Warsaw, day 20

April

2023

Decision

DKN.5131.31.2022

Based on Article. 104 § 1 of the Act of June 14, 1960 Code of Administrative Procedure (Journal of Laws of 2022, item 2000, as amended) in connection with Art. 7, art. 60, art. 101 and art. 103 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. d) and ... i), art. 83 sec. 1–3, art. 83 sec. 4 lit. a) in connection with art. 24 sec. 1, art. 25 sec. 1 and art. 32 sec. 1 and 2, as well as art. 83 sec. 5 lit. a) in connection with art. 5 sec. 1 lit. f) and art. 5 sec. 2 Regulation of the European Parliament and of the EU Council 2016/679 of April 27, 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46 / EC (general data protection regulations) (Official Journal of the EU L 119 of 04.05.2016, p. 1, Official Journal of the EU L 127 of 23.05.2018, p. 2 and Official Journal of the EU L 74 of 4.03.2021, p. 35), after conducting administrative proceedings initiated ex officio regarding the processing of personal data by the Disciplinary Spokesperson of the Bar Association in X. (X., ul. (...)), President of the Office for Personal Data Protection,

stating that the Disciplinary Prosecutor of the Bar Association in X. (X, ul. (…)) violated the provisions of Art. 5 sec. 1 lit. f), art. 5 sec. 2, art. 24 sec. 1, art. 25 sec. 1 and art. 32 sec. 1 and 2 of the Regulation of the European Parliament and of the EU Council 2016/679 of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46 / EC (general regulation on the protection of EU Official Journal L 119 of May 4, 2016, p. 1, EU Official Journal L 127 of May 23, 2018, p. 2 and EU Official Journal L 74 of March 4, 2021, p. 35), hereinafter referred to as "Regulation 2016/679", consisting in the failure by the Disciplinary Prosecutor of the Bar Chamber in X.:

a) appropriate technical and organizational measures ensuring a level of security corresponding to the risk of data processing using external data carriers, in order to protect personal data stored there, including their protection against accidental loss, destruction or damage and disclosure to unauthorized persons;

b) appropriate technical and organizational measures to ensure regular testing, measurement and evaluation of the

effectiveness of technical and organizational measures to ensure the security of processing, which resulted in a violation of the principle of data confidentiality and the principle of accountability;

1. imposes the Disciplinary Prosecutor of the Bar Chamber in X. (X., ul. (...)) for violation of Art. 5 sec. 1 lit. f), art. 5 sec. 2, art. 25 sec. 1 and art. 32 sec. 1 and 2 of Regulation 2016/679, an administrative fine in the amount of PLN 23,580 (say: twenty-three thousand five hundred and eighty zlotys).2. orders the Disciplinary Prosecutor of the Bar Association in X. (X., ul.(...)) to adapt the processing operations to the provisions of Regulation 2016/679 by: a) implementing appropriate technical and organizational measures in order to minimize the risk of processing personal data using external data carriers, in particular resulting from accidental or unlawful destruction, loss, modification, unauthorized disclosure or unauthorized access to personal data sent, stored or otherwise processed using external data carriers, after prior risk analysis, taking into account the state of the art implementation cost, nature, scope, context and purposes of processing as well as the risk of violating the rights or freedoms of natural persons, including risks related to the processing of personal data using external data carriers, taking into account theft and loss of these carriers, b) implementation of appropriate technical and organizational in order to ensure regular testing, measurement and evaluation of the effectiveness of technical and organizational measures to ensure the security of processing, within 6 months from the date of delivery of this decision

Justification

The Disciplinary Spokesman of the Bar Association in X. (X., ul. (...)), hereinafter also referred to as the Administrator, on (...) June 2021, notified the President of the Office for Personal Data Protection (hereinafter also referred to as "President of the Personal Data Protection Office") a breach of protection personal data that has been registered under the signature (…). In the notification of a breach of personal data protection, the Administrator indicated that (...) on May 2021, the defender of the defendant in the disciplinary proceedings conducted before the Disciplinary Prosecutor of the Bar Association in October reported to the Administrator's office. The defender informed the Administrator's employees about the receipt of a damaged parcel in which, contrary to the letter the guidebook lacked an attachment in the form of an external data carrier (flash drive). The medium contained a recording of a divorce hearing with personal data of 8 people in terms of name, surname, details of family life, relations between the parties and suspicions of marital infidelity.

In connection with the above-mentioned by reporting a breach, in a letter of (...) March 2022, the President of the Office for Personal Data Protection asked the Administrator to submit additional explanations regarding whether the external data carrier

(pen drive) being the subject of the breach was encrypted in accordance with the procedures for which referred to by the administrator in point 9A of the infringement notification form of (...) June 2021, i.e. "encryption, passwording of files containing personal data". In the response of (...) March 2022, the administrator indicated that the medium in question was not encrypted.

On (...) April 2022, the local Office requested the Administrator to:

Indication whether, before the breach, the Administrator had an implemented procedure for managing external data carriers in terms of their protection and proceedings in the event of destruction or theft.

Indication of technical and organizational security measures used so far to secure external data carriers.

Indication whether a risk analysis was carried out for the processing of personal data via external data carriers.

Indication whether the file with the recording on the lost external data carrier was secured (e.g. with a password or encryption mechanism), since the medium itself did not have appropriate security measures.

In response to the above summons, the Administrator, in the letter of .... April 2022, informed that:

The Disciplinary Prosecutor, as a body of the Bar Association, has a common IT infrastructure with the District Bar Council in X. In this respect, the Instruction (...) adopted by the Administrator on (...) August 2019, which describes the principles of media security (implemented before the event), is in force data. In addition, the Administrator has implemented a Policy (…) specifying the principles of personal data protection resulting from Regulation 2016/679 and procedures, such as the procedure for reporting personal data breaches.

A risk assessment was carried out in connection with the processing of personal data on external data carriers. The Administrator indicated (...) January 2021 as the date of its implementation. As an attachment to this letter, the Administrator posted the Procedure (...) together with the results of the assessment carried out before the start of processing. The conducted analysis takes into account the risk of destruction, theft and loss of data carriers on which processing takes place. In addition, the Administrator indicated that the risk assessment for the processing of personal data was scheduled to be repeated in June 2022. A risk analysis was also carried out in connection with the breach, but contrary to the information contained in the letter, it was not attached to the correspondence.

