Warsaw, 19

January

2023

Decision

DKN.5131.12.2020

Based on Article. 104 § 1 and art. 105 § 1 of the Act of June 14, 1960 Code of Administrative Procedure (Journal of Laws of 2022, item 2000, as amended), art. 7 sec. 1 and sec. 2, art. 60 and art. 102 sec. 1 item 1 i 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) in connection with art. 24 sec. 1, art. 25 sec. 1 and 2 and art. 32 sec. 1 and 2, as well as art. 83 sec. 5 lit. a) in connection with art. 5 sec. 1 lit. e) and f) and art. 5 sec. 2 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 of data) (OJ L 119 of 4.05.2016, p. 1, OJ L 127 of 23.05.2018, p. 2 and OJ L 74 of 4.03.2021, p. 35), after carrying out administrative proceedings initiated ex officio regarding the violation of the provisions on the protection of personal data by the District Court Szczecin-Centrum in Szczecin at ul. Kaszubska 42, President of the Office for Personal Data Protection

1) stating that the District Court Szczecin-Centrum in Szczecin violated the provisions of Art. 5 sec. 1 lit. f), art. 5 sec. 2, art. 24 sec. 1, art. 25 sec. 1 and 2 and art. 32 sec. 1 and 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 data protection) (Official Journal EU L 119 of 4.05.2016, 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), hereinafter referred to as Regulation 2016/679, consisting in the failure by the District Court of Szczecin-Centrum in Szczecin to implement appropriate technical and organizational measures ensuring a level of security corresponding to the risk of data processing using portable memory, which would prevent the 10th District Court of Szczecin-Centrum from recording The Center in Szczecin of personal data on two private and unsecured data carriers and, consequently, would avoid a breach of personal data protection, constituting a breach of confidentiality as a result of losing these carriers, imposes on the District Court Szczecin-Centrum with its registered office in Szczecin at ul. Kaszubska 42, for violation of Art. 5 sec. 1 lit. f), art. 5 sec.

2, art. 25 sec. 1 and 2 and art. 32 sec. 1 and 2 of Regulation 2016/679, an administrative fine of PLN 30,000 (say: thirty thousand zlotys 00/100),

2) discontinues the proceedings in the remaining scope.

JUSTIFICATION

The Personal Data Protection Office (…) of September 2020 received a preliminary notification of a personal data breach submitted by the District Court Szczecin-Centrum in Szczecin (hereinafter referred to as: the Court or the Administrator), registered under the reference number DKN (…), consisting in the loss by X three pendrives (one business - encrypted and two unencrypted - private), containing personal data of an undetermined number of people. On (…) September 2020, a supplementary notification was received. As indicated by the Administrator, the lost carriers contained personal data in the field of names and surnames, addresses of residence or stay, data regarding the workplace and data regarding health, contained in draft judgments and justifications prepared by X in the period from December 2004 to August 2020 r.

The President of the Office for Personal Data Protection, hereinafter also referred to as the President of the UODO, conducted explanatory proceedings regarding the reported infringement (registered under the reference number: DKN (…)), and then initiated ex officio on (…) December 2020 administrative proceedings (ref. no. : DKN.5131.12.2020) regarding the possible violation by the Court, as the data controller, in connection with the violation of the protection of personal data of persons participating in court proceedings, obligations under art. 5 sec. 1 lit. e) and ... f), art. 5 sec. 2, art. 24 sec. 1, art. 25 sec. 1 and 2 and art. 32 sec. 1 and 2 of Regulation 2016/679.

The President of the UODO, as a result of the explanatory proceedings regarding the reported breach of personal data protection and administrative proceedings, determined the following facts.

1. Lost data carriers (one business encrypted, two private unencrypted) contained draft judgments, justifications and orders that contained personal data in the field of names, surnames, addresses of residence or residence, information on health, information on workplaces and subjects of proceedings conducted by X during his employment at the Court, i.e. from December 2004 to August 2020. The administrator was unable to determine the amount of data or personal details of persons contained on the missing media, due to the fact that the infringer was unable to provide such information (cf. statement of the infringer of (...) September 2020, content of the notification).

2. The President of the UODO received explanations from the Court (letters of (...) October 2020, (...) January 2021 and (...)

May 2021), which show that the Court: 1) defined the rules for the processing of personal data using pen drives, while referring to point (...) of the Policy (...) of the Szczecin-Centrum District Court in Szczecin. Quote: "in order to protect the confidentiality of the transmitted and stored data, cryptographic security measures are used (...)2) as part of the steps taken to ensure the effectiveness of the implemented solutions, it successively equips employees with business data carriers such as flash drives with hardware encryption;3) the list of data carriers authorized by the IT Department of the Court includes the following information: department number, name and surname, name and model of the device, date, stamp and signature of the recipient;4) after the infringement occurred, the controller conducted an inventory of business carriers (until (...) October 2020) and blocks USB ports from October 2020 through the N software purchased in December 2019, thanks to which it is not possible to connect media other than media authorized by the IT Department of the Court (cf. § (...) Orders of the President of the District Court Szczecin - Centrum w Szczecin of September 2020, No. (…)/2020); 5) the use of private storage media was prohibited (the Administrator also referred to the content of § (…) of the Regulations (…), quoted: "[users are prohibited from: circumventing control mechanisms (e.g. using proXy servers), b) testing the implemented security measures, c) scanning network devices, servers and workstations in terms of examining the services provided, d) disabling programs that run automatically at system startup, e) uninstalling programs, f) connecting and using private equipment, including the use of private data carriers, g) making any attempts to interfere with the computer equipment, apart from activities related to daily operation").

