THE CHAIRMAN OF PERSONAL DATA PROTECTION

Warsaw, 19

January

2022

DECISION

DKN.5130.2215.2020

Based on Article. 104 § 1 and 105 § 1 of the Act of June 14, 1960 Code of Administrative Procedure (Journal of Laws of 2021, item 735, as amended), Art. 7 sec. 1, art. 60, art. 101 and 103 of the Personal Data Protection Act of May 10, 2018 (Journal of Laws of 2019, item 1781) and art. 57 sec. 1 lit. a) and h) 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 sec. 3, art. 32 sec. 1 and 2 and article. 34 sec. 1, as well as art. 83 sec. 1-3 and art. 83 sec. 4 lit. a) and art. 83 sec. 5 lit. a) Regulation of the European Parliament and of the EU Council 2016/679 of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46 / EC (General Data Protection Regulation) (Official Journal of the European Union L 119 of 04/05/2016, p. 1, Official Journal of the European Union L 127 of 23/05/2018, p. 2 and the Official Journal of the European Union L 74 of 04/03/2021, p. 35) , after conducting administrative proceedings initiated ex officio regarding the processing of personal data by Fortum Marketing and Sales Polska Spółka Akcyjna with its registered office in Gdańsk at ul. Marynarki Polskiej 197 and PIKA Sp. z o.o. with headquarters in Gdańsk at ul. Spadochroniarzy 7, President of the Office for Personal Data Protection

1) finding an infringement by Fortum Marketing and Sales Polska S.A. with headquarters in Gdańsk at ul. Polish Navy 197 Art. 5 sec. 1 lit. f), art. 24 sec. 1, art. 25 sec. 1, art. 28 sec. 1 and art. 32 sec. 1 and 2 of Regulation 2016/679, consisting in failure to implement appropriate technical and organizational measures to ensure the security of personal data, resulting in a breach of their confidentiality, and failure to verify the processor as to whether it provides 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, imposes on Fortum Marketing and Sales Polska S.A. with headquarters in Gdańsk at ul. Marynarki Polskiej 197, for violation of Art. 5 sec. 1 lit. f), art. 25 sec. 1, art. 28 sec. 1 and art. 32 sec. 1 and 2 of Regulation 2016/679, an administrative fine in the amount of PLN 4,911,732 (in words: four million nine hundred and eleven thousand

seven hundred and thirty two PLN),

2) finding a violation by PIKA Sp. z o.o. with headquarters in Gdańsk at ul. Paratroopers 7 Art. 32 sec. 1 and 2 and article. 32 sec. 1 and 2 in connection with Art. 28 sec. 3 lit. c) and f) of the Regulation of the European Parliament and of the EU Council 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46 / EC (general regulation on data protection) (Journal of Laws UE L 119 of May 4, 2016, p. 1, Journal of Laws UE L 127 of May 23, 2018, p. 2 and EU Official Journal L 74 of March 4, 2021, p. 35), hereinafter: "Regulation 2016/679", consisting in failure to implement appropriate technical and organizational measures ensuring the security of personal data, including ensuring their confidentiality, is imposed on PIKA Sp. z o.o. with headquarters in Gdańsk at ul. Paratroopers 7 an administrative fine of PLN 250,135 (in words: two hundred fifty thousand one hundred and thirty five PLN),

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

JUSTIFICATION

Fortum Marketing and Sales Polska S.A. based in Gdańsk (hereinafter also referred to as: "Fortum" or the "Administrator") conducts business in the field of electricity and gas fuel trading, including the sale of electricity and gas to end users, both in the business sector and households . As part of its business activities, Fortum cooperates with PIKA Spółka z o.o. based in Gdańsk at ul. Parochroniarzy 7 (hereinafter: "PIKA" or "Processing Entity"). PIKA provides Fortum with an archive management service, including a digital archive. The parties are bound by the contract for entrusting the processing of personal data of [...] May 2018 and the contract for storage (archive of documents) with accompanying services of [...] February 2016 with subsequent annexes.