The file on the lost medium, just like the medium, has not been encrypted.

At the same time, the Administrator, referring to the question related to securing the external data carrier on which the video file with the recording of the divorce hearing was located, noted that the carrier belonged to the defender accused in the

proceedings before the Disciplinary Prosecutor of the Bar Chamber in X. The data carrier was delivered to the Office of the Defender of the Disciplinary Chamber of the Bar Association in X. in order to provide access to the recording of the hearing provided by one of the persons participating in the hearing.

In connection with the reported violation of personal data protection and the explanations provided by the Administrator of the above-mentioned by letters, the President of the Office for Personal Data Protection on (...) May 2022 initiated administrative proceedings ex officio regarding the possible violation by the Disciplinary Prosecutor of the Bar Chamber in X., as the data controller, of the obligations under Art. 5 sec. 1 lit. f), art. 5 sec. 2, art. 24 sec. 1, art. 25 sec. 1, art. 32 sec. 1 and 2 of Regulation 2016/679, in connection with the violation of the protection of personal data of persons whose data was on the recording of the divorce hearing, placed on a lost external data carrier (sign. no. DKN.5131.31.2022.).

At the same time, due to the Administrator's failure to attach all attachments to the letter of ... April 2022, on ... June 2022, the President of the UODO requested the submission of the missing documents in the form of the Instruction ... adopted by the Administrator on (…) of August 2019 and the risk analysis carried out in connection with the infringement. On (...) June 2022, the administrator submitted the requested documents to the local Office.

In addition, in connection with the information contained in the Administrator's letter of ... April 2022 about the planned re-performance of the risk analysis in connection with the processing of personal data, the supervisory authority on ... August 2022 asked the Disciplinary Spokesman of the Bar Association in X with a request to provide the results of this analysis, and in a letter of (...) January 2023 for information whether the Administrator verified compliance by its employees with the procedures contained in the Instruction (...) (including those regarding the shipment of data carriers) along with an indication how and when the last such verification was carried out before the personal data protection breach occurred, and whether the effectiveness of these procedures was verified as part of regular testing of the adopted technical and organizational security measures. The administrator provided the analysis in question as an attachment to the letter of (...) October 2022. In turn, in the letter of (...) January 2023, he indicated that "(...) the last verification of employees' compliance with the procedures contained in the Instruction (...), including those regarding the shipment of data carriers, prior to the personal data breach in question, took place during a regular check, scheduled for (...) January 2021, based on the risk analysis procedure, in particular sec. (...) (attached in its entirety to the letter of (...) April 2022 and to the letter of (...) June 2022)".

In this factual state, after reviewing all the evidence collected in the case, the President of the Office for Personal Data

Protection considered the following:

In accordance with art. 39 point 3a) of the Act of 26 May 1982 Law on the Bar (Journal of Laws of 2022, item 1184, as amended), the disciplinary spokesman is a body of the bar chamber. Pursuant to Art. 51a sec. 1 of the Law on the Bar, the scope of activity of the disciplinary spokesman includes activities in disciplinary proceedings, specified in the act and regulations issued on its basis. Based on Article. 58 point 5a and point 12 let. i) of the Law on the Bar, the Polish Bar Council, by resolution No. 50/2018 of November 24, 2018, adopted the Rules of Procedure for Disciplinary Spokesmen and Deputy Disciplinary Spokesmen, as well as the mode and manner of their selection. Pursuant to § 4 sec. 1 above-mentioned of the regulations, the scope of activity of the disciplinary spokesman of the Bar Chamber includes procedural activities in disciplinary proceedings in cases that concern members of the Bar Chamber that selected the disciplinary spokesman of the Bar Chamber, excluding matters falling within the scope of activity of the Disciplinary Spokesman of the Bar and cases taken over by the Disciplinary Spokesman of the Bar or transferred to conducted by the Disciplinary Ombudsman of the Bar. Pursuant to § 11 sec. 1 of the aforementioned regulations, the disciplinary ombudsman conducts the proceedings ex officio. In turn, pursuant to § 41 section 1 of the indicated regulations, the disciplinary ombudsman runs a law firm, the financing of which is provided by the relevant bar council. In the office of the disciplinary prosecutor, in accordance with § 41 sec. 2 lit. a) above of the Rules, files of disciplinary investigations are maintained. In connection with the above provisions, it should be considered that the Disciplinary Spokesman of the Bar Chamber in X. is the administrator, within the meaning of Art. 4 item 7 of Regulation 2016/679, data processed in connection with disciplinary proceedings conducted by him.

Pursuant to Art. 34 of the Act of May 10, 2018 on the Protection of Personal Data (Journal of Laws of 2019, item 1781) - hereinafter referred to as: the Act of May 10, 2018, the President of the UODO is the competent authority on data protection and the supervisory authority within the meaning of Regulation 2016/679. Pursuant to Art. 57 sec. 1 lit. (a) and (h) of Regulation 2016/679, without prejudice to other tasks defined under that Regulation, each supervisory authority in its territory monitors and enforces the application of this Regulation and conducts proceedings for infringements of this Regulation, including on the basis of information received from another supervisory authority or other public authority.

Article 5 of Regulation 2016/679 sets out the rules for the processing of personal data that must be respected by all administrators, i.e. entities that individually or jointly with others determine the purposes and methods of personal data processing. In accordance with art. 5 sec. 1 lit. f) of Regulation 2016/679, personal data must be processed in a manner that

ensures adequate security of personal data, including protection against unauthorized or unlawful processing and accidental loss, destruction or damage, using appropriate technical or organizational measures ("confidentiality and "). Pursuant to Art. 5 sec. 2 of Regulation 2016/679, the administrator is responsible for compliance with the provisions of para. 1 and must be able to demonstrate compliance with them ("accountability"). Specification of the confidentiality principle referred to in art. 5 sec. 1 lit. f) of Regulation 2016/679 are further provisions of this regulation, including art. 24 sec. 1 of Regulation 2016/679, which indicates that, 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 with different probabilities and severity, the administrator implements appropriate technical and organizational measures to ensure that the processing takes place in accordance with Regulation 2016/ 679 and to be able to prove it. These measures are reviewed and updated if necessary. As follows from art. 24 sec. 1 of Regulation 2016/679, the nature, scope, context and purposes of processing as well as the risk of violating the rights or freedoms of natural persons with different probabilities and severity are factors that the controller is obliged to take into account in the process of building a data protection system, also in particular from the point of view of other obligations indicated in art. 25 sec. 1, art. 32 sec. 1 or Art. 32 sec. 2 of Regulation 2016/679. The indicated provisions specify the confidentiality principle specified in art. 5 sec. 1 lit. f) of Regulation 2016/679, and compliance with this principle is necessary for the proper implementation of the accountability principle resulting from art. 5 sec. 2 of Regulation 2016/679.