3. The risk analysis submitted by the Court, conducted (...) in December 2019, shows that the data controller anticipated the risk of losing data confidentiality through "access to data by unauthorized persons due to: storage on unsecured removable media, storage of data/photos on private devices” by unauthorized persons. The primary risk was assessed at a medium level, with a value of "6". As a conclusion from the risk analysis, it was indicated that although the risk is at an average level, due to the security measures applied by the administrator, it drops to an acceptable level. However, it was emphasized that "in order to minimize it, a blockade on the use of external carriers or an obligation to use only encrypted data carriers can be introduced".

4. In the letter of (...) January 2021, the Court indicated that before the infringement, in addition to the security risk analysis, which was carried out in 2019, it also took steps to verify the technical and organizational measures used in the years 2018 - 2020 and regularly tested, measured and assessed the effectiveness of technical and organizational measures to ensure the

security of processed personal data through: a) external audit of information security and data protection in common courts in the context of the requirements of the KRI (i.e. National Interoperability Framework), ISO 27001 and data protection of personal data carried out by "C Sp. z o.o.” on (...) September 2018. The assessment covered, among others asset management, including removable media, encryption and cryptography. As part of the audit findings, the following was stated: "lack of clear, formalized rules for handling, supervising and using removable media (e.g. flash drives). No formal procedures for applying cryptographic security and encryption of mobile devices, removable media and e-mail attachments" and the following quote was recommended: "updating the Information Security Management System by updating the existing requirements in the documentation according to ISO 27001", b) an external audit carried out on (...) May and (...) July 2020 by "C Sp. z o.o.” in the scope of analyzing the Information Security Management System in accordance with KRI. As part of the audit findings, it was stated that: "[n]e is not used a control mechanism over portable media in the form of blocking USB ports on computers" and it was recommended to: "introduce a control mechanism over portable media (e.g. by blocking USB ports or introduction of the so-called white list of devices)";c) an audit called "Assessment (...)" by the District Court of Szczecin-Centrum in Szczecin, carried out by an internal auditor on (...) June - (...) September 2020. The auditor assessed the area "Functioning of other good practices in the field of cybersecurity". As a result of the audit, it was found that: "(...) [in] the unit there is a formal ban on using private flash drives, scanning of the media before opening its content is forced, autorun is disabled. However, in the unit, workstations are not blocked in terms of the possibility of using private (unregistered) external media, this is to take place in the near future" and the following quote was recommended: "to block workstations of company desktops and laptops in terms of the possibility of connecting private flash drives to them ".

5. The data controller in the submitted explanations (letter of (...) January 2021) also stated that: 1) the period of storage of personal data to which the breach relates is regulated in § 19-21 of the Regulation of the Minister of Justice of March 5, 2004 on the storage of court files and their transfer to state archives or to their destruction (Journal of Laws of 2014, item 991, as amended);2) in accordance with the recommendations of the Data Protection Officer and the internal auditor, in October 2020 security measures have been introduced in the form of blocking the use of external media other than those issued by the IT Department and only encrypted data carriers authorized by the IT Department are used.

6. The administrator, in a letter of (...) October 2022, informed the authority that: 1) employees (including X) were issued with encrypted portable memory media, (X who committed the infringement received the encrypted medium (...) in September 2019

.), and the Court's IT Department keeps a record of them;2) The Court's IT Department regularly (at least once every six months) reminds employees of the need to bring issued business equipment in order to install software updates and to review and inventory the equipment,3) are kept by of the administrator, audits in the premises after the working hours of the Court - such an audit is aimed at checking whether the employee properly secures the processed information and entrusted assets (an example of an employee's statement of (...) November 2020 about their familiarization with the results of the audit is included in the case files). As the administrator explained, such audits are aimed at checking whether the employee properly secures the processed information and entrusted assets (declarations are received from employees about having read the results of such checks).

7. X, who committed the breach, was trained in the field of personal data protection and information security - copies of sample certificates from the trainings conducted on (...) November 2020, (...) November 2020, (...) December 2021 and (...).03.2021 are in the case files.

8. The case files contain copies of X's statements, e.g. o: 1) commitment to comply with the principles of safe remote work while performing official duties from (...) March 2020 and (...) April 2020, including: a) to perform remote work on the encrypted equipment provided and on which an anti-virus system is installed, b) to connect to the VPN before logging into the Court's systems, c) not to transfer data to private data carriers; 2) to read the documents in the field of information security in the Court of (...) October 2020 and of (...) September 2022;3) undertaking to keep confidential the personal data to which X had access in connection with the performance of his official duties - of (...) May 2009;4) a copy of the annex to the scope of duties employee No. (...) of 2009

9. The case files include a copy of: a) Policy (...) of the District Court of Szczecin-Centrum in Szczecin of (...) January 2013 (updated, inter alia, (...) January 2019 and (...) January 2020 .; before the breach), which states that:- in order to maintain the confidentiality of the transmitted and processed data, cryptographic security measures are applied, (…); b) Policy (…) of the District Court of Szczecin-Centrum in Szczecin of (…) September 2020 (after the occurrence of a breach), which states that: - in order to protect the confidentiality of the transmitted and stored data, cryptographic security measures are used, (...). - in the case of remote work, it should be performed only on the provided company equipment (...); c) of the Regulations (...) of the District Court of Szczecin-Centrum in Szczecin of (...) January 2019 (modified, inter alia, (...) January 2019 and (...) January 2020; before the infringement occurred) - in accordance with § (...) users are prohibited from connecting and using private

equipment, including the use of private data carriers; private equipment, including the use of private data carriers (...); e) the Regulations (...) of the District Court of Szczecin-Centrum in Szczecin of (...) September 2020 (modified (...) August 2021), from which it follows that “[in] the Court, there is a ban on using private electronic information carriers such as flash drives. Authorized persons received official, encrypted flash drives” (…).