On [...] April 2020, Fortum Marketing and Sales Polska Spółka Akcyjna notified the President of the Personal Data Protection Office (hereinafter also referred to as the "President of the Personal Data Protection Office") of a breach of personal data protection, which was registered under the number DKN.5130.2215.2020. The notification of violation indicated that the data of the Administrator's clients was "copied", and the event was related to the fact that a change was introduced in the ICT environment for the [...] service (a system that functions as a digital archive of documents and information about customers, derived from the processing of paper media to electronic) in order to increase the efficiency of the entire repository. The change was made by the processor, ie PIKA, following the Administrator's notification of the slow operation of the service [...]

of which the Processor was the supplier. The change consisted in the creation and installation of an additional Fortum customer database (which was then copied by unauthorized entities), operating on the basis of the […] solution. The breach of confidentiality concerned the newly created database containing information about Fortum's customers in the scope of: name and surname, address of residence or stay, PESEL number, type, series and number of an identity document, e-mail address, telephone number, number and address of the collection point and data concerning contract (eg contract date and number, fuel type, meter number), identified by Fortum on the application as "secondary, secondary, back-up metadata database named […]". The notification indicated that the breach concerned the personal data of 137,314 people of Fortum's customers. The administrator resigned from notifying data subjects about the breach of personal data protection, as in his opinion there was no high risk of violating the rights or freedoms of natural persons.

[...] On April 2020, Fortum sent to the President of UODO a notification about the possibility of committing a crime, which was submitted by Fortum to the District Prosecutor's Office in Gdańsk. In the justification of the notification, Fortum indicated the possibility of committing the prohibited act specified in Art. 267 of the Act of 6 June 1997 Penal Code (Journal of Laws of 2020, item 144, as amended), i.e. obtaining illegal access to information in connection with unauthorized copying of the customer database.

Due to the fact that Fortum did not notify the persons affected by the infringement about the infringement, and in the opinion of the President of the Personal Data Protection Office, due to the wide scope of the disclosed data of Fortum's customers, there was a high risk of infringement of the rights or freedoms of natural persons, the President of the Personal Data Protection Office on [...] April 2020 r. addressed an application to the Administrator, in which he asked to take appropriate actions aimed at: 1) immediately notifying data subjects about the breach of their personal data, 2) providing these persons with recommendations to minimize the potential negative effects of the breach, 3) elimination of similar irregularities in the future.

The answer to the above-mentioned the statement of the President of the Personal Data Protection Office was sent by Fortum in a letter of [...] May 2020. The administrator informed the supervisory authority about notifying the persons affected by the infringement, presenting the content of the communication sent to customers before receiving the request of the supervisory authority, as well as the content of the supplemented notification of infringement sent to clients in connection with the request of the President of the Personal Data Protection Office. In this letter, Fortum also presented the results of the analysis, which finally determined the number of persons who should be notified about the breach of personal data protection due to the high

risk of violating the rights or freedoms of natural persons. The explanations indicated that the data of a total of 120,428 people were disclosed, of which 95,711 people had to be notified of the violation. The remainder are business clients and deceased persons.

At the same time, on [...] April 2020, the President of the Personal Data Protection Office (UODO) initiated ex officio administrative proceedings regarding the possibility of Fortum violating Art. 5 sec. 1 lit. f), art. 24 sec. 1, art. 25 sec. 1, art. 32 sec. 1 and 2 and article. 34 sec. 1 of the Regulation 2016/679, in connection with the breach of personal data protection registered under reference number DKN.5130.2215.2020.

When initiating administrative proceedings, the President of the Personal Data Protection Office called on Fortum to indicate, inter alia, the final categories of personal data and categories of data subjects and an indication of the detailed, including technical, description of the breach. The President of the Personal Data Protection Office also called on Fortum to indicate whether and which Fortum and the Processing Entity had adopted technical and organizational security measures in accordance with Art. 24 of Regulation 2016/679 (data protection policy), art. 25 of Regulation 2016/679 (taking into account data protection by design and data protection by default) and art. 32 of Regulation 2016/679, as well as indication of whether, and if so, when and how the Controller and the Processing Entity regularly tested, measure and assess the effectiveness of technical and organizational measures to ensure the security of personal data processed in the IT systems affected by the breach .

In response to the notification about the initiation of administrative proceedings in this case, by letter of [...] May 2020, Fortum sent additional explanations, in which it indicated, inter alia, that: 1. The categories of data affected by the breach indicated in the notification include: name and surname, address of residence or stay, PESEL number, type, series and number of the identity document, e-mail address, telephone number, number and address of the collection point, and contract data (e.g. date and contract number, fuel type, meter number). As explained by Fortum, the above scope of data results from the structure of the database affected by the infringement. At the same time, Fortum stated that not all fields contained values (they were filled in). Thus, for one person, the personal data contained in the database may be limited to the name and surname, contract number and PESEL number, and for another, it may include all the above-mentioned data. categories of personal data 2. The vulnerability that led to unauthorized access to the additional database created on the basis of the solution […] was detected after two independent Internet users informed them that they had access to Fortum's customer base.3. The breach occurred