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

From the content of art. 32 sec. 1 of Regulation 2016/679 shows that the administrator is obliged to apply technical and organizational measures corresponding to the risk of violating the rights and freedoms of natural persons with different probability of occurrence and severity of the threat. The provision specifies that when deciding on technical and organizational measures, the state of technical knowledge, the cost of implementation, the nature, scope, context and purposes of processing

as well as the risk of violating the rights or freedoms of natural persons with different probability and severity should be taken into account. The quoted provision shows that the determination of appropriate technical and organizational measures is a two-stage process. First of all, it is important to determine the level of risk associated with the processing of personal data, taking into account the criteria indicated in art. 32 sec. 1 of Regulation 2016/679, and then it should be determined what technical and organizational measures will be appropriate to ensure a level of security corresponding to this risk. These arrangements, where applicable, should include measures such as pseudonymisation and encryption of personal data, the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services, the ability to quickly restore the availability and access to personal data in the event of a physical incident or technical and regularly testing, measuring and assessing the effectiveness of technical and organizational measures to ensure the security of processing. Pursuant to art. 32 sec. 2 of Regulation 2016/679, when assessing whether the level of security is appropriate, the administrator takes into account in particular the risk related to processing, in particular resulting from accidental or unlawful destruction, loss, modification, unauthorized disclosure or unauthorized access to personal data sent, stored or otherwise processed.

Taking into account, in particular, the scope of personal data processed by the Administrator, contained in a file on a stolen (lost) external data carrier, in order to properly fulfill the obligations imposed on the above. the provisions of Regulation 2016/679, the Administrator was obliged to take action to ensure an appropriate level of data protection by implementing appropriate technical and organizational measures to ensure the security of personal data being processed. The nature and type of these activities should result from the risk analysis carried out, in which vulnerabilities related to the resources used and the resulting threats should be identified, and then adequate security measures should be defined. Incorrect estimation of the level of risk makes it impossible to apply appropriate security measures for a given resource and increases the probability of its occurrence. The result of the above was the materialization of the risk, as a result of which the unauthorized person (s) gained access to the data contained in the file located on the stolen (lost) external data carrier.

It should be pointed out that Regulation 2016/679 introduced an approach in which risk management is the foundation of activities related to the protection of personal data. Risk management is a continuous process that forces the data controller not only to ensure compliance with the provisions of Regulation 2016/679 through a one-time implementation of organizational and technical security measures, but also to ensure continuous monitoring of the level of threats and ensure accountability in

terms of the level and adequacy of the introduced security measures. In view of the above, it becomes necessary to be able to prove to the supervisory authority that the solutions introduced to ensure the security of personal data are adequate to the level of risk, as well as take into account the nature of the organization and the mechanisms used for processing personal data. Therefore, the administrator is to independently conduct a detailed analysis of the data processing processes carried out and perform a risk assessment, and then apply measures and procedures that will be adequate to the assessed risk. The consequence of this approach is the need to independently select security measures based on a threat analysis. The administrators are not provided with specific security measures and procedures. Conducting a detailed analysis of the conducted data processing processes and carrying out a risk assessment is the responsibility of the Administrator, who then, based on such an analysis, should apply measures and procedures that will be adequate to the assessed risk.

In view of the above, a properly conducted risk assessment provides the administrator with the opportunity to define and introduce technical and organizational measures that will eliminate or at least significantly reduce the established level of risk of materialization of identified threats to the processed personal data. The risk assessment carried out by the administrator should be documented and justified by the facts existing at the time of its implementation. The main factors contributing to the correct assessment that should be taken into account when conducting the analysis are the characteristics of the processing processes taking place, assets, vulnerabilities, threats and current security measures. It should be remembered that factors such as the scope and nature of the personal data processed by the administrator are also important when assessing the risk, as they will determine the possible negative effects for a natural person at the time of a breach of the protection of his personal data.

The "Procedure (...)" attached by the Administrator to the letter of ... April 2022, together with the risk analysis sheet containing the risk assessment for data processing activities adopted by the administrator, carried out on [...] January 2021, raises many doubts . The sheet contains, among other things, a risk assessment in the event of a "failure, theft or loss of data carriers". The presented methodology assumes the determination of appropriate values for individual factors, which include: A. Probability of:a) occurrence of the eventb) exposurec) expected time for which the breach may occurB. Impact on assets: a) confidentiality b) integrity c) availability

The degree of risk for this category of processing is defined as "1", which after getting acquainted with the procedure means "acceptable risk, not requiring further action (taking minimizing measures)". In addition, the risk mitigation measures that were

indicated in the above risk assessment, i.e. "Data backups once a day. Fast recovery time” in the opinion of the President of the UODO are not adequate to the potential threats that the administrator has accepted for this processing process, and for which the assessment is carried out. When analyzing the preventive measures adopted by the administrator, it should be considered that data backups are a means of minimizing the effects of the loss of availability of data on a lost (stolen) external data carrier, but they do not minimize the risk of possible consequences in the event of access to the data carrier and processed with it the use of personal data by a third party and its use, i.e. situations in which data confidentiality is breached. It should be emphasized that the protection of data on external data carriers, in order to effectively counteract the threat of "lost data carriers", must focus on the proper protection of data on such carriers against unauthorized access by third parties in the event of loss of such a carrier as a result of theft or loss. Meanwhile, the Administrator, carrying out the above-mentioned risk assessment, in the opinion of the President of the UODO, focused only on determining the actions to minimize the effects only in the event of a media failure, i.e. a violation of data availability, completely ignoring actions to minimize the consequences of a violation of their confidentiality. At this point, reference should therefore be made to the judgment of the Provincial Administrative Court in Warsaw of August 26, 2020, file ref. II SA/Wa 2826/19, in the justification of which the Court stated that "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 the risk associated with the processing of such personal data should also be taken into account, which risk may be of different levels. (...) The adopted measures are to be effective, in specific cases, some measures will have to be measures of a low-risk nature, others - must eliminate high risk, but it is important that all measures (and each one separately) are adequate and proportionate to the degree of risk."