10. By letter of (...) October 2020, the Court informed the authority about the publication on (...) October 2020 of a public announcement at https://szczecin-centrum.sr.gov.pl, constituting the fulfillment of the obligation under Art. . 34 of Regulation 2016/679 (at the same time attaching its content).

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

In the proceedings in question, the President of the UODO assessed whether the data controller, when processing personal data, properly fulfills the obligations arising from the provisions of Regulation 2016/679, i.e. Art. 5 sec. 1 lit. e) and ... f), art. 5 sec. 2, art. 24 sec. 1, art. 25 sec. 1 and sec. 2 and art. 32 sec. 1 and sec. 2, in connection with a breach of personal data protection reported to the supervisory authority. The President of the UODO assessed the security measures used by the data controller and their effectiveness in the proceedings in question.

The breach of personal data protection reported by the administrator consisted in the disappearance of a sachet containing three data carriers, one encrypted and two unencrypted, from the room where X performed work. Despite the searches carried out in the Court, no data carriers were found. The content of the lost media contained personal data from court cases conducted by X in the years 2004 - 2020 and indicated the possibility of using private media (unsecured and unverified by the Court's IT Department) on company computer equipment by X for many years. As the proceedings showed, the administrator did not apply adequate technical and organizational measures that would prevent the breach in question, despite the recommendations received from three different audits (the first - (...) September 2018, the second - (...) and (...) July 2020 and the third - (...) June - (...) September 2020). The administrator blocked the USB inputs on company computers only in October 2020, thus preventing the use of data carriers unauthorized by the IT Department of the Court on company equipment.

Due to the fact that the missing data carriers contained personal data contained in draft judgments and justifications prepared by X in connection with his court proceedings, it should be considered that the data controller, pursuant to art. 175db of the Act of July 27, 2001, Law on the Common Courts System (Journal of Laws of 2020, item 2072), hereinafter referred to as Pusp, is

the Court. In accordance with the content of art. 175dd § 1 Pusp, supervision over the processing of personal data whose administrators are courts, in accordance with art. 175 da and art. 175 db, within the scope of the court's activity: 1) district court - president of the regional court, 2) district court - president of the court of appeal, 3) appellate court - the National Council of the Judiciary. The powers of these bodies are provided for by the legislator in Art. 175dd § 2 Pusp. In accordance with the content of art. 55 § 3 of Regulation 2016/679, the President of the UODO is not competent to supervise processing operations carried out by courts as part of their administration of justice. However, it needs to be emphasized that the activities of common courts, apart from activities strictly related to the administration of justice and legal protection, also include administrative activities (Article 8 of the Pusp), thanks to which the courts have the conditions necessary to perform their statutory tasks (i.e. administering justice). Administrative tasks may include: ensuring technical and organizational conditions (i.e. premises, equipment, personnel), or ensuring security. Therefore, the competent authorities referred to in Art. 175dd § 1 Pusp, but the President of the UODO. Due to the fact that the breach in question constitutes a violation of the confidentiality principle expressed in Art. 5 sec. 1 lit. f) of Regulation 2016/679 and is caused by the controller's failure to implement effective technical and organizational measures ensuring a level of security corresponding to the risk of personal data processing, the President of the UODO retains full competence in this matter.

When undertaking operations on personal data, the data administrator is obliged to ensure that it respects the rules on the protection of personal data, ensuring their security.

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

In accordance with the content of art. 24 sec. 1 of the 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 with different probabilities and severity, the administrator implements appropriate technical and organizational measures so that the processing takes place in accordance with this regulation and to be able to demonstrate it . These measures are reviewed and updated if necessary.

This provision defines the basic obligations of the administrator, who is responsible for implementing appropriate technical and organizational measures to ensure 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 and the possibility of demonstrating their implementation, pursuant to art. 5 sec. 2 of Regulation 2016/679.

However, pursuant to art. 25 sec. 1 of Regulation 2016/679, taking into account the state of the art, 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 of the threat 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 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 apply (taking data protection into account in the design phase). However, pursuant to art. 25 sec. 2 of Regulation 2016/679, the administrator implements appropriate technical and organizational measures so that by default only those personal data that are necessary to achieve each specific processing purpose are processed. This obligation applies to the amount of personal data collected, the scope of their processing, the period of their storage and their availability. In particular, these measures ensure that, by default, personal data is not made available without the intervention of a given person to an indefinite number of natural persons.

Pursuant to Art. 32 sec. 1 of the Regulation 2016/679, taking into account the state of the art, 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, where appropriate, the ability to continuously ensure the confidentiality, integrity, availability and resilience of processing systems and services (point b) and regularly testing, measuring and assessing the effectiveness of technical and organizational measures to ensure the security of processing (letter d).

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

The provisions of art. 25 sec. 1 and art. 32 sec. 1 and 2 of Regulation 2016/679, together with art. 24 sec. 1 above-mentioned of the regulation, therefore they constitute a specification of the indicated in art. 5 sec. 1 lit. f) regulation 2016/679, the principle of integrity and confidentiality, and thus data security.

Data confidentiality is a property that ensures, in particular, that data will not be made available to unauthorized entities, obtained, inter alia, through the use of technical and organizational measures, adequate to the scope of data, context of processing and identified risks. The indicated principle, as it results from the established facts, was violated by the Administrator by allowing a situation in which it was possible to use private data carriers, unencrypted, which, as a result of losing these carriers by X, resulted in allowing unauthorized persons access to personal data processed on these carriers . As it was established, the security applied by the Court was a procedure that did not allow the use of private data carriers and the issuance of an X business encrypted data carrier. However, the Administrator's implementation of these safeguards, as the case in question shows, did not prevent the occurrence of a personal data protection breach, and therefore it was not effective.

