THE CHAIRMAN OF PERSONAL DATA PROTECTION

Warsaw, day 11

February

2021

DECISION

DKN.5130.2024.2020

Based on Article. 104 § 1 and art. 105 § 1 of the Act of June 14, 1960, Code of Administrative Procedure (Journal of Laws of 2020, item 256, as amended) in connection with Art. 7 sec. 1, art. 60, art. 102 paragraph 1 point 1) and sec. 3 of the Act of May 10, 2018 on the Protection of Personal Data (Journal of Laws of 2019, item 1781) and Art. 57 sec. 1 lit. a) and art. 58 sec. 2 lit. i) in connection with Art. 5 sec. 1 lit. f), art. 24 sec. 1, art. 25 sec. 1, art. 28 sec. 1 and 3 and article. 32 sec. 1 and 2, as well as art. 83 sec. 1 - 3, art. 83 sec. 4 lit. a) and art. 83 sec. 5 lit. a) Regulation of the European Parliament and the EU Council 2016/679 of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46 / EC (general regulation on data protection ) (Journal of Laws UE L 119 of 04/05/2016, p. 1, as amended), after conducting administrative proceedings regarding the processing of personal data by the National School of Judiciary and Public Prosecution based in Krakow, ul. Przy Rondzie 5, 31-547 Kraków, and e. Sp. z o.o. based in W., President of the Personal Data Protection Office,

1) finding a breach by the National School of Judiciary and Public Prosecution based in Krakow of the provisions of Art. 5 sec. 1 lit. f), art. 25 sec. 1, art. 28 sec. 3, art. 32 sec. 1 and 2 of Regulation 2016/679 of the European Parliament and of the Council and of the EU Council 2016/679 of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46 / EC (general regulation on data protection) (Journal of Laws EU L 119 of 04/05/2016, p. 1 as amended), hereinafter referred to as "Regulation 2016/679", consisting in failure to fulfill the obligations incumbent on the administrator, resulting from Regulation 2016 / 679, through:

a) failure to apply appropriate technical and organizational measures to ensure the ability to continuously ensure the confidentiality of processing services, failure to test and evaluate the effectiveness of technical and organizational measures aimed at ensuring the security of personal data contained in a copy of the database of the training platform of the National School of Judiciary and Public Prosecution, and thus, incorrect consideration of the risks associated with changes in the

processing process,

b) entrusting the processing of personal data e. Sp. z o.o. based in W., in violation of Art. 28 sec. 3 of Regulation 2016/679, i.e. without the contractual obligation of the processor to process personal data only on the documented administrator's request, and without specifying the categories of persons in the contract for entrusting the processing of personal data and without specifying the type of personal data by indicating their category,

imposes an administrative fine in the amount of PLN 100,000 (one hundred thousand zlotys) on the National School of Judiciary and Public Prosecution based in Kraków;

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

Justification

On [...] April 2020, the National School of Judiciary and Public Prosecution (hereinafter also referred to as: "KSSiP" or "administrator") notified the President of the Personal Data Protection Office (hereinafter also referred to as: "the President of the Personal Data Protection Office") registered under the reference number […]. The notification was completed by the KSSiP [...] April 2020. The violation notification indicated that [...] April 2020 the administrator was notified by the Police Headquarters about the appearance of personal data related to the kssip.gov.pl domain on the Internet. On the same day, the controller found a breach of personal data protection. After getting acquainted with the type of data, he determined that these were data from the database of the training.ksip.gov.pl website created on [...] February 2020 during the test migration to the new training platform ekssip.kssip.gov.pl. The breach concerned the personal data of 50,283 people (KSSiP explained it in a letter of [...] April 2020, originally it indicated 50,776 people in the report). The categories of data concerned by the infringement were finally indicated in the supplementary notification and include: name and surname, e-mail address, user name, telephone number, unit, department, unit address, city, technical data: IP address, date of the first and last login, password (in secret form). The administrator informed that analytical activities are being carried out to determine whether the violation also applied to PESEL identification numbers. In order to remedy the breach and minimize the negative consequences for the data subjects, the controller sent a notification to the administration of the forum publishing a link to the database with a request to block the information and to the administration of the portal providing the data file for blocking the possibility of downloading. In addition, he removed all passwords on the new platform and posted information about the need to change the password when logging in to the new platform. Noting a high risk of violating the rights and freedoms of data subjects, he started informing all

affected persons about the situation (by e-mail). In the supplementary notification, the KSSiP provided the content of the notification and stated that the notification was addressed to 50,283 data subjects.

In a letter of [...] April 2020, the controller further specified the categories of data subjects that had originally been identified in the initial breach notification (employees of the Ministry of Justice). In addition, KSSiP indicated that the violation concerns users subject to continuous training, whose personal data was collected on the KSSiP Training Platform. These persons perform professions and hold positions specified in Art. 2 clause 1 point 2 and point 3 of the Act of 23 January 2009 on the National School of Judiciary and Public Prosecution (Journal of Laws of 2020, item 1366, as amended), i.e. judges, assessors, prosecutors and assessors of the prosecutor's office, referendaries judges, assistants to judges, assistants to prosecutors, professional probation officers as well as court and prosecutor's office clerks. The KSSiP training platform also included the accounts of some lecturers conducting continuous training, the few KSSiP applicants and people whose accounts were activated on the basis of individual decisions. The latter category of people includes employees of the Ministry of Justice who, using accounts such as supervised the implementation of projects financed by this ministry, verifying, for example, the inclusion of certain information or training materials.

In a letter of [...] June 2020, the President of the Office for Personal Data Protection notified the National School of Judiciary and Public Prosecution about the initiation of administrative proceedings, the subject of which is the possibility of breach by KSSiP, as a data controller, of obligations under the provisions of Regulation 2016/679 in the scope of obligations arising from art. 5 sec. 1 lit. f), art. 24 sec. 1, art. 25 sec. 1, art. 28 sec. 1 and 3 and article. 32 sec. 1 and 2. In addition, by letters of [...] July 2020, he informed KSSiP and e. Sp. z o.o. with its seat in W., hereinafter referred to as "e.", that the pending proceedings also apply to the obligations of e. as a processor entrusted by KSSiP with the processing of personal data of persons affected by the violation. Thus, there were grounds for recognizing e. As a party to the proceedings, pursuant to Art. 28 of the Act of June 14, 1960, Code of Administrative Procedure (Journal of Laws of 2020, item 256, as amended).