The security measures adopted by the Administrator to minimize the effects of the threat described in the conducted analysis of the risk of "failure, theft or loss of data carriers" are therefore not adequate to the identified risk related to processing, and this leads to the conclusion that the risk assessment in connection with data processing on external data carriers was carried out with the adoption of incorrect values related to the risk of theft or loss of such carriers or their complete omission. The above is also supported by the fact that in the risk analysis provided by the Administrator on (...) October 2022, which was carried out after the breach of personal data protection, the impact assessment for the processing of personal data on external

data carriers in the event of "failure, theft, or loss of data carriers" has been replaced only with an impact assessment in the event of "data carrier failure". Therefore, the Administrator failed to carry out a risk analysis for the situation that resulted in a personal data breach reported to the President of the UODO, which should be considered inconsistent with the above-mentioned provisions of Regulation 2016/679, in particular in a situation where the Administrator provides for the possibility of further processing of personal data on external media data, and the event in question directly indicates what consequences may occur in the event of their loss or theft.

It should be noted, however, that despite the fact that in the risk analysis carried out, the Administrator did not specify security measures to minimize the risk of theft or loss of external data carriers, but in practice he introduced certain solutions focusing on the security of this category of personal data processing. These solutions are included in the "Instruction (...)" (hereinafter: I (...)), introduced on (...) August 2019, which includes a chapter on the security of information carriers. It was indicated there that the person who is currently the user of such a medium is responsible for ensuring the security of external data carriers. In the notification of a breach of personal data protection, the Administrator indicated "(...) that the employees of the disciplinary prosecutor's office, when packing the parcel containing the USB flash drive with the recording, took a number of steps to secure this medium, e.g. the carrier was placed in a plastic sleeve, which was tightly sewn, several people checked the tightness of this sleeve, the sleeve was sewn to the cover letter in a way that prevented the carrier from falling out without breaking the above-mentioned protection or foil (plastic sleeve). The letter together with the T-shirt was placed in an envelope, which was sealed and sent via X. S.A. (...)". The collected material shows that the employees of the Office of the Disciplinary Prosecutor of the Bar Association in X took steps to secure the medium in question, but they were not in accordance with the procedure contained in I (...). The procedure "Method, place and period of storage of electronic information carriers" resulting from this document defines the procedure in the case of using external data carriers, such as hard drives, CDs, DVDs and pen drives, and clearly indicates that in the case of transferring media, on which personal data are contained, "(...). In the response given by the Administrator on (...) March 2022, the President of the UODO received information that "(...) the medium in question was not encrypted (...)". In turn, in the letter of (...) April 2022, the administrator stated that "(...) in response to the question regarding whether the file with the recording on an external data carrier was secured with a password or encryption mechanism, I indicate that the the file was not secured in this way (...)". The findings made in this regard clearly show that neither the file with personal data nor the data carrier itself has been secured in any way, which resulted in a very high

probability of unauthorized persons gaining access to personal data on this medium in the event of loss of the shipment In addition, the above-mentioned the procedure provides for the use of deposit envelopes, which are commonly used to increase the security of the content being sent, including documents containing personal data, due to the fact that visible signs appear in the event of tampering with the packaging (once opened, the packaging cannot be sealed again). The above explanations of the Administrator indicate that the deposit envelope was replaced with a plastic sleeve tightly sewn with staples, which was then attached to the cover letter and placed in an ordinary envelope. The shipment prepared in this way was sent via X. S.A. despite the clear entry in I(...) that "(...)". The Administrator's employees did not comply with the provisions of I (...), including the point indicating that "(...) persons using information carriers should be aware of the risks and are obliged to exercise due diligence by applying applicable organizational, technical and legal measures described in AND(…)(…)". It should be noted that the mere introduction of provisions regarding the use of organizational and technical measures in I (...) does not release the Administrator from verifying whether the security measures adopted in this way limit or completely eliminate the risks associated with data processing using external data carriers, including the risk of loss confidentiality of data as a result of theft or loss of such a medium. This verification should first take place as part of the risk analysis, which in the case of the Disciplinary Prosecutor of the Bar Chamber in X, as shown above, was carried out incorrectly, and then as part of regular testing, measuring and assessing the effectiveness of the organizational and technical measures used to ensure safety processed personal data.

In a letter of (...) April 2022, the Disciplinary Prosecutor of the Bar Chamber in X. indicated that "(...) the flash drive on which the recording was located and which was lost was the property of the defender accused in the proceedings before the Disciplinary Prosecutor of the Bar Chamber in X. (…)". In connection with the above-mentioned statement, it should be noted that the data on the lost external data carrier are the subject of protection for which the Administrator is responsible. Thus, even assuming that this medium was not the property of the Administrator, and therefore it may not have been able to properly secure it, the Disciplinary Spokesperson of the Bar Association in X. should have secured the file that was to be uploaded to the medium, which was, moreover, his duty to own procedure in I (...), which he did not do. Attention should also be paid to the judgment of the Provincial Administrative Court in Warsaw of January 19, 2021, file ref. II SA/Wa 702/20, in the justification of which it was stated that "(...) the data controller should adequately protect personal data against their accidental loss by means of appropriate technical and organizational measures. Personal data should be processed in a manner that ensures their

appropriate security and appropriate confidentiality, including protection against unauthorized access to them and the equipment used for their processing, and against unauthorized use of these data and equipment (recital 39 of Regulation 2016/679)" .