It needs to be emphasized that "[r]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 regulation through a one-time 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 measures. This means that 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. The administrator is to independently conduct a detailed analysis of the conducted data processing processes and perform a risk assessment, and then apply measures and procedures that will be adequate to the assessed risk. The consequence of this orientation is the resignation from lists of requirements in the field of security imposed by the legislator, in favor of self-selection of security measures based on threat analysis. The administrators are not provided with specific security measures and procedures. The administrator is to independently conduct a detailed analysis of the conducted data processing processes and perform a risk assessment, and then apply measures and procedures that will be adequate to the assessed risk." [judgment of the Provincial Administrative Court in Warsaw of September 3, 2020, ref. No. II SA/Wa 2559/19]. In the context of the aforementioned judgment, it should be pointed out that the risk analysis carried out by the

personal data controller should be documented and justified on the basis of, above all, a specific state factual, existing at the time of its implementation. In particular, the characteristics of the ongoing processes, assets, vulnerabilities, threats and existing safeguards as part of the ongoing personal data processing processes should be taken into account. Also, during this process, the scope and nature of personal data processed in the course of activities carried out by the data controller cannot be omitted, 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 the protection of their personal data will depend. The term asset is used to indicate anything that is of value to the data controller. Certain assets will be of a higher value than others, and they should also be assessed and secured from this perspective. The interconnections of existing assets are also very important, e.g. the confidentiality of assets (personal data) will depend on the type and method of processing this data. Determining the value of assets is necessary to assess the effects of a possible incident (breach of personal data protection). Determining the existing or applied safeguards is necessary, among other things, in order not to duplicate them. It is also essential to check the effectiveness of these safeguards, because the existence of an untested security, firstly, may eliminate its value, and secondly, it may give a false sense of security and may result in the omission (non-detection) of a critical vulnerability, which, if used, will cause very negative effects, including, in particular, lead to a breach of personal data protection. Vulnerability is commonly referred to as a weakness or a security gap that, when used by a given threat, may interfere with the functioning and may also lead to incidents or breaches of personal data protection. Identifying threats consists in determining what threats and from what direction (reason) may appear. In order for the risk analysis to be carried out properly, threats that may occur in the data processing processes should be defined for each of the assets.

Risk management (conducting a risk analysis and, on this basis, defining and implementing appropriate safeguards) is one of the basic elements of the personal data protection system, and, as also indicated by the judgment quoted above, is a continuous process. Therefore, both the adequacy and the effectiveness of the security measures applied should be periodically verified.

The risk analysis submitted by the Court, carried out (...) in December 2019 (before the infringement) shows that the data controller foresaw the risk of loss of confidentiality through "access to data by unauthorized persons due to: storage on unsecured removable media, storage of data/ photos on personal devices. The primary risk was assessed at a medium level, with a value of "6". As a conclusion from the risk analysis, it was indicated that despite setting the risk level at a medium level,

due to the security measures applied by the Administrator, it drops to an acceptable level. However, it was emphasized that "in order to minimize it, a blockade on the use of external carriers or an obligation to use only encrypted data carriers can be introduced".

In the opinion of the President of the UODO, in the risk analysis carried out, the Administrator did not foresee the risk of losing confidentiality of data due to their storage on unsecured or private storage media, the source of which would be the court employee himself (including X). In this case, it cannot be considered that X was an unauthorized person to process the data he had on the lost data carriers. However, there is no doubt that the implementation of the conclusions of the analysis by introducing a blockade of the use of external media would also minimize the risk of X using such devices.

The conclusion of the conducted analysis was the suggestion to introduce a blockade of the use of private storage media or the obligation to use encrypted data storage media. Regardless of the personal source of such a threat, the Administrator, as it turns out, in connection with the occurrence of a breach of personal data protection, did not implement a blockade of USB ports to completely prevent the use of private data carriers, nor did it block the use of storage carriers not registered by the IT Department of the Court, limiting itself only to introducing a formal ban on the use of "private media". Such a ban resulted from § (...) of the Regulations (...).

It should also be emphasized that since December 2019, the Administrator had a program that enabled blocking USB ports, i.e. a program called N . Such a blockade was introduced in the Court, however, only in October 2020, using the N program (allowing the IT Department to control external media and blocking workstations from connecting unauthorized equipment).

The action resulting from the conducted risk analysis, aimed at minimizing the risk of the identified threat related to the possibility of using a private storage medium for personal data processing, was therefore taken approximately 11 months after the purchase of the above-mentioned program and conducting a risk analysis (and two months after the threat materialized). It should also be emphasized that after each of the audits carried out at the Court, the persons conducting them identified the above-mentioned vulnerability and articulated recommendations to block USB ports to increase data security, in order to prevent the use of private data carriers in the Court. In this case, the Administrator therefore applied only organizational measures, but not technical ones. As indicated by the Provincial Administrative Court in Warsaw in the judgment of August 26, 2020, file ref. II SA/Wa 2826/19, "[the] adopted measures are to be effective, in specific cases some measures will have to be measures of a low-risk nature, others - must mitigate high risk, but it is important that all measures (and also each separately)

were adequate and proportionate to the degree of risk." With this action, the Administrator, as the data breach reported to the authority, did not effectively take care of the security of the data processed by the Court. The Administrator, before the violation occurred, did not implement technical measures (no blocked the USB ports in order to prevent the use of private data carriers (not authorized by the IT Department of the Court), although such conclusions were included in the audit reports and resulted from the risk analysis carried out by the Court of (...) December 2019.