In the course of the proceedings conducted in this case, the President of the Personal Data Protection Office, in letters of: [...] April, [...] May, [...] June, [...] July and [...] October 2020, called KSSiP to provide explanations. In addition, by letters of: [...] July, [...] September and [...] October 2020, the President of UODO called for explanations also e .. Based on the explanations submitted by the KSSiP in letters of: [...] April, [...] May , […] July, […] July and […] October 2020 and by e. In letters of: […] July, […] September and […] November 2020, the supervisory authority established the following facts :

As the KSSiP indicated in the letter of [...] July 2020 - The e-KSSiP Training Platform, operating from [...] March 2020 at the address ekssip.kssip.gov.pl, is a tool enabling the implementation of the assumptions of the project "Implementation of modern research methods training needs and education as the key to effective justice ", implemented from the European Social Fund under the Knowledge Education Development Operational Program 2014-2020, Priority Axis II Effective public policies for the labor market, economy and education, Measure 2.17 Effective administration of justice. OSA is responsible for the design, development, implementation and technical support of this platform, under contract No. [...] of [...] April 2019 and contract for entrusting the processing of personal data No. [...] of [...] April 2019 (copy of the contract entrustment constitutes an attachment to the letter from KSSiP of [...] May 2020).

The existing KSSiP Training Platform (Edukacja.kssip.gov.pl) and the target e-KSSiP Training Platform (ekssip.kssip.gov.pl) are located on IT resources made available under the hosting agreement concluded between the National School of Judiciary and Prokuratury and e. Sp. . z o.o. based in W .. The data processing agreement constitutes Annex No. [...] to the hosting agreement No. [...] concluded in Krakow on [...] December 2019 between these entities. Copies of both agreements were attached to the letter of the KSSiP of [...] April 2020. The remaining annexes were provided by the KSSiP in a letter of [...] October 2020 and e. In a letter of [...] November 2020.

In connection with the procedure adopted to launch the new platform, as indicated in the KSSiP letter of [...] April 2020, two migration stages were planned: "test" and "production". The "test" migration took place on [...] - [...] February 2020, and the "production" migration - on [...] February - [...] March 2020.

On [...] - [...] February 2020, an employee of the IT department of KSSiP, AM and the Director of the IT Department of KSSiP, PT, received messages from the contractor of the new platform, OSA, with the implementation schedule and scope of responsibility for individual areas (KSSiP / ABOUT.).

[...] February 2020 at [...] AM, sent an e-mail to e. Asking for "(...) making a copy of the database (dump) PROD PS" and "(...) packing the Moodledata directory from the PROD server" and "(...) transferring the above 2 copies to the new PROD eKSSiP server ". In response, the employee of E., K. J., asked for clarification of the above-mentioned requests, incl. by indicating the IP addresses of the servers and full paths to the source and target resources, indicating ignorance of the internal designations of KSSiP services and resources. After A. M. provided this information on the same day, K. J. in an e-mail at [...] announced the end of "copying". The above-mentioned e-mails constitute attachments to the e. Letter of [...] July 2020, which are identical

to the explanations provided in point 3 of the KSSiP letter of [...] April 2020.

[...] February 2020 at [...], due to the completed assumptions of the "test" migration, AM, "[in] in connection with the migration (...)" requested to perform activities analogous to those performed on [...] February 2020, immediately indicating the addresses IP and full paths to source and target resources. The above, on the same day, was implemented and confirmed by the correspondence of K. J ..

[...] April 2020 on the website. an unknown person has placed a link to a file hosted on the [...] platform, which is a copy of the user table from the KSSiP Training Platform database.

[...] April 2020, the Police Headquarters notified the administrator of the above circumstances. On the same day, based on the record of the last login from a publicly shared user table and a copy of the database owned by OSA, used as part of the "test" migration, KSSiP concluded that a breach of personal data protection occurred on [...] February 2020. , i.e. on the day on which the data-based activities were commissioned to processors, i.e. e. and contractors of the new platform - OSA

[...] in April 2020, the administrator reported the incident to the Incident Management Team of the Cybersecurity Bureau of the Ministry of Justice and CSiRT gov.pl (the report was redirected to CSiRT NASK). The data protection officer at KSSiP was also informed about the situation. In addition, KSSiP commissioned the contractor of the e-KSSiP Training Platform (O. S.A.) to urgently reset the passwords of all users of the e-KSSiP Training Platform together with relevant information. At the same time, O. S.A. was requested to conducting an urgent security audit of the e-KSSiP server and securing information (logs). KSSiP also sent a request to the forum administration [...] to remove the information and a second request to the operator of the [...] website on which the file is located (both the information on the forum and the file have been deleted).

[...] April 2020, the Head of the IT Department of the KSSiP (the manager's official note is an attachment to the KSSiP letter of [...] April 2020) commissioned A. M. to contact e. And O. S.A. on the verification of the availability of personal data of the current and target platform, on servers provided by e ..

[...] on April 2020, the KSSiP sent a notification to the National Prosecutor's Office about the possibility of committing a crime.

[...] April 2020, the KSSiP reported the violation to the President of the Personal Data Protection Office.

On [...] - [...] April 2020, there was an exchange of correspondence between an employee of the KSSiP, A. M. (as part of the activities ordered by the Head of the IT Department of KSSiP [...] April 2020), and representatives of e., K. J. and K. O .:

[...] in April 2020, the question was asked if the files stored in the public _ [...] directory were safe. The reply indicated, inter

alia, that this directory "(...) is not hosted in any way by the functionality of the web server, because the directory ../ public _ [...] for [...], which was created during the server implementation and not it is functional ”.

[...] April 2020, requests were made to "check in the logs whether the files in the public _ [...] directory were somehow moved, copied, downloaded from the moment they were sent to the specified server on [...]. 02.2020 ". The reply indicated that "[a] ccess logs are not kept for that long and, in addition, such operations are not logged (...)".

[...] in April 2020, requests were made to "(...) check why all files are visible in the https: // [...] network". The response indicated that "directory listing has been disabled".

On [...] - [...] April 2020, platform users were notified of a personal data breach by means of messages sent to e-mail addresses and a message on the controller's website. According to the submitted explanations, this information was preliminary.