as a result of the action of the Processing Entity performing the service for the Administrator [...], i.e. PIKA Fortum explained that upon identifying the system whose data was exposed, it informed the service provider (i.e. PIKA), who immediately turned off the system and blocked access. 4. When describing how the infringement took place, Fortum indicated, inter alia, that it was related to the fact that a programming change was introduced in the IT environment for the service [...]. The change consisted in adding to the [...] environment an additional computer (database server) for the database running on the [...] solution in order to improve the document search efficiency. It was supposed to significantly shorten the time during which information from the system [...] is available to the end user. Fortum pointed out that such a solution significantly speeds up the search for documents and is a popular solution in this type of service. 5. The introduced modifications and the manner of their introduction have not been consulted by the Processing Entity. In its explanations, Fortum indicated that it cooperates with the Processor on the basis of a storage agreement (document archive) with accompanying services concluded in 2016 (with subsequent annexes) and a contract for entrusting the processing of personal data concluded on [...] May 2018, which set out the requirements in the scope of personal data security to be applied by the Processing Entity, including pseudonymization and encryption of personal data. According to Fortum's assessment, these requirements were not met by the Processor in the case of the implemented modification in the [...] service.

In connection with the explanations provided by Fortum in response to the notification of the initiation of administrative proceedings, in a letter of [...] May 2020, the President of UODO asked her to provide additional information and indicate, inter alia, whether, and if so, when and what verification procedures of the Processor, in terms of its compliance with the requirements of Regulation 2016/679, it carried out before concluding a data processing agreement with this entity and whether, beyond the planned control of all processors, it exercised the right of control, referred to in Art. 28 sec. 3 lit. h) of Regulation 2016/679, in terms of PIKA's provision of the measures required under Art. 32 of Regulation 2016/679. The President of the Personal Data Protection Office also asked for an explanation as to how, in Fortum's opinion, a modification should be made to speed up the search for documents in the system [...].

In response, in a letter of [...] June 2020, Fortum explained that prior to the conclusion of the contract for entrusting the processing of personal data, it had not carried out additional verification of the Processor. As indicated in the explanations, “Fortum cooperates with PIKA. Sp. z o.o. for many years and so far there have been no security incidents. In addition, PIKA is a market leader in the field of services provided and represents a high standard in the field of archiving and digitization. The

administrator considered it sufficient to sign a contract for entrusting the processing of personal data along with the arrangements indicated in the Annex. "

Fortum also indicated that it had not yet exercised the right of control referred to in Art. 28 sec. 3 lit. h) of Regulation 2016/679, in terms of PIKA's provision of the measures required under Art. 32 of Regulation 2016/679. After finding a breach of personal data security, on [...] May 2020, the Administrator sent to the Processor a previously prepared questionnaire for the processor, which is the first element of the process of verification of processors.

Fortum also explained how, in its opinion, the process of implementing changes to the system by a processor aimed at improving the operation of the service [...] should look like. The administrator indicated that in his opinion, the application of a specific solution aimed at accelerating the search for documentation in the system [...] should be preceded by an analysis taking into account both the benefits and potential threats resulting from a specific, planned solution. When analyzing potential threats, the service provider should analyze the risk of implementing such a solution and prepare a detailed plan to secure the operations performed. Fortum indicated that it did not receive the results of the risk analysis and alternative solutions to choose from. A unilateral decision to apply the implemented solution was made by the Processor itself, and moreover, it did not provide any detailed analysis justifying the selected technical solution. The administrator also argued that in the previous practice of introducing changes to Fortum systems by the Processor, such changes were introduced according to a previously agreed work plan, tested by Fortum in a test environment and only then implemented for production.

The administrator also provided a copy of the procedures implemented at PIKA, which he referred to in the reply of [...] May 2020, i.e. "Policy [...]", "Instruction [...]", "Analysis [...]" and "Principles […] ". A list of internal inspections performed by PIKA and external inspections carried out at PIKA by its contractors other than Fortum was also presented, which is attached as Appendix 5 to Fortum's letter of [...] June 2020, and reports on the last two safety and personal data protection inspections carried out by PIKA before the infringement, which constitute Appendix 6 to the above-mentioned Administrator's letters.