Considering the above, it should be pointed out that the lack of security measures adequate to the risks (lack of blocking USB ports to prevent the use of private storage media) in the Court resulted in the Administrator's violation of the provisions of art. 24 sec. 1, art. 25 sec. 1 and art. 32 sec. 1 and 2 of Regulation 2016/679, as a result of which the principle of data confidentiality was violated - art. 5 sec. 1 lit. f) Regulation 2016/679. The consequence of violating the confidentiality principle is violating the accountability principle referred to in Art. 5 sec. 2 of Regulation 2016/679. Provincial Administrative Court in Warsaw in the judgment of February 10, 2021, file ref. II SA/Wa 2378/20, indicated that "The principle of accountability is therefore based on the legal responsibility of the controller for the proper fulfillment of obligations 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 principles." The issue of the principle of accountability is similarly interpreted by the Provincial Administrative Court in Warsaw in the judgment of August 26, 2020, file ref. II SA/Wa 2826/19, stating that "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."

It should also be emphasized that the Administrator, despite the procedures in place (the ban on the use of private data carriers regulated in the Regulations (...) of the Court) and the knowledge of threats (mainly from audits), did not supervise whether the employees of the Court comply with internal regulations in apply in this respect, which proves a violation of Art. 32 sec. 1 lit. d) Regulation 2016/679. Reviewing and updating the implemented organizational and technical measures is also expressly formulated in art. 24 sec. 1 of Regulation 2016/697. It should also be emphasized that the implementation of technical and organizational measures by the administrator is not a one-time action, but it should take the form of a process under which the administrator reviews and, if necessary, updates the previously adopted security measures. Regular

assessment of the applied security measures, pursuant to art. 32 sec. 1 lit. d) of Regulation 2016/679, would allow the Administrator to verify whether the introduced procedure prohibiting the use of private data carriers is respected, and therefore effective, and, consequently, gave the opportunity to determine whether appropriate actions are being taken to ensure the protection of data processed by employees of the court. It should therefore be emphasized that regular testing, measuring and assessing the effectiveness of technical and organizational measures to ensure the security of the processed data, including the effectiveness of the implemented procedures, also serves to ensure the fulfillment of the Administrator's obligations and the security of the processed data.

In the facts of the case in question, in the opinion of the President of the UODO, verification of the method of implementation (application) of an organizational measure in the form of a ban on the use of private data carriers would significantly reduce the risk of infringement or lead to its complete elimination, e.g. by using a technical measure in the form of blocking USB ports . It needs to be emphasized again that as a result of the audits carried out in the Court, such vulnerability was indicated by the persons conducting them (i.e. no blocked USB ports preventing the use of private data carriers), and recommendations were issued to block them. In addition, as a conclusion from the risk analysis carried out (...) in December 2019, it was indicated that the risk of breach is at an acceptable level for the Administrator, but "[in] order to mitigate the risk, a blockade of the use of external media or the obligation to use only encrypted data media may be introduced ". However, the Court, as the data controller, only in October 2020 (i.e. after the infringement) blocked the USB ports for data carriers not authorized by the IT Department, thus preventing the use of private data carriers by Court employees.

In addition, in order to meet the requirement of Art. 32 sec. 1 lit. d) of Regulation 2016/679, indicated in the abovementioned According to the judgment of the Provincial Administrative Court in Warsaw, as an obligation to ensure continuity of monitoring the level of threats and to ensure accountability in terms of the level and adequacy of implemented security measures, the personal data controller should regularly test, measure and evaluate the effectiveness of technical and organizational measures to ensure the security of processing. In the case in question, such measurement took place in connection with the audits carried out, but the recommendations that were then indicated by the persons conducting them were not implemented. The Administrator's failure to respond to the recommendations of the auditors weakens the data protection system and exposes it to legal consequences, both on the part of the authorities (administrative and criminal liability), as well as on the part of the persons whose data has been breached (civil liability). In this way, the administrator took the risk that materialized in the

breach in question. This breach, however, showed irregularities in the process of securing data by the Administrator. Considering the above, there is no doubt that the Administrator, before the infringement occurred, was aware of the threat posed by the use of private data carriers. This is evidenced by both the risk analysis carried out and the resulting conclusions as to how to minimize the identified threats, conclusions from subsequent audits carried out in the Court, as well as organizational measures taken in the form of a ban on the use of private data carriers specified in the Regulations (...) of the Szczecin-Centrum District Court in Szczecin, or the order to use encrypted data carriers contained in the Policy (…) of the District Court of Szczecin-Centrum in Szczecin and specifying the principles of safe remote work. Despite this awareness, however, the Court did not implement technical measures to ensure the security of personal data. Before the personal data protection breach occurred, the administrator limited himself to implementing only organizational security measures. Considering the above, it should be pointed out that the lack of application of adequate security measures to the identified threats to personal data processed by the Court (possibility of using private data carriers) caused the Administrator to violate the provisions of art. 24 sec. 1, art. 25 sec. 1, art. 32 sec. 1 and 2 of Regulation 2016/679, as a result of which the principle of data confidentiality was violated - art. 5 sec. 1 lit. f) of Regulation 2016/679 (and as a consequence of the violation of the accountability principle expressed in Article 5(2) of Regulation 2016/679), because the data was first recorded on unauthorized data carriers (out of the Administrator's control), and then lost by X In the opinion of the President of the UODO, the Administrator's failure to apply the above-mentioned security measures, despite his knowledge of both threats and vulnerabilities in the organization, leads to the conclusion that no action has been taken in the Court to ensure default data protection. And this constitutes a violation of Art. 25 sec. 2 of Regulation 2016/679.