[...] April 2020, an employee of the IT department of KSSiP, BK, analyzing the information contained in the server management panel and e-mail (services provided under the contract with e.), Found the presence of entries indicating the download [...] April 2020 . via two IP addresses, files located in a location accessible from a web browser, directly after the IP address, without the need to provide the internet domain of the current KSSiP Training Platform, i.e. http: // [...] / BACKUP- [...] -02-2020 /. One of these files was a file entitled "[...] .sql", 5.9 GB in size, last modified on [...] February 2020. This information, together with its graphical representation, can be found in the official notes of the above-mentioned the employee and the Director of the IT Department of the KSSiP, attached to the explanations of the KSSiP of [...] April 2020.

On [...] - [...] April 2020, the controller sent an e-mail to data subjects entitled "Notice of breach of personal data protection which may involve a high risk of violating your rights or freedoms".

[...] in April 2020, on the website of the National School of Judiciary and Public Prosecution www.kssip.gov.pl, a communication on the finding of a breach of personal data protection was published.

On [...] - [...] April 2020, the controller sent an e-mail to data subjects entitled "Updated communication pursuant to Art. 34 of the GDPR of [...] April 2020 "

[...] and [...] in April 2020, officers of the Police and the Internal Security Agency secured logs and disks, which are administered by e ..

[...] April 2020, the National Prosecutor's Office publishes on its website the announcement to which the KSSiP refers in its

explanations of [...] April and [...] May 2020. The announcement is available at: https://pk.gov. pl / aktualnosci / aktualnosci-prokuratury-national / detention-suspect-about-causing-data-leakage-z-kssip /.

By letter of [...] May 2020, KSSiP withdrew from the contract for the provision of hosting services No. [...] of [...] December 2019, concluded with e. Sp. z o.o., due to the fault of the contractor, due to the gross, in the opinion of KSSiP, violation of § 6 sec. 1 lit. d of the contract and the provisions of the contract for entrusting the processing of personal data, constituting Appendix No. 5 to the above-mentioned the contract. Information on the withdrawal from the contract for the provision of services was provided by KSSiP in the explanations of [...] May 2020 and confirmed by e. In the explanations of [...] September 2020.

[...] May 2020 e. Provided by protocol all data obtained from KSSiP and in connection with the above-mentioned the contract is obliged to delete any existing copies of the data processed under the contract. This information was provided in the KSSiP letter of [...] May 2020. The deletion of the data was confirmed by e. In letters of [...] July and [...] September 2020.

In addition, to the letters of [...] July 2020 and [...] November 2020 in order to clarify the obligations arising from the relationship with the KSSiP, e. Submitted sample correspondence between its representatives and KSSiP, both before and after the breach of protection personal data.

With regard to the analytical activities carried out to determine whether the breach also concerned PESEL registration numbers, the KSSiP in a letter of [...] April 2020, indicated that it was, inter alia, the subject of proceedings conducted by the Regional Prosecutor's Office in Lublin. In connection with the above, the President of UODO, in a letter of [...] May 2020, asked the Regional Prosecutor's Office in Lublin to inform, inter alia, whether and how many PESEL numbers of the users of the KSSiP Training Platform, the confidentiality was breached and how. In response from [...] May 2020, the Prosecutor's Office informed that "(...) the database of users of the Training Platform of the National School of Judiciary and Prosecution, which was downloaded from the servers of the company providing hosting services for KSSiP, and then made public on the Internet, includes 44 262 records containing PESEL numbers ".

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

Pursuant to the wording of Art. 24 sec. 1 of Regulation 2016/679, taking into account the nature, scope, context and purposes of processing as well as the risk of violating the rights or freedoms of natural persons of varying probability and seriousness,

the controller implements appropriate technical and organizational measures to ensure that the processing takes place in accordance with this Regulation and to be able to demonstrate it. These measures are reviewed and updated as necessary. This means that when assessing the proportionality of the safeguards, the controller should take into account the factors and circumstances relating to the processing (e.g. type, method of data processing) and the risks associated with it. At the same time, the implementation of appropriate safeguards is an obligation which is a manifestation of the implementation of the general principle of data processing - the principle of integrity and confidentiality, as defined in Art. 5 sec. 1 lit. f) of Regulation 2016/679, according to which personal data should be processed in a manner ensuring adequate data security, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, by appropriate technical or organizational measures.

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

Art. 32 sec. 1 of Regulation 2016/679 provides that the controller is required to apply technical and organizational measures corresponding to the risk of violating the rights or freedoms of natural persons with a different probability of occurrence and the severity of the threat. The provision specifies that when deciding on technical and organizational measures, one should take 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 likelihood and severity. It follows from the above-mentioned provision that the determination of appropriate technical and organizational measures is a two-stage process. In the first place, it is important to determine the level of risk related to the processing of personal data, taking into account the criteria indicated in art. 32 of Regulation 2016/679, and then it should be determined what technical and organizational measures will be appropriate to ensure the level of security corresponding to this risk.

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

the risk associated with the processing, in particular resulting from accidental or unlawful destruction, loss, modification, unauthorized disclosure or unauthorized access to personal data sent, stored or otherwise processed.

If the processing is to be carried out on behalf of the controller, then pursuant to Art. 28 sec. 1 of Regulation 2016/679, it uses only the services of such processors that provide sufficient guarantees for the implementation of appropriate technical and organizational measures so that the processing meets the requirements of Regulation 2016/679 and protects the rights of data subjects. Moreover, in accordance with par. 3 lit. h) of this Article, the controller has the power to obtain from the processor all information necessary to demonstrate compliance with the obligations set out in Art. 28 of the Regulation 2016/679 and has the power to conduct audits, including inspections. However, pursuant to Art. 28 sec. 3 lit. b) of Regulation 2016/679, the processor ensures that the persons authorized to process personal data have committed themselves to secrecy or are subject to an appropriate statutory obligation of secrecy.

According to the content of Art. 28 sec. 3 of Regulation 2016/679, the processing by the processor takes place on the basis of a contract or other legal instrument that are governed by Union law or the law of a Member State and are binding on the processor and the controller, determine the subject and duration of processing, nature and purpose of processing, type of personal data and categories of data subjects, obligations and rights of the controller.

The provisions of Regulation 2016/679 therefore oblige administrators and processors to adopt appropriate technical and organizational measures to ensure a level of security corresponding to the risk related to the processing of personal data.

Taking into account the presented facts, in order to properly resolve the matter being the subject of this decision, it was first necessary to examine the compliance of the concluded entrustment agreement with the provisions on the protection of personal data and the scope of liability of the parties to this agreement, taking into account the above-mentioned the provisions of Regulation 2016/679, and in particular the criteria contained in art. 28 sec. 3 of the Regulation 2016/679.