In connection with the above findings, it should be pointed out that the Disciplinary Spokesman of the Bar Association in X., at the time of the breach of personal data protection, despite the lack of defining security measures to minimize the risk of loss of data confidentiality as a result of theft or loss of an external data carrier due to an incorrectly carried out on (…) January 2021 risk analysis, was in possession of procedures for the security of data processed using this type of media, including the transfer of external data media containing personal data to third parties outside the Administrator's office. However, there are doubts about the effectiveness of the implementation of the above-mentioned procedures due to the failure to apply their provisions by law firm employees when sending an external data carrier with the recording of a divorce hearing, which led to a violation of personal data protection. As indicated by the Administrator in the letter of (...) January 2023, "the last verification of employees' compliance with the procedures contained in the Instructions (...), including those regarding the shipment of data carriers, prior to the breach of personal data protection in question, took place during a regular, scheduled for (...) of January 2021, checks based on the risk analysis procedure, in particular sec. 10" and "regularly tested and verified the effectiveness of the adopted procedures in accordance with the planned and organized as well as documented activities in specific time intervals, regardless of the course of data processing, in accordance with the implemented personal data protection documentation". However, the collected evidence shows that the verification of the adopted procedures carried out by the Administrator, contrary to his claims, was not effective, taking into account the fact that the employees of the office of the Disciplinary Spokesman of the Bar Association in X. did not comply with the provisions of I (...) when sending an external data carrier that was lost , which (as a result of the lack of protection of the file with the recording of the divorce hearing on this medium) led to a breach of personal data protection. In addition, the section (...) of the procedure (...) indicated by the Administrator states that "(...). Despite a clear indication to provide explanations in this regard and evidence to confirm them in the letter sent by the supervisory authority to the Administrator on (...) January 2023, the Disciplinary Spokesman of the Bar Chamber in X. did not provide any evidence in the form of a written report confirming the monitoring of procedures in force in his organization, and only declared the existence of procedures for regular testing of security measures. This means that the Administrator, contrary to the obligation arising from art. 5 sec. 2 of Regulation 2016/679 has not demonstrated that in this

respect it fulfills the obligations arising from the provisions of Regulation 2016/679.

It needs to be emphasized that regular testing, measuring and assessing the effectiveness of technical and organizational measures to ensure the security of processing is the basic obligation of each administrator under art. 32 sec. 1 lit. d) Regulation 2016/679. The administrator is therefore obliged to verify both the selection and the level of effectiveness of the technical measures used at each stage of processing. The comprehensiveness of this verification should be assessed through the prism of adequacy to the risks and proportionality in relation to the state of technical knowledge, implementation costs and the nature, scope, context and purposes of processing. However, in the present facts, it should be considered that the Administrator did not duly fulfill the obligation imposed on him to regularly test, measure and evaluate the effectiveness of technical and organizational measures to ensure the security of personal data processing. As it has been shown above, the Administrator did not monitor the effectiveness of the procedures introduced under I (...), regarding the duties of employees of the office of the Disciplinary Spokesman of the Bar Association in X. related to securing personal data on the external data carrier sent. Doubts may also be raised by the period resulting from point (...) of the procedure (...), the period at which such reviews should be carried out, in the case of such an organization as the Disciplinary Spokesman of the Bar Chamber in X. As indicated in this point "At least once a year (and in the case of modifications or planned modifications in the processing of personal data), a risk review should be carried out in accordance with the above-mentioned points." The adoption of such a period may result in the use of a measure (technical or organizational) that has ceased to be effective, i.e. one that has already ceased to ensure security for the processed personal data, regardless of the reasons for the loss of this effectiveness. As a side note, it should also be noted that the terminology adopted in point (...) of the procedure (...) and the description of individual actions to be performed as part of the review suggest a description of risk management, including the dates for conducting a risk analysis for personal data processing operations, rather than a description actions to be taken as part of regular testing, evaluating and measuring the effectiveness of technical and organizational measures to ensure the security of data processing. Meanwhile, the indicated testing, measuring and evaluating, so that it constitutes the implementation of the requirement arising from Art. 32 sec. 1 lit. d) of Regulation 2016/679, must be carried out on a regular basis, which means conscious planning and organization, as well as documenting (in connection with the accountability principle referred to in Article 5(2) of Regulation 2016/679) of this type of activities in specified time intervals, regardless of changes in the organization and course of data processing processes caused, for example, by an organizational change at the data controller

or a change in the legal environment.

In order to prove that the employees of the office of the Disciplinary Spokesman of the Bar Association in X. the above-mentioned procedures were verified The Administrator in the letter of (...) January 2023 informed that "In addition, the Administrator regularly trained employees of the Disciplinary Prosecutor's Office (May 2020) in the scope of procedures contained in the documentation of processing and protection of personal data in force at the Disciplinary Prosecutor of the Bar Association in October and (August 2020) in the scope of personal data breaches, their types and procedures for reporting them". From the above The explanations show that the training on the procedures specified in I (...) took place in May 2020, i.e. a year before the finding of a personal data breach consisting in the loss of an unsecured external data carrier with an unsecured file with the recording of a divorce hearing containing personal data, which took place on (...) May 2021. It should therefore be emphasized that the training is conducted only on the date indicated in the above-mentioned in the Administrator's letter is not a sufficient means of influencing the awareness of persons obliged to protect personal data and to apply procedures specifying security measures for such data. Properly conducted training will allow the trainees to properly understand the principles of personal data processing specified by the Administrator, and consequently contribute to reducing the risk of violations in this area. It should also be pointed out that conducting training in the field of personal data protection, in order to be considered an adequate security measure, must be carried out in a cyclical manner, which will ensure constant reminder and, consequently, consolidation of the principles of personal data processing covered by the training. In addition, all persons authorized to process personal data must participate in such training, and the training itself must cover all issues related to the processing of personal data within the agreed training topic. Omitting one of these elements will result in the training not fulfilling its role, because some people will not be trained at all or the training participants will not receive full knowledge in a given area. The consequence of the above may be a violation of the protection of personal data, as in the case being the subject of these proceedings. Moreover, the lack of training in the manner described above means that this security measure in practice does not reduce the risk of personal data breaches, which undoubtedly contributes to the weakening of the level of personal data protection and determines the need to recognize a violation of the provisions of Regulation 2016/679 relating to administrator's obligations in the field of data security.