At the same time, it should be emphasized that despite the Administrator's request to demonstrate what trainings X, who committed the infringement, had undergone, and when they took place, to what extent (and whether they concerned the principles of data processing, in particular on data carriers), the Court sent information about the training, in which this X participated after the infringement occurred and copies of the statements referred to in point 8 of the facts. However, the administrator has not demonstrated that the above-mentioned X has been trained in the protection of personal data or security measures before the occurrence of a breach. Therefore, it should be emphasized that merely receiving statements from X that he is familiar with the rules in force in the Court, without additional dedicated training in this area, is not a sufficient means of influencing the awareness of a given person. 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 any 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.

To sum up, despite the removal by the Court of deficiencies in ensuring the security of the processed data, including by blocking USB ports against the possibility of using data carriers unauthorized by the IT Department, the lack of which was an indirect cause of the breach of confidentiality of personal data, there were premises justifying the application to the Court of the President of the Office the power to impose an administrative fine for breaching the principle of data confidentiality [Art. 5 sec. 1 lit. f) of Regulation 2016/679], and consequently the accountability principle [Art. 5 sec. 2 of Regulation 2016/679] in connection with the violation of the administrator's obligations when implementing security measures during data processing, in order to effectively implement data protection principles and ensure default data protection [art. 25 sec. 1 and 2 of Regulation 2016/679]; obligations to ensure confidentiality, integrity, availability and resilience of data processing systems and services [art. 32 sec. 1 lit. b) Regulation 2016/679]; the obligation to regularly test, measure and evaluate the effectiveness of the adopted technical and organizational measures to ensure the security of processing [art. 32 sec. 1 lit. d) of Regulation 2016/679] and the obligation to take into account the risk of processing, resulting from unauthorized access to personal data being processed [art. 32 sec. 2 of Regulation 2016/679].

The use by the President of the UODO of the power vested in him to impose an administrative penalty on the data controller results primarily from the fact that the Controller violated the basic principles of data processing, i.e. the principle of

confidentiality, by failing to apply effective technical and organizational measures in the Court, guaranteeing their security and, consequently, the principle of accountability described in art. 5 sec. 2 of 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 corrective measures provided for in art. 58 sec. 2 lit. a) - h) and point. j) of this Regulation, an administrative fine under Art. 83 of Regulation 2016/679, depending on the circumstances of a particular case.

When deciding to impose an administrative fine on 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 the circumstances incriminating the Court to the extent indicated below.

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 [Art. 83 sec. 2 lit. a) of Regulation 2016/679]. The violation of personal data protection provisions found in this case, which resulted in the possibility of obtaining unauthorized access to the data processed by the Court by an unauthorized person or persons, and, consequently, the possibility of obtaining personal data of persons for whom projects were prepared rulings and judgments, is of considerable weight and serious nature, as it poses a high risk of negative legal consequences for an undetermined, potentially (taking into account that the documents on lost private data carriers were from 2004 - 2020) large number of people whose data unauthorized person or persons may have access. At the same time, the Court was not able to show the number of persons affected by the infringement, nor the scope of data. The violation by the Court 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 the provisions of Regulation 2016/679 e.g. in order to establish legal relations or incur liabilities on behalf of the persons whose data was obtained. In addition, until this decision is issued, the missing data carriers have not been found, so an unauthorized person or persons may still have access to personal data on these carriers. At this point, it needs to be emphasized that the Court, as an institution of public trust, but also a state authority administering justice, is obliged to apply higher standards, in particular with regard to the security of processed data.

The long duration of the infringement of the provisions of Regulation 2016/679 should also be emphasized, as it should be assumed that the infringement began on May 25, 2018, i.e. on the date of application of Regulation 2016/679, and ended in

October 2020 (the administrator did not provided the date of the day on which the USB ports were blocked). It is true that the data carriers were most likely lost in August 2020 (on (...) August 2020, the Administrator found a violation of personal data protection), which showed the lack of adequate security measures, but from May 25, 2018 the Administrator was obliged to adapt data processing processes to the requirements of Regulation 2016/679.

In the present case, there is no evidence that persons whose data was 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 was obtained in an unauthorized manner may at least feel fear of losing control over their personal data, identity theft or identity fraud, discrimination, or finally financial loss. In addition, public notice to individuals does not guarantee that the information has reached every person it should reach. Thus, a situation could have arisen in which persons affected by the breach, having no knowledge of the breach, could not take action to ensure at least a minimum sense of security by increasing caution in using their own personal data.

2. Intentional or unintentional nature of the infringement [Art. 83 sec. 2 lit. b) of Regulation 2016/679]. Unauthorized access to personal data of persons against whom actions were taken by the Court became possible as a result of failure to exercise due diligence by the Court. In the opinion of the supervisory body, this constitutes an unintentional nature of the infringement, resulting from the negligence of the Court, because the Administrator had knowledge of the risks associated with the use of private storage media and the lack of blocking USB ports, which is clearly evidenced by the recommendations made after the above-mentioned tests. audits or after a risk analysis. Despite this knowledge, the Administrator has taken steps to ensure data security only in the scope of organizational measures, excluding those of a technical nature. The court, as the administrator, is therefore responsible for any irregularities found in the data processing process. In particular, what deserves a negative assessment, which should be emphasized again, is the fact that the Court only introduced a ban on the use of private storage media, but did not test the effectiveness of this protection, including whether employees actually comply with this ban.