Along with the letter of [...] April 2020, KSSiP sent the contract for entrusting the processing of personal data concluded with e. Sp. z o.o., constituting the attachment number [...] to the contract of [...] December 2019, number [...], hereinafter referred to as the "main contract". As it results from the content of this contract and the collected evidence, e., As the provider of the hosting service, he was selected in the public procurement procedure under the open tender procedure, in accordance with the provisions of the Act of January 29, 2004 - Public Procurement Law (Journal U. of 2019, item 1843). As rightly pointed out in the above-mentioned in writing, in the event of entrusting the processing of personal data to an external entity, the contract for

entrusting the processing of personal data specifies the subject and duration of processing, the nature and purpose of processing, the type of personal data and categories of data subjects, as well as the obligations and rights of the administrator. Considering the processing of personal data through the prism of the entire Regulation 2016/679, the requirement to include a relatively detailed description of processing in the entrustment agreement is fully justified. Comprehensive inclusion of the elements resulting from Art. 28 sec. 3 of Regulation 2016/679 is aimed at ensuring the precise determination of the boundaries of the processor's operation, which is the basis for the entrustment agreement due to the fact that the processor is bound to the purpose set by the administrator.

The content of the entrustment agreement, in the opinion of the President of the Personal Data Protection Office, in § 2 point 1 insufficiently specifies the scope of the entrusted data, i.e. it was indicated that "[p] the processing entity as part of the hosting service will process the entrusted ordinary personal data including personal data sets necessary for performing work in the IT system for the administrator ". The administrator did not indicate the categories of data subjects required by art. 28 sec. 3 of the Regulation 2016/679. He only used the concept of a personal data set. When applying the teleological interpretation, it should be noted that in this context the "type of data", also required by the above-mentioned provision, refers to information on the characteristics of a specific group of personal data subjects, known to the administrator, that have not been indicated in the entrustment agreement. When describing the processing of data, the contract should also refer to their categories, if they can be clarified. While in the case of data processing related to, for example, the e-mail service, it is difficult to clearly indicate such scope, in the case of data processing for purposes related to the functioning of the KSSiP training platform, such information, as possible to define, should be included.

Therefore, the KSSiP, entrusting the processing of personal data e., Did not enter into the contract to entrust the processing of personal data of the category of persons and did not specify the type of personal data by indicating their category, which constitutes a violation of Art. 28 sec. 3 of the Regulation 2016/679.

Pursuant to Art. 28 sec. 3 point a) of Regulation 2016/679, the data processing agreement stipulates, inter alia, that the processor processes personal data only on a documented administrator's request. While this element can be interpreted to some extent from § 3 point 3 of the main contract, according to which "[the] claims of faults related to hosting services, including their unavailability, will be made in writing, by fax or e-mail", in the opinion of Of the President of the Personal Data Protection Office, the indicated provision of the contract is insufficient. The entrustment agreement concluded with e. Should

contain at least a general wording obliging the processor to act only on the documented administrator's instruction.

In view of the above, the KSSiP, entrusting the processing of personal data e., Did not conclude in the contract the obligation of the processor to process personal data only on the documented administrator's instruction, which constitutes a violation of Art. 28 sec. 3 lit. a) of Regulation 2016/679.

Referring to the nature of the entrustment agreement, § 2 point 2 of the entrustment agreement indicates that the entrusted personal data will be processed only for the purpose of implementing the main agreement, i.e. performing on dedicated servers, provided by e., Website hosting services and a training platform, e-mail hosting, as well as providing full administrative support for the above-mentioned servers on the terms described in the main contract. The main agreement in § 3 and § 4 refers to communication channels, conditions ensuring the continuity of the hosting service and obligations related to ensuring its availability, e.g. with regard to informing about interruptions in access to services. Annex 1 to the contract, in turn, specifies technical requirements, such as computing power, memory, disk resources, environment (virtualization of hosts and their management) and the issues of administrative support for these servers, including technical consultations. The scope of the service provided, and thus the nature of entrusting data processing, is therefore the same as the description of the subject of the contract contained in the specification of essential terms of the contract specified in the tender, under which e. He was selected as the service provider. The specification is attached as Annex No. [...] to the letter e. Of [...] November 2020.

The processor in the explanations of [...] November 2020, referring to the content of Art. 14 and art. 15 of the Act of 18 July 2002 on the provision of electronic services (Journal of Laws of 2020, item 344, i.e.), hereinafter referred to as "u.ś.ude", indicates that "(...) we corresponded several times aimed at clearly delimiting the issue of our activities over the host system and the area of customer data and applications, which we did not deal with and we had no access to, or the possibility of logging in to his administration panel ". As confirmation of the above, he attached a sample correspondence with KSSiP. It shows that the employees of the KSSiP, both before and after the breach of data protection, were not fully aware of the rights and obligations between the administrator and the processor, resulting from the contract of [...] December 2019 Administrator several times expected to perform tasks beyond the scope of this contract. The nature of the hosting service, indicated in the contract, did not oblige e. To interfere with the source code of the application, which is a tool for processing personal data. The processing entity did not know the structure and configuration of proprietary applications installed by the administrator on these resources, including no obligation, without the knowledge of the administrator and on his documented command, to carry out

configuration activities in the field of access to directories or databases used by these applications. In line with the essence of the service provided, this area is characterized by a certain autonomy on the part of the administrator and he has full knowledge of what personal data is processed, how, in what location (within the provided resources) and with what tools. The processor may interfere with the scope resulting from the nature of the services provided and the concluded contract only upon the documented instruction of the controller.

KJ, in e-mails of [...] February or [...] March 2020, in response to requests falling within the scope of technical support resulting from the hosting agreement, pointed out that in the messages addressed to e. nomenclature and markings (e.g. PROD PS database, "old" training platform, e-learning platform, training base), which for the hosting service provider, due to the nature of the service provided, is not known, which in turn causes problems interpretative. One of such inquiries was sent on [...] February 2020 by a representative of the KSSiP, A. M., in which he asked, inter alia, o "make a copy of the database (dump) PROD PS" and "transfer (...) the copy to a new server PROD eKSSIP.". In reply, K. J. pointed to the above-mentioned aspects and asked for a precise indication of, inter alia, "Path to the folder to which we want to copy and IP of the target server". In response, the KSSiP employee indicated the requested information. The word "migration" in relation to the processor, as it results from the collected evidence and as rightly indicated by e., Appeared for the first time in the e-mail of [...] February 2020 addressed by AM to e. In a similar case, as of [...] February 2020. He mentioned in it that in connection with the migration he is asking for specific actions, i.e. o to make a copy of the indicated database and send it to the indicated resources. This information, however, still did not in any way refer to the nature of the activities undertaken and did not include personal data as information of particular importance from the point of view of ensuring their security.