In the light of the identified irregularities in the risk analysis, the selection of measures to ensure the security of personal data processed using external data carriers and the lack of documented regular testing, measurement and assessment of the

effectiveness of technical and organizational measures to ensure the security of processing, it should be considered that the Disciplinary Spokesman of the Bar Chamber in X violated the principle of data confidentiality (Article 5(1)(f) of Regulation 2016/679) in connection with the violation of the controller's obligations when implementing technical and organizational measures to ensure that the processing was carried out in accordance with Regulation 2016/679 (Article 24(1)(f) of Regulation 2016/679) 1 of Regulation 2016/679), in order to provide the processing with the necessary safeguards (Article 25(1) of Regulation 2016/679) and to ensure a level of security corresponding to the risk, including the ability to ensure confidentiality at all times (Article 32(1) of Regulation 2016/679) 679) and the obligation to take into account the risk of processing, resulting from unauthorized access to the personal data being processed, when assessing whether the level of security is appropriate (Art. 32 sec. 2 of Regulation 2016/679). Violation of the confidentiality principle expressed in art. 5 sec. 1 lit. f) of Regulation 2016/679 is related to the violation of the accountability principle referred to in art. 5 sec. 2 of Regulation 2016/679. As pointed out by the Provincial Administrative Court in Warsaw in the judgment of February 10, 2021, file ref. II SA/Wa 2378/20, "The accountability principle is therefore based on the legal responsibility of the controller for the proper fulfillment of duties and imposes on him the obligation to demonstrate, both to the supervisory authority and to the data subject, evidence of compliance with all data processing rules." Similarly, the issue of the accountability principle of the Provincial Administrative Court in Warsaw is interpreted in the judgment of August 26, 2020, file ref. II SA/Wa 2826/19, "Taking into account all the standards of Regulation 2016/679, it should be emphasized that the administrator has considerable freedom in terms of the security measures used, but at the same time is responsible for violating the provisions on the protection of personal data. The principle of accountability directly implies that it is the data controller who should demonstrate, and thus prove, that he complies with the provisions set out in Art. 5 sec. 1 of Regulation 2016/679".

Considering the above irregularities, as well as the content of Art. 58 sec. 2 lit. d) of Regulation 2016/679, the President of the UODO ordered the Administrator to adapt the processing operations to the provisions of Regulation 2016/679 by performing a risk analysis taking into account the risks associated with the loss or theft of external data carriers on which personal data are processed, as well as implementing appropriate technical measures and organizational in order to ensure regular testing, measurement and evaluation of the effectiveness of technical and organizational measures to ensure the security of processing.

When assessing the circumstances of the breach of personal data protection in question, it should be emphasized that 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 rights to the protection of personal data and that the protection of individuals in connection with the processing of personal data is one of the fundamental rights (first sentence of recital 1 of the preamble). In case of any doubts, e.g. as to the performance of duties by administrators - not only in a situation where personal data protection has been breached, but also when developing technical and organizational security measures to prevent them - these values should be taken into account in the first place.

Taking into account the above findings and the identified violations of the provisions of Regulation 2016/679, the President of the UODO, using the power vested in him specified in art. 58 sec. 2 lit. i) of Regulation 2016/679, according to which each supervisory authority has the power to apply, in addition to or instead of other corrective measures provided for in art. 58 sec. 2 lit. a)-h) and point. j) of this Regulation, an administrative fine under Art. 83 sec. 4 lit. a) and sec. 5 lit. a) of Regulation 2016/679, taking into account the circumstances established in the proceedings in question, stated that in the case under consideration there were premises justifying the imposition of an administrative fine on the Administrator.

In accordance with art. 83 sec. 4 lit. a) of Regulation 2016/679, violation of the provisions on the obligations of the administrator and the processing entity referred to in art. 8, 11, 25-39 as well as 42 and 43 are subject to sec. 2, 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 applicable.

In accordance with art. 83 sec. 5 lit. a) of Regulation 2016/679, violation of the provisions on the basic principles of processing, including the conditions of consent, referred to in art. 5, 6, 7 and 9 are subject to, in accordance with sec. 2, an administrative fine of up to EUR 20,000,000, and in the case of an enterprise - up to 4% of its total annual worldwide turnover from the previous financial year, with the higher amount applicable.

Article 83 sec. 3 of Regulation 2016/679, on the other hand, provides that if the controller or processor intentionally or unintentionally violates several provisions of this regulation as part of the same or related processing operations, the total amount of the administrative fine does not exceed the amount of the penalty for the most serious infringement.

In this case, an administrative fine against the Administrator was imposed for violation of Art. 25 sec. 1 and art. 32 sec. 1 and 2 of Regulation 2016/679 on the basis of the above-mentioned art. 83 sec. 4 lit. a) of Regulation 2016/679, while for violation of Art. 5 sec. 1 lit. f) and art. 5 sec. 2 of Regulation 2016/679 - pursuant to art. 83 sec. 5 lit. (a) of this Regulation. At the same

time, an administrative fine of PLN 28,296 (in words: twenty-eight thousand two hundred and ninety-six zlotys) imposed on the Administrator jointly for violating all of the above provisions - pursuant to the provision of art. 83 sec. 3 of Regulation 2016/679 - does not exceed the amount of the fine for the most serious violation found in this case, i.e. violation of Art. 5 sec. 1 lit. f) and art. 5 sec. 2 of Regulation 2016/679, which, pursuant to Art. 83 sec. 5 lit. a) of Regulation 2016/679 is subject to an administrative fine of up to EUR 20,000,000, and in the case of an enterprise - up to 4% of its total annual worldwide turnover from the previous financial year.

When deciding to impose an administrative fine, the President of the UODO - pursuant to art. 83 sec. 2 lit. a) - k) of Regulation 2016/679 - took into account the following circumstances of the case, which make it necessary to apply this type of sanction in this case and have an aggravating effect on the amount of the imposed administrative fine:

1. The nature, gravity and duration of the infringement, taking into account the nature, scope or purpose of the given processing, the number of data subjects affected and the extent of the damage suffered by them (Article 83(2)(a) of Regulation 2016/679). in this case, the violation of the provisions on the protection of personal data, which resulted in the possibility of obtaining unauthorized access to the data contained in the file with the recording of the divorce hearing, placed on a lost external data carrier, by an unauthorized person or persons (violation of the confidentiality principle), is of considerable importance and nature, as it poses a high risk of negative effects for at least 8 data subjects. The violation by the Disciplinary Prosecutor of the Bar Association in X. of the obligations to apply measures to protect the processed data against disclosure to unauthorized persons, entails not only the potential, but also the real possibility of using these data by third parties without the knowledge and against the will of the data subjects, contrary to with the provisions of Regulation 2016/679. In addition, until this decision is issued, the missing external data carrier has not been found, so an unauthorized person or persons may still have access to personal data on this medium. It should also be emphasized the long duration of the violation of the provisions on the protection of personal data, i.e. from (...) January 2021, when the Administrator conducted the risk analysis incorrectly, as shown above, until now.

