at every stage of processing. In the case in question, the administrator did not take any steps to fulfill the obligations arising from the

above-mentioned provisions of Regulation 2016/679, i.e. it did not implement technical and organizational measures adequate to the risk level to ensure the confidentiality of the processed data, and moreover, it shifted this obligation to probation officers. The transfer of the personal data administrator's obligations in the selection and application of appropriate technical measures to other persons resulted in the use of a technical measure in the form of storing a portable storage device in a closed business bag, and therefore completely inadequate in relation to the state of technical knowledge, implementation cost and the nature of , the scope, context and purpose of processing as well as the risk of violation of the rights or freedoms of natural persons with different probability and severity of the risk. f) Categories of personal data affected by the violation (Article 83 (2) (g). names and surnames, dates of birth, addresses of residence or stay, PESEL registration numbers, data on earnings and / or property, series and numbers of ID cards, telephone numbers and data subject to special protection in accordance with art. 9 of Regulation 2016/679 (health data), as well as data on criminal convictions and offenses referred to in art. 10 of Regulation 2016/679, may result in a wide range of negative effects for data subjects. As indicated in recital 75 of the preamble to Regulation 2016/679, "The risk of violating the rights or freedoms of persons, with different probability and severity of threats, may result from the processing of personal data that may lead to physical or material or non-material damage, in particular: if the processing may result in discrimination, identity theft or identity fraud, financial loss, breach of reputation, breach of confidentiality of personal data protected by professional secrecy, unauthorized reversal of pseudonymisation or any other significant economic or social harm; if data subjects may be deprived of their rights and freedoms or the ability to exercise control over their personal data; if personal data is processed revealing racial or ethnic origin, political opinions, religion or philosophical beliefs or trade union membership and if genetic data, data concerning health or data concerning sexuality or criminal convictions and violations of the law or related security measures are processed (...) ". In turn, recital 85 of the preamble to Regulation 2016/679 shows that "In the absence of an appropriate and quick response, a breach of personal data protection may result in physical, 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 harm (…) ". In addition, it should be noted that the processing of personal data of specific categories, specified in art. 9 of Regulation 2016/679 and the data on convictions referred to in Art. 10 of Regulation 2016/679, due to its scope, and thus possible negative consequences of their disclosure, should result in the introduction of a much

higher level of protection of these personal data.

When determining the amount of the administrative fine, the President of the Personal Data Protection Office took into account, as a mitigating circumstance that had an impact on reducing the amount of the fine imposed, good cooperation of the President of the Court with the supervisory authority, undertaken and carried out in order to remove the infringement and mitigate its possible negative effects (Article 83 par. 2 (f) of the Regulation 2016/679). It should be noted here that the President of the Court correctly fulfilled his procedural obligations during the administrative procedure, which ended with the issuance of this decision. The President of the Court also took specific and quick actions, the effect of which was to remove the possibility of an infringement. In particular, the President of the Court removed the susceptibility to violation of the protection of personal data being processed, within 8 days from the occurrence of the violation, he issued an order specifying new rules for dealing with portable memory devices, then within the next 14 days he introduced recording and encryption of the used portable memory devices and notified natural persons about the violation protect their personal data by posting a message about a breach of personal data protection.

The fact that the President of the Office applied in this case the sanctions in the form of an administrative fine, as well as its amount, did not apply to other sanctions indicated in Art. 83 sec. 2 of Regulation 2016/679, the circumstances: a) actions taken by the President of the Court in order to minimize the damage suffered by data subjects (Article 83 (2) (c) of Regulation 2016/679) - such actions have not been taken; b) relevant previous violations of the provisions of Regulation 2016/679 by the President of the Court (Article 83 (2) (e) of Regulation 2016/679) - no other violations of personal data protection were found; c) the manner in which the supervisory authority learned about the violation (Article 83 (2) (h) of Regulation 2016/679). According to Art. 33 paragraph 1 of Regulation 2016/679, in the event of a breach of personal data protection, the controller shall, without undue delay - if possible, no later than 72 hours after finding the breach - reports it to the supervisory authority. It is a fact that in the notification of a personal data breach constituting the basis for initiating administrative proceedings, the District Court in Zgierz was indicated as the administrator of personal data, but it is also a fact that the President of the Court acted on behalf of the Court - it can therefore be assumed that it is this data administrator has sent a notification of a breach of personal data protection, so it should be considered that he has fulfilled the obligation indicated in the above-mentioned provision; d) compliance with the measures previously applied in the same case, referred to in Art. 58 sec. 2 of Regulation 2016/679 (Article 83 (2) (i) of Regulation 2016/679) - the measures indicated in Art. 58 sec. 2 of Regulation 2016/679; e)

application of 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 approved codes of conduct have not been applied; k) - no material benefits or loss avoidance were found.