As indicated by e. In the above-mentioned writing, the concept of hosting should be equated with the wording of Art. 14 sec. 1 "u.ś.u.d.e.", i.e. as the provision of ICT system resources for the purpose of data storage. From the perspective of entrusting processing, the contract may, however, specify other obligations of the processor. Therefore, the premise referred to by e. Citing the content of Art. 15 u.ś.u.d.e., i.e. that there is no obligation to check the transferred, stored or shared data by the entity providing the hosting service. In the entrustment agreement, the controller may oblige the processor to perform such activities. However, in the case examined in this decision, the nature of the service provided, the administrative obligations and the established facts did not impose e. General obligations related to the monitoring of personal data.

The provisions of Regulation 2016/679 provide a certain freedom in terms of shaping the relationship between the controller

and the processor. Therefore, looking from the perspective of the obligations under Art. 24 sec. 1 and art. 25 sec. 1 of Regulation 2016/679 in connection with Art. 28 sec. 1 and sec. 3 of Regulation 2016/679 that the administrator will develop a model of cooperation with the processor that will ensure processing in accordance with the provisions on the protection of personal data, and in particular enable the implementation of the principle of accountability expressed in art. 5 sec. 2 of Regulation 2016/679. While the parties to the contract have established communication channels and designated persons performing activities related to the performance of the contract (Annexes [...] and [...] to the main contract), and the orders issued were documented, as is clear from the above-mentioned correspondence, the designated persons by KSSiP still not aware of the rights and obligations between the KSSiP and e .. in consultation with e. use concepts that are understandable to both parties, minimizing the risk of breach of personal data protection.

KSSiP, in a letter of [...] July 2020, in response to a question from the President of the Personal Data Protection Office (UODO) aimed at determining whether the administrator had undertaken verification activities in terms of removing an unnecessary copy of the database after the migration was completed, did not answer directly, but only emphasized that " the subject of the order sent to e. Sp. z o.o. on [...] February 2020 (...) regarding the performance of migration-related activities, there was (...) transfer of the above 2 copies to the new eKSSiP PROD server ". As KSSiP points out, the very "transfer", according to the common understanding of the word, should be understood as "(...) taking something (made copy) from one place and placing it without duplicating it elsewhere, in another location, in this case on a new server EXSiP PROD. This means that after completing the migration process carried out in accordance with the order, no unnecessary copy of the database that needs to be deleted should not be left. "

As the above explanations indicate, KSSiP, in line with its purpose and processing method, decided that no copy of the database should remain after the migration process was completed. Both before and after commissioning the activities on [...] February 2020 and [...] February 2020, the administrator did not verify whether the said copy is still on the KSSiP resources. It was not until [...] April 2020, an employee of the KSSiP, A. M., asked e. Whether the data contained in the above-mentioned locations are safe. Since the administrator made the decision that the said copy of the database should be deleted, it was his duty to verify that this operation had been performed. Even if, as a result of an error, the employee e. Did not remove the copy made because he did not comply with the request for its "transfer", the administrator was still obliged to verify whether the indicated location ensures the security of processing. It is the controller who initiates the actions taken as the entity deciding

about the purposes and methods of processing. Pursuant to the contract for the provision of services, it is him who has been provided with the environment in which he performs this processing and he is primarily responsible for its security, and as it results from the contract for the provision of services, he uses the assistance of the processor, if necessary.

In the opinion of the President of the Personal Data Protection Office, the model of cooperation between the controller and the processor was ineffective. Misunderstandings resulting from the presented correspondence and the controller's lack of understanding of the role it plays in relation to the processor have led to a breach of personal data protection.

As indicated by both KSSiP and e., All logs from the hosting server and data carriers affected by the violation were transferred to [...] and [...] April 2020 to the authorities that secured them for the proceedings conducted by the Regional Prosecutor's Office in Lublin.

While, on the basis of the collected evidence, it is not possible to indicate an unequivocal date of the first download of the database copy and to determine the moment at which the incorrect configuration of the hosting machine took place, allowing direct access to the copy of the database by unauthorized persons, the circumstances under which mentions e. in its explanations of […] July and […] September 2020. The processor performed a number of steps to establish how the root directory was made public directly after the server's IP address. As indicated by e., The extensive documentation of the panel software does not answer this question, because according to this documentation, the configuration preventing such access was set as expected at the time of checking (i.e. after finding a violation by KSSiP). The processor indicates that in its opinion, one of the indications that there have been changes in the settings of the hosting management software is the correspondence with the KSSiP between [...] February 2020 and [...] March 2020 regarding the provision of the platform training by IP address, which he refused, citing technical and data security reasons. Moreover, e. Based on the conducted analyzes, it indicates that the indexation of the hosting root directory (i.e. making it available to search engines), which contained a copy of the database, took place between [...] and [...] February 2020.

Regardless of the above, as e. Rightly indicates in the explanations of [...] July 2020, in accordance with the requirements of the tender and the contract for the provision of services, hosting is managed by dedicated software that creates configuration files on an ongoing basis in accordance with the settings of the user, i.e. employees KSSiP. In addition, e. Indicated a number of other configuration options that were the responsibility of KSSiP, which could result in the publication of the directory containing a copy of the database directly after the IP address.

In the opinion of the President of the Personal Data Protection Office, the processing entity fulfilled the obligations arising from the entrustment agreement and the main agreement, as well as applied organizational measures adopted by it to ensure the security of IT systems. This goal is indicated, inter alia, through the technical support referred to in Annex 1 to the main contract. Evidence of the processor's compliance with the above, significant from the point of view of the breach of personal data protection of [...] February 2020, is the correspondence dated [...] March 2020, attached to the letter of [...] November 2020, which e. also mentions in the explanations of [...] September 2020. In this correspondence, e. refused to help the KSSiP employee to configure the server so as to allow access to specific resources of the KSSiP Training Platform directly at the indicated IP address, referring to data security and incompatibility with the system used to control the configuration of the host machine. He proposed a different, safe in his opinion, solution that would be a response to the reported demand.