In the present case, there is no evidence that persons whose data could be accessed by an unauthorized person or persons suffered material damage. Nevertheless, the mere breach of confidentiality of their data constitutes non-pecuniary damage (harm) to them; natural persons whose data were obtained in an unauthorized manner may at least feel fear of losing control over their personal data, discrimination or violating their reputation. It should also be pointed out that, in accordance with

Resolution No. 50/2018 of the Polish Bar Council of November 24, 20218, the Rules of Procedure for Disciplinary Spokesmen and Deputy Disciplinary Spokesmen and the mode and manner of their selection, correspondence in disciplinary matters is confidential, and the Disciplinary Spokesman of the Chamber of the Adwokacka St. in X. is covered by attorney's secrecy in the scope of proceedings conducted by him.

2. Intentional or unintentional nature of the infringement (Article 83(2)(b) of Regulation 2016/679). Unauthorized access to personal data of persons whose data is included in the recording of a divorce hearing on a lost external data carrier became possible as a result of failure to exercise due diligence by the Disciplinary Prosecutor of the Bar Association in X. In the opinion of the supervisory body, this constitutes an unintentional nature of the infringement, resulting from the Administrator's negligence, because the Disciplinary Prosecutor of the Bar Chamber in X., despite an incorrectly conducted risk analysis, had an implemented procedure for sending external data carriers along with specifying organizational measures guaranteeing, in the Administrator's opinion, an appropriate level of security of data processed using these media. Despite its development, the Administrator's employees did not comply with its provisions regulating the actions to be taken to ensure the security of data sent on an external data carrier. This calls into question the effectiveness of employee training conducted by the Administrator in this regard and periodic verification of compliance with the provisions of these procedures.

3. Categories of personal data affected by the breach (Article 83(2)(g) of Regulation 2016/679). Personal data on a lost external data carrier, i.e. name and surname, voice, details of family life, the parties' relationship and suspicions of marital infidelity, as a rule, are not considered to belong to special categories of personal data, however, the context of the nature of the event under which they were recorded in the form of a recording, i.e. a divorce hearing, may determine that they will be subject to such protection as personal data of special categories, and as a consequence, it will be associated with a high risk of violating the rights or freedoms of natural persons affected by the breach. This is also evidenced by the risk level adopted by the Administrator, which in point 8B of the personal data breach notification form indicated that the breach causes a high risk of violating the rights or freedoms of natural persons. In view of the above, the occurrence of non-pecuniary damage (harm) cannot be ruled out, as natural persons whose data were stored on this medium may feel fear of losing control over their personal data, discrimination, as well as violating their reputation.

When determining the amount of the administrative fine, the President of the Personal Data Protection Office took into account as a mitigating circumstance having an impact on reducing the amount of the fine imposed the fact that when examining the

case, he did not notice circumstances other than those described above that could affect the assessment of the infringement and the amount of the adjudicated administrative fine [Article . 83 sec. 2 letter k) of Regulation 2016/679].

The fact that the President of the UODO applied sanctions in the form of an administrative fine in this case, as well as its amount, had no impact on the other ones indicated in art. 83 sec. 2 of Regulation 2016/679, circumstances:

1. Actions taken to minimize the damage suffered by data subjects (Article 83(2)(c) of Regulation 2016/679). Immediately after disclosing the breach of personal data protection, the Disciplinary Spokesman of the Bar Chamber in X. filed a complaint with the postal operator . The administrator also provided the data subjects with a correct notification of a data protection breach, together with an indication of how they can protect their personal data against further use. It should be noted, however, that notifying the data subjects of a breach of the protection of their personal data constitutes the fulfillment of the legal obligation under Art. 34 sec. 1 and 2 of Regulation 2016/679, and as provided for in the Wp Guidelines. 253 (with regard to the premise "the manner in which the supervisory authority found out about the infringement") "[simple] fulfillment of [...] the obligation by the Administrator cannot be interpreted as a weakening/mitigating factor".

2. The degree of responsibility of the administrator, taking into account the technical and organizational measures implemented by him pursuant to art. 25 and 32 (Article 83(2)(d) of Regulation 2016/679). Adopted on October 3, 2017, Guidelines of the Article 29 Data Protection Working Party on the application and determination of administrative fines for the purposes of Regulation No. 2016 /679 indicate that when considering this premise, "the supervisory authority must answer the question to what extent the controller "did everything that could be expected", given the nature, purposes or scope of processing and in the light of the obligations imposed on it by the regulation".

The President of the UODO stated in this case that the Disciplinary Prosecutor of the Bar Association in X. violated the provisions of art. 25 sec. 1 and art. 32 sec. 1 and 2 of Regulation 2016/679. In his opinion, the administrator bears a high degree of responsibility for failure to implement appropriate technical and organizational measures that would prevent a breach of personal data protection. It is obvious that in the considered context of the nature, purpose and scope of personal data processing, the Administrator did not "did everything that could be expected of him"; thus failed to comply with the provisions of Art. 25 and 32 of Regulation 2016/679 obligations.

In the present case, however, this circumstance determines the essence of the infringement itself; it is not merely a factor mitigating or aggravating its assessment. For this reason, the lack of appropriate technical and organizational measures

referred to in Art. 25 and art. 32 of Regulation 2016/679, cannot be considered by the President of the UODO in this case as a circumstance that may additionally affect the stricter assessment of the infringement and the amount of the administrative fine imposed on the Administrator.

3. Any relevant previous violations by the controller or processor (Article 83(2)(e) of Regulation 2016/679). therefore, there are no grounds for treating this circumstance as aggravating, however, it is the responsibility of each administrator to comply with the law (including the provisions on the protection of personal data), therefore the lack of previous violations of personal data protection cannot be considered a mitigating circumstance when imposing sanctions.

4. Degree of cooperation with the supervisory authority in order to remove the infringement and mitigate its possible negative effects (Article 83(2)(f) of Regulation 2016/679). The Disciplinary Spokesman of the Bar Chamber in X. correctly fulfilled his procedural obligations in during the administrative procedure, which ended with the issuance of this decision.