Taking into account all the above-mentioned circumstances, the President of the Personal Data Protection Office decided that imposing an administrative fine on the President of the Court is necessary and justified by the weight, nature and scope of the violations alleged against the President of the Court. It should be stated that the application to the President of the Court of any other remedy provided for in Art. 58 sec. 2 of Regulation 2016/679, and in particular stopping at an admonition (Article 58 (2) (b)), would not be proportionate to the identified irregularities in the processing of personal data and would not guarantee that the President of the Court will not make further negligence in the future .

Referring to the amount of the administrative fine imposed on the President of the Court, the President of the Personal Data Protection Office concluded that in the established circumstances of the case - i.e. in the event of a breach of several provisions of Regulation 2016/679 (the principle of data confidentiality, expressed in Art. f), and reflected in the obligations set out in Art. 25 sec. 1, art. 32 sec. 1 lit. b) and lit. d) and art. 32 sec. 2) and the fact that the President of the Court is a body of the public finance sector entity - Art. 102 of May 10, 2018 on the protection of personal data (Journal of Laws of 2019, item 1781), which results in the limitation of the amount (up to PLN 100,000) of an administrative fine that may be imposed on a public finance sector entity.

In the presented facts, the most serious breach by the President of the Court of the principle of confidentiality specified in Art. 5 sec. 1 lit. f) Regulation 2016/679. This is supported by the serious nature of the breach, the scope of the personal data subject to the breach and the group of people affected by it (400 - four hundred people administered by the President of the Court). Importantly, in relation to the above-mentioned number of people, there is still a high risk of unlawful use of their personal data, because the purpose for which a person or unauthorized persons may take steps to use this data is unknown.

In the opinion of the President of the Office, the applied administrative fine performs the functions referred to in Art. 83 sec. 1 of Regulation 2016/679, i.e. it will be effective, proportionate and dissuasive in this individual case.

In the opinion of the President of the Office, the penalty imposed on the President of the Court will be effective, because it will lead to a state in which the President of the Court will apply such technical and organizational measures that will ensure the level of security for the data processed, corresponding to the risk of violating the rights and freedoms of data subjects and the

gravity of the threats accompanying the processes. processing of this personal data. The effectiveness of the penalty is therefore equivalent to the guarantee that the President of the Court, from the moment of the conclusion of these proceedings, will be diligent in approaching the requirements of the provisions on the protection of personal data.

The applied administrative pecuniary penalty is also proportional to the infringement found, including in particular its severity, effect, the group of individuals affected by it and the very high risk of negative consequences that they incur in connection with the infringement. In the opinion of the President of the Office, the administrative fine imposed on the President of the Court will not constitute an excessive burden for him. The amount of the fine has been set at such a level that, on the one hand, it constitutes an adequate reaction of the supervisory body to the degree of breach of the administrator's obligations, on the other hand, it does not result in a situation in which the necessity to pay it will entail negative consequences, such as a significant deterioration of the financial situation of the administrator. . In the opinion of the President of the Office, the President of the Court should and is able to bear the consequences of his negligence in the field of data protection, hence the imposition of a fine of PLN 10,000 (ten thousand PLN) is fully justified.

In the opinion of the President of the Personal Data Protection Office, the administrative fine will fulfill a repressive function in these specific circumstances, as it will be a response to the violation by the President of the Court of the provisions of Regulation 2016/679, but also preventive, as it will contribute to preventing future violations of the obligations of the President of the Court. resulting from the provisions on the protection of personal data, both when processing data by the President of the Court himself and in relation to entities acting on his behalf.

In the opinion of the President of the Personal Data Protection Office, the applied fine 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) Regulation 2016/679.

The purpose of the penalty imposed is to ensure that the President of the Court complies with the provisions of Regulation 2016/679 in the future.

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

2021-07-22