KSSiP, referring to the risks associated with the migration process in the letters of [...] July and [...] July 2020, indicated that: representatives of the KSSiP Aid Funds Department took into account that the migration was to take place within the resources of one professional hosting provider, e. Sp. z o.o., having the necessary certificates (including ISO), which, in the opinion of KSSiP, significantly limited the risk of a possible breach of data security, with appropriate security of access to the system from the side of e-KSSiP,

contact of the employees of the IT Department of KSSiP was limited to only one person on the part of e.

In the opinion of the President of the Personal Data Protection Office, the risk analysis carried out in this way is inadequate to the nature of the activities undertaken in connection with the migration and the nature of the hosting service contract concluded. Citing the status of a "professional hosting provider with the necessary certificates" is related solely to the nature of the service provided, ie the provision of ICT system resources for the purpose of data storage. The administrator did not undertake an analysis whether by indicating to the processor a place to back up the database, he does not expose the personal data contained therein to a breach of their confidentiality, without informing e. About the importance of the actions taken in terms of personal data protection.

In addition, the KSSiP, referring to the announcement of the National Prosecutor's Office, indicates that "(...) it seems legitimate to find that even more extensive verification by the administrator of the performance by the processor of the obligations referred to in § 3 para. 3 and 4 of the contract would not guarantee avoidance of the breach. ". In the opinion of the President of the Personal Data Protection Office, the thesis formulated in this way is an attempt to remove the responsibility

from KSSiP for the event that has occurred. It should be clearly emphasized that in the period from [...] February 2020 to [...] April 2020, the KSSiP IT resources contained a copy of the database, the existence and security of which has not been verified in any way by the administrator, which is its legal an obligation resulting from the provisions on the protection of personal data. In the light of the established facts, it should be stated that the presence of a copy of the database in the resources indicated by the KSSiP employee was a surprise for the administrator, which, in the opinion of the President of the Personal Data Protection Office, means that the administrator has no control over the processing of personal data. It should be emphasized that the addressees of the obligations specified in Art. 24 sec. 1 and art. 25 sec. 1 of Regulation 2016/679 is only the administrator. He is responsible for implementing appropriate technical and organizational measures to provide the necessary security measures for the processing.

While Art. 28 sec. 3 lit. f) of Regulation 2016/679, the processor is obliged to support the administrator in fulfilling the obligations set out in art. 32-36 of this regulation, however, it is subject to conditions that must be taken into account each time, i.e. the nature of the processing and the information available to the processor. § 3 point 6 of the entrustment agreement stipulates that the processor assists in this respect "as far as possible". However, KSSiP, in the orders of [...] February 2020 and [...] February 2020, did not ask for prior verification of the security of the indicated location and did not inform e. About the circumstances of the activities, i.e. the migration, which the subject is personal data of 50,283 people, and that the process must ensure their appropriate security. The processor, who does not have such information, cannot always guess the nature of the activity performed and perform each operation by first verifying whether it is dealing with personal data and whether the environment and resources made available to the controller in accordance with the contract are properly and securely configured. Due to the nature of the contract, he has no right to interfere with the configuration without prior, documented instruction from the administrator. The context of the activities carried out was known only to the controller and it is the controller who has an absolute obligation to make sure that the activities carried out will not expose the data subjects to violation of their rights or freedoms.

In the summons of [...] April 2020, the President of the Personal Data Protection Office (UODO) addressed KSSiP, inter alia, for disclosure of whether and which the administrator has adopted technical and organizational security measures in accordance with the above-mentioned regulations and providing relevant documentation. In the letter of [...] April 2020, although the KSSiP mentioned its data security policy, it did not provide such documentation. However, to the letter of [...] July

2020, he attached an e-mail containing a new platform implementation plan, indicating the parties (KSSiP / O.) Responsible for individual activities. The attached schedule indicates that KSSiP was responsible for all operations related to making a copy of the database and transferring it to the target server. As it results from the collected evidence, e. Was not involved or informed about the nature of the activities undertaken, which is repeatedly emphasized by the processor in the complex explanations. Employee e., K. J., did not have any information about the changes introduced by KSSiP in the processing of personal data contained in the file being a copy of the database from [...] February 2020, and the activities carried out by the above-mentioned of the employee constituted the implementation of tasks resulting from the contract for the provision of services, i.e. as part of technical support. In the opinion of the President of the Personal Data Protection Office, on the basis of the collected evidence, these were not activities consisting in "sharing" or granting "public" powers enabling "(...) unauthorized access to information stored in the KSSiP IT system". Therefore, the President of the Personal Data Protection Office does not see grounds for accusing the processor of breaching the obligation to support the controller in fulfilling the obligations set out in Art. 32 of Regulation 2016/679.

In addition, to the letter of [...] July 2020, e. photocopies of security policies, regulations, including regulations for the provision of services, ISO / EIC 27001 internal audit reports, documents on risk assessment in the organization, procedures for granting access and controlling granted authorizations in IT systems, documents confirming the authorization to process and professional qualifications of K. J ..

Therefore, on the basis of the collected material, there are no indications that e. Breach of the obligations under Art. 32 sec. 1 and 2 of Regulation 2016/679 and art. 32 in connection with Art. 28 sec. 3 lit. f) Regulation 2016/679. As a consequence, the President of the Personal Data Protection Office (UODO) discontinued the proceedings in this respect.

Based on the collected evidence, the President of the Personal Data Protection Office stated that the National School of Judiciary and Public Prosecution based in Krakow did not take sufficient steps to verify the security of the processing environment before and after the start of migration activities, in particular, it did not verify during [... ] February 2020 - [...] April 2020, is there still a copy of the database from [...] February 2020 in the location indicated by the KSSiP. Deciding not to involve the processor in the migration process and not to provide full information about the activities undertaken and the expected results, the controller did not make sure that the processed personal data is properly secured. The controller did not undertake this verification until the date of finding the infringement. This constitutes a gross neglect of the obligations of the

KSSiP and a breach of the provisions of Art. 32 sec. 1 and sec. 2 of Regulation 2016/679 by failure to apply appropriate technical and organizational measures to ensure the ability to ensure the confidentiality of processing services on an ongoing basis and failure to test and evaluate the effectiveness of technical and organizational measures, and thus incorrectly taking into account the risks associated with changes in the processing process. The administrator's obligation, as stated in the above-mentioned regulations, as well as art. 24 sec. 1 and art. 25 sec. 1 of Regulation 2016/679, when assessing the proportionality of security, it is necessary to take into account the factors and circumstances relating to the processing (e.g. type, method of data processing) and the risks associated with it. Any changes in the processing of personal data are a circumstance that makes the controller responsible for the materialization of risks related to failure to comply with the above obligations. Ensuring adequate security of personal data at every stage of processing should be a subject of special care for the controller. Thus, this constitutes a violation by KSSiP of Art. 24 sec. 1 and art. 25 sec. 1 of Regulation 2016/679. Failure to comply with these obligations resulted in downloading a copy of the database from [...] February 2020 by unknown and unauthorized persons, which constitutes a breach by KSSiP of the confidentiality principle expressed in Art. 5 sec. 1 lit. f) Regulation 2016/679 by processing personal data in a manner that does not ensure adequate security of personal data.