3. Categories of personal data affected by the breach [Art. 83 sec. 2 lit. g) of Regulation 2016/679]. The lost data carriers contained draft judgments, justifications and orders drawn up by X in the period from December 2004 to August 2020 in connection with his social insurance cases. This means that the data could also include information on health, data on the course of employment, information on salaries. The administrator was unable to demonstrate the exact scope of the missing data. The statement of X, who lost the data carriers, shows that they could contain the names and surnames of the parties to

the proceedings, information about their subject and data on the health of the participants in the proceedings. However, the content of the application form shows that, apart from the name and surname and information about health, the lost data carriers also contained information about workplaces or addresses of residence / stay of these people (information in this regard in the supplementary form was withdrawn). Therefore, if there was information about health, it means that there were special categories of data (Article 9 of Regulation 2016/679) that are associated with a high risk of violating the rights or freedoms of persons affected by the violation. Unauthorized disclosure of special categories of data in connection with the name, surname and information on the subject and course of court proceedings may have a real and negative impact on the protection of the rights or freedoms of natural persons.

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 good cooperation of the Court with the supervisory authority undertaken and carried out in order to remove the infringement and mitigate its possible negative effects [art. 83 sec. 2 lit. f) Regulation 2016/679]. It should be indicated here that, apart from the proper fulfillment of the procedural obligations incumbent on the Court during the administrative proceedings, which ended with the issuance of this decision, the Court fully implemented the recommendations of the President of the Office regarding supplementing the notification of data subjects about the breach. The court also took specific and quick actions, which resulted in removing the possibility of recurrence of the infringement. In particular, the Court removed the susceptibility to a violation of the protection of personal data being processed by introducing recording and encryption of portable memory, blocked USB ports, preventing the use of private data carriers not registered by the IT Department.

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 by the Court to minimize the damage suffered by the data subjects [Art. 83 sec. 2 lit. c) of Regulation 2016/679]. The Administrator's activities in this regard were limited only to notifying persons of the infringement, through a public message, made available on the Administrator's website. The administrator does not know whose data was actually on the missing storage media. However, this communication is only the fulfillment of the legal obligation under Art. 34 sec. 3 lit. c) of Regulation 2016/679, and as stipulated in the Wp Guidelines. 253 (referring to the premise of "the manner in which the supervisory authority became aware of the breach") "[simple] fulfillment of [...] the obligation by the controller cannot be

interpreted as a weakening/mitigating factor".

2. The degree of responsibility of the Court, taking into account the technical and organizational measures implemented by it pursuant to Art. 25 and 32 of Regulation 2016/679 [art. 83 sec. 2 lit. d) of Regulation 2016/679]. The 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, adopted on October 3, 2017, indicated that - 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 the 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 Court violated the provisions of art. 25 sec. 1, art. 32 sec. 1 lit. b) and lit. d) and Art. 32 sec. 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 Court did not "did everything that could be expected of it"; 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, may not 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 Court."

3. Relevant previous infringements of the provisions of Regulation 2016/679 by the Court [Art. 83 sec. 2 lit. e) of Regulation 2016/679]. The President of the UODO did not find any previous violations of the provisions on the protection of personal data by the Administrator, therefore there are no grounds for treating this circumstance as aggravating. It is the duty of each administrator to comply with the law (including the protection of personal data), so the lack of previous violations cannot be a mitigating circumstance when imposing sanctions.

4. The manner in which the supervisory authority found out about the infringement [Art. 83 sec. 2 letter h) of Regulation 2016/679]. The President of the UODO found a violation of the provisions of Regulation 2016/679 as a result of the notification of a personal data breach made by the Administrator, however, due to the fact that the Administrator, by making this

notification, only carried out his legal obligation, no there is reason to believe that this circumstance constitutes a mitigating circumstance for him. In accordance with 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 breach 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.'

5. Compliance with the measures previously applied in the same case referred to in Art. 58 sec. 2 of Regulation 2016/679 [art. 83 sec. 2 lit. 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.

6. Application of approved codes of conduct under Art. 40 of Regulation 2016/679 or approved certification mechanisms under Art. 42 of Regulation 2016/679 [art. 83 section 2 lit. j) of Regulation 2016/679]. The administrator does not use the instruments referred to in art. 40 and art. 42 of Regulation 2016/679. However, their adoption, implementation and application is not - as stipulated in the provisions of Regulation 2016/679 - mandatory for controllers and processors, therefore the circumstance of their non-application cannot be considered to the disadvantage of the Controller 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.

7. Financial benefits achieved directly or indirectly in connection with the infringement or losses avoided [art. 83 sec. 2 lit. k) of Regulation 2016/679]. The President of the UODO did not find that the controller gained any financial benefits or avoided such losses in connection with the infringement. 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.

8. Other aggravating or mitigating factors (Article 83(2)(k) of Regulation 2016/679). The President of the UODO, examining the case comprehensively, did not notice any circumstances other than those described above that could affect the assessment of the infringement and the amount of the adjudicated administrative fine.

Taking into account all the circumstances discussed above, the President of the Personal Data Protection Office decided that the imposition of an administrative fine on the Court is necessary and justified by the weight, nature and scope of the infringements alleged against the Court. It should be stated that the application of any other remedy provided for in Art. 58 sec. 2 of Regulation 2016/679, and in particular, limiting oneself to a warning (Article 58(2)(b) of Regulation 2016/679) would not be proportionate to the identified irregularities in the processing of personal data and would not guarantee that the Court will not further omissions.

Referring to the amount of the administrative fine imposed on the Court, the President of the Personal Data Protection Office decided that in the circumstances of this case - i.e. in view of finding a violation of several provisions of Regulation 2016/679 (principle of data confidentiality, expressed in Article 5(1)(a) f), and reflected in the form of the obligations set out in Art. 25 sec. 1, art. 32 sec. 1 and 2 of Regulation 2016/679, which in turn means a violation of the accountability principle referred to in art. 5 sec. 2 of Regulation 2016/679) and the fact that the Court is a public finance sector entity - Art. 102 of the Act of May 10, 2018 on the protection of personal data (Journal of Laws of 2019, item 1781), which limits the amount (up to PLN 100,000) of the penalty that may be imposed on a public finance sector entity.