5. The manner in which the supervisory authority found out about the breach (Article 83(2)(h) of Regulation 2016/679). The President of the UODO found a breach as a result of reporting a personal data breach by the Disciplinary Spokesman of the Bar Association in X. By doing so, the Controller the notification only fulfilled the legal obligation incumbent on him, therefore there are no grounds to consider that this circumstance is a mitigating circumstance. According to the Guidelines on the application and determination of administrative fines for the purposes of Regulation No. 2016/679 (Wp. 253), "The supervisory authority may become aware of a violation as a result of proceedings, complaints, articles in the press, anonymous tips or notification by the data controller. Pursuant to the regulation, the controller is obliged to notify the supervisory authority of a breach of personal data protection. The mere fulfillment of this obligation by the controller cannot be interpreted as a mitigating factor.'

6. 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). Before issuing this decision, the President of the UODO did not apply any measures listed in Art. 58 sec. 2 of Regulation 2016/679, therefore the administrator was not required to take any action related to their application, and which actions, subject to the assessment of the President of the UODO, could have an aggravating or mitigating impact on the assessment of the infringement found.

7. Application of approved codes of conduct under Art. 40 of Regulation 2016/679 or approved certification mechanisms under Art. 42 of Regulation 2016/679 (Article 83(2)(j) of Regulation 2016/679). The Disciplinary Prosecutor of the Bar Chamber in X.

does not apply approved codes of conduct or approved certification mechanisms referred to in the provisions of Regulation 2016/679. However, their adoption, implementation and application is not - as provided for by the provisions of Regulation 2016/679 - mandatory for controllers and processors, therefore the circumstance of their non-application cannot be considered to the Administrator's disadvantage in this case. In favor of the Administrator, however, the circumstance of adopting and applying such instruments as measures guaranteeing a higher than standard level of protection of personal data being processed could be taken into account.

8. Financial benefits achieved directly or indirectly in connection with the infringement or losses avoided (Article 83(2)(k) of Regulation 2016/679). precipitate. Therefore, there are no grounds for treating this circumstance as incriminating the controller. The finding of measurable financial benefits resulting from the violation of the provisions of Regulation 2016/679 should be assessed definitely negatively. On the other hand, failure by the administrator to achieve such benefits, as a natural state, independent of the infringement and its effects, is a circumstance that, by nature, cannot be a mitigating factor for the Administrator. This is confirmed by the wording of Art. 83 sec. 2 lit. k) of Regulation 2016/679, which requires the supervisory authority to pay due attention to the benefits "achieved" - occurred on the part of the entity committing the infringement.

In the opinion of the President of the UODO, the applied administrative fine fulfills 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 UODO, the administrative fine imposed on the Disciplinary Prosecutor of the Bar Chamber in X. will be effective, as it will lead to a state in which the Disciplinary Prosecutor of the Bar Chamber in X. will apply such technical and organizational measures that will ensure a level of security for the processed data corresponding to the risk of violation of rights or freedom of the data subjects and the importance of the risks associated with the processing of such personal data. The effectiveness of the administrative fine is therefore equivalent to the guarantee that the Disciplinary Prosecutor of the Bar Chamber in October will, from the moment of completion of these proceedings, approach the requirements of the provisions on the protection of personal data with the utmost care.

The applied administrative fine is also proportional to the violation found, in particular its weight, effect, the circle of affected individuals and the very high risk of negative consequences that they incur in connection with the violation. In the opinion of the President of the UODO, the administrative fine imposed on the Disciplinary Prosecutor of the Bar Association in October will not be 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 authority to the degree of violation of the administrator's obligations, but on the other hand, it does not cause a situation where the necessity to pay it will have negative consequences in the form of a significant deterioration of the Administrator's financial situation . According to the President of UODO, the Disciplinary Prosecutor of the Bar Association in X. should and is able to bear the consequences of his negligence in the field of data protection, hence the imposition of an administrative fine of PLN 23,580 (in words: twenty-three thousand five hundred and eighty zlotys) is fully justified.

In the opinion of the President of the Office for Personal Data Protection, the administrative fine will fulfill a repressive function in these specific circumstances, as it will be a response to the violation by the Disciplinary Prosecutor of the Bar Chamber in X. of the provisions of Regulation 2016/679, but also a preventive one, as it will contribute to preventing future violation by the Disciplinary Prosecutor of the Bar Chamber in X. of the obligations arising from the provisions on the protection of personal data.

In the opinion of the President of the UODO, the applied administrative fine meets the conditions referred to in art. 83 sec. 1 of Regulation 2016/679, due to the importance of the violations 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.

Pursuant to the content of art. 103 of the Act of May 10, 2018 on the protection of personal data (Journal of Laws of 2019, item 1781), the equivalent of the amounts expressed in euros referred to in art. 83 of Regulation 2016/679, is calculated in PLN according to the average euro exchange rate announced by the National Bank of Poland in the table of exchange rates as at January 28 of each year, and if in a given year the National Bank of Poland does not publish the average euro exchange rate on January 28 - according to the average euro exchange rate announced in the exchange rate table of the National Bank of Poland, which is the closest after that date.

Considering the above, the President of the Personal Data Protection Office, pursuant to art. 83 sec. 4 lit. a) and art. 83 sec. 5 lit. a) in connection with art. 83 sec. 3 Regulation 2016/679 and in connection with Art. 103 of the Act of May 10, 20218 on the protection of personal data, for the violation described in the operative part of this decision, imposed on the Disciplinary Prosecutor of the Bar Chamber in October - using the average euro exchange rate of January 30, 2023 (EUR 1 = PLN 4.7160)) - an administrative fine in the amount of PLN 23,580 (equivalent to EUR 5,000).

The purpose of the imposed administrative fine is to ensure that the Disciplinary Prosecutor of the Bar Chamber in X. complies

with the provisions of Regulation 2016/679 in the future and, consequently, to conduct data processing in accordance with applicable law.

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

Print article

Metadata

Provider:

Inspection and Infringement Department

Produced information:

John Nowak

2023-04-20

Entered the information:

Wioletta Golanska

2023-05-17 15:16:09

Recently modified:

Edith Magziar

2023-05-18 12:54:59