The above is also indicated by the case law of the Provincial Administrative Court in Warsaw, which in the judgment of August 26, 2020, file ref. II SA / Wa 2826/19 ruled, inter alia, that Art. 32 of Regulation 2016/679 "(...) does not require the data controller to implement any technical and organizational measures that are to constitute personal data protection measures, but requires the implementation of adequate measures. Such adequacy should be assessed in terms of the manner and purpose for which personal data are processed, but also the risk related to the processing of such personal data should be taken into account, the risk of which may vary. " In addition, he also stressed that "[p] taken measures are to be effective, in specific cases some measures will have to be low risk mitigating measures, others must deal with high risk, but it is important that all measures (as well as all measures) separate) are adequate and proportional to the degree of risk. ”.

The analogous understanding of the obligations imposed on the administrator is also confirmed in the judgment of the Provincial Administrative Court of September 3, 2020, II SA / Wa 2559/19. In it, the court ruled that "Regulation 2016/679 introduced an approach in which risk management is the foundation of activities related to the protection of personal data and is an ongoing process. Entities processing personal data are obliged not only to ensure compliance with the guidelines of the above-mentioned of the regulation through one-off implementation of organizational and technical security measures, but also

to ensure the continuity of monitoring the level of threats and ensuring accountability in terms of the level and adequacy of the introduced security. This means that it becomes necessary to prove to the supervisory authority that the implemented solutions aimed at ensuring the security of personal data are adequate to the level of risk, as well as taking into account the nature of the organization and the personal data processing mechanisms used. The administrator is to independently carry out a detailed analysis of the data processing processes carried out and assess the risk, and then apply such measures and procedures that will be adequate to the assessed risk.

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

The subjective party of the obligations referred to in Art. 5 sec. 1 letter f), art. 24 sec. 1, art. 25 sec. 1 and art. 28 sec. 1 of Regulation 2016/679 is the administrator. As it results from the collected evidence, e. Sp. z o.o. based in W. has the status of a processor within the meaning of art. 4 point 8 of Regulation 2016/679. Therefore, pursuant to Art. 105 § 1 of the Code of Civil Procedure, the President of the Personal Data Protection Office (UODO) discontinued the proceedings against e. In this regard.

In the light of the provisions of Art. 28 sec. 1 and art. 28 sec. 3 lit. h) of Regulation 2016/679, the choice of a processor that guarantees adequate security is the responsibility of the controller. Along with the explanations of [...] July 2020, e. Submitted numerous documents that regulate the relationship between him and the administrator. President of the Personal Data Protection Office, based on the submitted documentation and explanations submitted by the KSSiP, among others in a letter of [...] May 2020, from the point of view of the above-mentioned provisions, did not find any circumstances that would allow to conclude that e. did not provide sufficient guarantees for the security of personal data and did not provide the administrator with all information necessary to demonstrate compliance with the obligations set out in art. 28 of Regulation 2016/679 or prevented the administrator from carrying out audits, including inspections. As a consequence, the President of the Personal Data Protection Office (UODO) discontinued the administrative proceedings against e. Breach of Art. 28 sec. 3 lit. h) Regulation 2016/679. Thus, it also discontinued the proceedings against KSSiP in the scope of violation of Art. 28 sec. 1 in the

context of the selection of a processor providing sufficient guarantees for data security. Therefore, it does not constitute the basis for the imposition of an administrative fine.

Bearing in mind the above findings, the President of the Office for Personal Data Protection, exercising his powers specified in art. 58 sec. 2 lit. i) Regulation 2016/679, pursuant to which each supervisory authority has the power to apply, in addition to or instead of other remedial measures provided for in Art. 58 sec. 2 lit. a-h and lit. (j) of that Regulation, an administrative fine pursuant to Article 83 of the Regulation 2016/679, having regard to the circumstances established in the present proceedings, stated that in the case under consideration there were premises justifying the imposition of an administrative fine.

When deciding to impose an administrative fine on KSSiP, as well as determining its amount, the President of the Personal Data Protection Office - pursuant to Art. 83 sec. 2 lit. a-k of the regulation 2016/679 - took into account the following circumstances of the case, aggravating and affecting the size of the imposed financial penalty:

1. Categories of personal data affected by a personal data breach (Article 83 (2) (g) of Regulation 2016/679) - data of persons registered on the KSSiP training platform include in particular: name and surname, e-mail address, username , telephone number, unit, department, unit address, city, PESEL identification number. KSSiP in a letter of [...] April 2020 indicated that the correct, i.e. 11-character string of numbers representing PESEL numbers, is in the database 44 577. The President of the Personal Data Protection Office assumed that the number of persons affected in this respect with a data protection violation was 44 262 , according to the information provided by the Regional Prosecutor's Office in Lublin in a letter of [...] May 2020.