Due to the fact that in the facts in question, more than one provision of Regulation 2016/679 was violated, the violation of which affected the amount of the financial penalty imposed, pursuant to art. 83 sec. 3 of Regulation 2016/679, the breach by the Court of the principle of confidentiality set out in Art. 5(1)(a) f) Regulation 2016/679 and, consequently, the principle of accountability specified in art. 5 sec. 2 of Regulation 2016/679. This is supported by the serious nature of the breach, the scope of personal data subject to the breach and the group of people affected (an undetermined number of people for whom draft judgments, justifications and orders were prepared from December 2004 to August 2020, data whose administrator is the Court). Importantly, in relation to the above persons, there is still a high risk of unlawful use of their personal data, because the purpose for which the unauthorized person or persons may take action to use this data is unknown.

In the opinion of the President of the UODO, the applied administrative fine fulfills the functions referred to in art. 83 section 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 for Personal Data Protection, the penalty imposed on the Court will be effective, as it will lead to a state in which the Court will apply such technical and organizational measures that will ensure a level of security for the processed data corresponding to the risk of violating the rights and freedoms of data subjects and the severity of the accompanying threats the processing of this personal data. The effectiveness of the penalty is therefore equivalent to the guarantee that the Court will take actions adequate to the risks from the moment of completion of these proceedings.

The fine applied is also proportional to the infringement found, in particular its gravity, the circle of affected natural persons and the risk they incur in connection with the infringement. In the opinion of the President of the UODO, the fine imposed on the Court will not constitute an excessive burden for it. 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 infringement of the administrator's obligations, but on the other hand, it does not cause a situation where the need to pay an administrative fine will have negative consequences, in the form of a significant deterioration of the situation of the Court. According to the President of the Personal Data Protection Office, the Court should and is able to bear the consequences of its negligence in the field of data protection, hence the imposition of a fine of PLN 30,000 is fully justified.

In the opinion of the President of the UODO, in these specific circumstances, the administrative fine will fulfill a repressive function, as it will be a response to the violation by the Court of the provisions of Regulation 2016/679, but also a preventive one, as it will contribute to preventing future violations of the Court's obligations under the provisions on the protection personal data, both when processing data by the Court itself.

In the opinion of the President of the Office for Personal Data Protection, the fine applied in the circumstances of this case 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.

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

On the other hand, with regard to the allegation of violation by the Court of Art. 5 sec. 2 in connection with art. 5 sec. 1 lit. e) of Regulation 2016/679, it should be pointed out that due to the fact that personal data on lost private storage media were contained in X's draft decisions or orders, i.e. processed in connection with X's official activities, consisting on the

administration of justice, it should be considered that the President of the UODO is not competent to take a position, but one of the authorities indicated in art. 175dd Pusp.

In accordance with the content of art. 5 sec. 1 letter e) of Regulation 2016/679, personal data must be stored in a form that allows identification of the data subject for no longer than is necessary for the purposes for which the data is processed; personal data may be stored for a longer period, as long as they are processed solely for archival purposes in the public interest, for scientific or historical research purposes or for statistical purposes pursuant to art. 89 sec. 1, subject to the implementation of appropriate technical and organizational measures required under this Regulation to protect the rights and freedoms of data subjects ("storage limitation"). Examining the necessity of personal data processed by the Court and their retention is not within the competence of the President of the UODO. In each proceeding, it is the court itself who, through decisions, resolutions, ordinances, determines the usefulness of evidence containing, among others, personal data by allowing or not allowing them, according to their knowledge, experience and legal provisions (appropriate procedure - civil, criminal or court-administrative). Adopting a different position would lead to the President of the UODO examining the legality of personal data processing processes directly related to the conducted court proceedings, which could lead to the interference of this authority in the administration of justice by the court. Thus, the proceedings, in the opinion of the President of the UODO, have become pointless in this respect and are subject to discontinuation.

In connection with the above, it should be pointed out that Art. 105 § 1 of the Act of June 14, 1960 Code of Administrative Procedure (Journal of Laws of 2022, item 2000, as amended), hereinafter referred to as the Code of Administrative Procedure, when the proceedings for any reason became pointless in whole or in part , the public administration body issues a decision to discontinue the proceedings in whole or in part, respectively. The doctrine indicates that: "the groundlessness of administrative proceedings, as provided for in Art. 105 § 1 of the Code of Administrative Procedure, means that there is no element of a substantive legal relationship, and therefore a decision cannot be issued to settle the case by resolving it on the merits. The premise for discontinuation of the proceedings may exist even before the proceedings are initiated, which will only be revealed in the pending proceedings, and it may also arise during the proceedings, i.e. in a case already pending before the administrative authority" (B. Adamiak, J. Borkowski, "Kodeks Administrative Proceedings. Commentary", 14th edition, Wydawnictwo C.H.Beck, Warsaw 2016, p. 491).

Determination by a public authority of the existence of the premise referred to in Art. 105 § 1 k.p.a., obliges him, as

emphasized in the doctrine and jurisprudence, to discontinue the proceedings, because then there are no grounds to resolve the case on the merits, and further conduct of the proceedings in such a situation would constitute its defectiveness, having a significant impact on the outcome of the case . In a situation where the authority lacks competence in matters belonging to the judiciary, it is reasonable to discontinue the proceedings.

Considering the above, the President of the Office for Personal Data Protection decided as in the conclusion of this decision.

Print article

Metadata

Provider:

Inspection and Infringement Department

Produced information:

John Nowak

2023-01-19

Entered the information:

Wioletta Golanska

2023-02-08 14:02:22

Recently modified:

Iwona Jeleń

2023-02-20 11:15:46