2. The nature and gravity of the violation, taking into account the number of people injured (Article 83 (2) (a) of Regulation 2016/679) - when imposing the penalty, it was important that the number of people affected by the violation was 50,283. that the breach of data confidentiality concerns persons practicing professions and holding positions specified in art. 2 clause 1 items 2 and 3 of the Act of 23 January 2009 on the National School of Judiciary and Public Prosecution (Journal of Laws of 2020, item 1366, as amended), i.e. judges, assessors, prosecutors and assessors of the public prosecutor's office, court referendaries , assistants to judges, assistants to prosecutors, professional probation officers as well as court and prosecutor's office clerks. The KSSiP training platform also included the accounts of some lecturers conducting continuous training, the few KSSiP applicants and people whose accounts were activated on the basis of individual decisions. The latter category of people includes employees of the Ministry of Justice. The breach resulted in a high risk of negative consequences in the future resulting from the nature of the data, the large number of data subjects, possibly the ill-will of the unauthorized person, and the

large-scale and professional nature of the processing. Violation of confidentiality of the telephone number, e-mail address or PESEL number of the above-mentioned persons may result in an unprecedented entry into the private life of those affected by the violation, and from the point of view of their functions, taking action to deprive them of public trust. Such a request is particularly legitimate in the case of judges and prosecutors, due to the fact that the breach of data confidentiality concerns persons professionally related to the judiciary and legal professions. In relation to the above-mentioned of persons, there is still a high risk of unlawful use of their personal data, because the purpose for which the person or unauthorized persons may take unlawful actions is unknown. The data subjects may therefore suffer material damage, and the very breach of data confidentiality is also non-pecuniary damage (harm). This is because data subjects may, at the very least, fear losing control of their personal data, identity theft or identity fraud, and finally financial loss. Summarizing the above, it must be considered that the infringements found in the present case are of significant gravity and serious nature and the probability of their negative consequences for the data subjects is high.

3. Duration of the infringement (Article 83 (2) (a) of Regulation 2016/679) - the collected evidence allowed the President of the Personal Data Protection Office to state that the KSSiP did not take appropriate steps to verify whether the copy of the database from [...] February 2020 r. is still available on the KSSiP IT resources and whether these resources are properly configured to ensure the security of the data contained in this copy. It did not perform this action until [...] April 2020, i.e. on the date of establishing the breach of personal data protection. The duration of the violation, i.e. the period from [...] February 2020 to [...] April 2020, has a significant impact on the amount of the fine imposed by the President of the Personal Data Protection Office, as ongoing verification of the safety of the environment in which the migration process was carried out could minimize the risk to the rights or the freedom of the persons concerned, including the avoidance of the event that resulted in the publication of [...] April 2020 on breakingin.to a link to a file constituting a table of users from a copy of the database.

4. Unintentional nature of the breach (Article 83 (2) (b) of Regulation 2016/679). Taking into account the findings in the case being the subject of this decision, it should be stated that the KSSiP has been guilty of gross negligence resulting in the breach of data confidentiality. This is a significant circumstance with a negative impact on the amount of the administrative fine.

5. The high degree of responsibility of the controller (Article 83 (2) (d) of Regulation 2016/679) - Considering that it is the controller who is responsible for assessing the security measures at every stage of processing, in particular during any changes to the data processing process personal data, it should be stated that the KSSiP has not implemented appropriate

technical and organizational measures to ensure the security of personal data processing in a situation where, on its own initiative, it has taken steps related to the process of personal data migration to the new processing environment.

The fact of imposing and the size of the administrative fine had no influence on other, specified in Art. 83 sec. 2 of Regulation 2016/679, the circumstances:

1. Actions taken by KSSiP to minimize the damage suffered by data subjects (Article 83 (2) (c) of Regulation 2016/679) - KSSiP fulfilled its obligation to notify data subjects about a breach of their personal data referred to in Art. 34 of the Regulation 2016/679. However, it did not take any additional (beyond the legal obligation) measures to mitigate or compensate for the harm suffered by the affected persons.

2. The way in which the supervisory authority learned about the breach (Article 83 (2) (h) of Regulation 2016/679) - the breach of personal data protection was reported to the President of the Personal Data Protection Office by the KSSiP, which is the fulfillment by the KSSiP of its obligation referred to in art. 33 of the Regulation 2016/679.

3. KSSiP does not apply the approved codes of conduct pursuant to Art. 40 of the Regulation 2016/679 or approved certification mechanisms pursuant to Art. 42 of the Regulation 2016/679.

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

5. It was not found that the Administrator obtained financial benefits or avoided the losses referred to in Art. 83 sec. 2 lit. k) Regulation 2016/679.

When determining the amount of the administrative fine, the President of the Personal Data Protection Office also took into account the actions taken by the administrator to minimize the damage suffered by the data subjects (Article 83 (2) (c) of Regulation 2016/679). The main part of these activities are the obligations arising directly from Regulation 2016/679 and other acts, i.e. reporting a breach of personal data protection to the President of the Personal Data Protection Office, informing about the breach of data protection to the data subjects, notifications of law enforcement agencies or the Incident Management Team of the Cybersecurity Bureau of the Ministry. Justice and CSiRT NASK. It should be emphasized that the Administrator sent a direct request to the forum administration [...] and a second request to the website operator [...] to delete the file with the database copy and the link leading to this database. This action resulted in the removal of both the file with the database copy from the anonfiles.com website and the removal of the link from the breakingin.to forum leading to the file.

The above-mentioned actions are undoubtedly the circumstances which, as a rule, mitigate the responsibility of the data

controller. However, their occurrence does not have a direct impact on the amount of the administrative fine imposed by this decision due to the fact that the KSSiP is a public entity to which the provisions of Art. 102 paragraph 1 point 1) The Act of 10 May 2018 on the protection of personal data (i.e. Journal of Laws of 2019, item 1781). This provision reduces the possibility of imposing the fine in question on a public entity to the maximum amount of PLN 100,000. In the opinion of the President of the Personal Data Protection Office, the maximum fine imposed in the present case is still disproportionate to the scale and gravity of the infringement from the perspective of Regulation 2016/679. The reduction of the fine due to mitigating circumstances was consumed in the present case by a circumstance more favorable to KSSiP, ie the statutory limitation of the fine to PLN 100,000.

Taking into account all the above-mentioned circumstances, the President of the Personal Data Protection Office decided that the imposition of an administrative fine in the amount of PLN 100,000 (one hundred thousand zlotys) on the KSSiP is necessary and justified by the weight, nature and scope of the violations made by KSSiP.

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

The administrative fine will perform a repressive function in these specific circumstances, as it will be a response to the breach by KSSiP of the provisions of Regulation 2016/679, but also preventive, i.e. preventing future violations of the provisions on the protection of personal data by both KSSiP and other data administrators.

The purpose of the imposed penalty is to ensure that KSSiP performs its duties properly, in particular in Art. 5 sec. 1 lit. f), art. 24 sec. 1, art. 25 sec. 1, 28 sec. 3, art. 32 sec. 1 and 2 of Regulation 2016/679, and consequently to conduct data processing processes in accordance with applicable law.

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

2021-02-18