In connection with the reply provided in the letter of [...] June 2020, in the letter of [...] June 2020, the President of the Personal Data Protection Office asked Fortum to submit further explanations, inter alia, in the scope of indicating when the Administrator cooperates with PIKA and indicating whether (and if so, when and what content) the Processor, from the moment of concluding the contract with Fortum, under point 3.4.3 of the data processing agreement of [...] May 2018 (Annex 7 to the response to the initiation of the administrative procedure of [...] May 2020), sent notifications to the Administrator of any

changes that may affect data protection or security with regard to personal data processed by Fortum. Moreover, the President of the Personal Data Protection Office (UODO) requested additional information to confirm both the number and effectiveness of the notification of the breach by the Administrator of the data subjects.

By letter of [...] June 2020, Fortum provided additional explanations regarding the determination of the manner and number of persons notified about the breach of their personal data. In addition, the Administrator presented the content of the correspondence of [...] April 2020, in which the need to make changes to the system [...] was reported due to its slow operation.

Fortum also indicated in its explanations that the need to introduce changes had been notified to the Processing Entity many times earlier, due to the slow operation of the system [...]. The administrator also indicated that in Annex 2 "[...]" to the storage agreement with accompanying services of [...] February 2016, point 1.3. Describes the procedure for implementing changes to the system. In the described case, the aforementioned procedure was not followed by PIKA. The processor did not provide the Administrator with the concept of changes or functional and technical designs. According to Fortum's statement, if it had received guidance from PIKA early enough, it would have been possible to react to the potential threat associated with the use of a specific solution to solve the problem with the slow operation of the system [...].

Due to the fact that the findings made so far in the course of the proceedings indicate that PIKA is also involved in the processing of personal data covered by the breach of personal data protection reported by Fortum, the President of the Personal Data Protection Office decided that the proceedings also apply to PIKA's obligations as a processor, entrusted by Fortum with the processing of the personal data of the affected persons. By letter of [...] July 2020, the President of UODO notified PIKA that she was considered a party to the proceedings, in accordance with Art. 28 of the Code of Civil Procedure while pointing out that the proceedings also concern the possibility of violating also Art. 28 sec. 1 and 3 of Regulation 2016/679.

The President of the Personal Data Protection Office, pursuant to art. 58 sec. 1 lit. a) and e) of Regulation 2016/679 called on PIKA to provide explanations and indicate, inter alia: 1. Who, when and what actions were taken to implement changes in the IT system [...] (installation of the solution [...]) in response to problems related to the performance of this system reported by the Administrator. 2. What procedures has been adopted by PIKA regarding the introduction of changes to IT systems provided to data controllers in response to the demand signaled by them 3. Did PIKA undertake verification activities in terms

of the security of the IT environment that was modified, if so, what were the measures and when were they taken, and if not, why 4. Indication of whether, and if so, when and how PIKA regularly tested, measured and assessed the effectiveness of technical and organizational measures to ensure the security of personal data processed in the IT systems affected by the breach, in particular, if and what technical measures and organizational planning has been planned by the Processing Entity for the IT system modification process [...] and whether it has assessed the effectiveness of these measures.

In response from [...] August 2020, PIKA indicated that its actions were taken in connection with Fortum's request to resolve the poor performance of the repository [...] causing extended operational service time for Fortum's customers.

As explained by PIKA, after an internal analysis of the application, a recommendation was developed along with a proposal to solve the performance problem [...], which was submitted to Fortum for approval. After receiving approval from Fortum, the PIKA IT Systems Development Department began implementing the changes. The first stage of implementing the changes for Fortum was the creation and configuration of a new virtual server and the installation of the software […]. As indicated in the explanations of [...] August 2020, this task was delegated to a person with appropriate qualifications, and one of the technical aspects of the task implementation was to establish secure communication of the new server with other ICT elements of the entire Fortum environment in such a way that the transmission / access only the appropriate application had to use the data.

As explained by PIKA., After creating and configuring the server and installing the […] software on it, another task was started as part of the implementation of the change for Fortum, ie the new database operating on the basis of the […] solution was started to supply Fortum customers with data. On [...] April 2020, Fortum received an e-mail information from the Head of the Design and Implementation Department of PIKA about the testing of the new functionality and the possibility of final validation before the production launch of the above-mentioned changes.

In response to the question about the procedures for introducing changes to the IT systems provided to data administrators in response to the demand signaled by them, PIKA indicated that the basic and therefore binding document regulating its IT areas is the "Instruction [...]". However, when it comes to introducing changes to PIKA systems, individual Departments of the IT Division are required to record all changes made to the systems in internal systems supporting project management and their control. The main tools are: a) project and change management […], b) documentation system […], c) repository management system […]. As indicated by PIKA, tasks to be performed are registered in the above-mentioned systems, which are then assigned for implementation by specific engineers employed by PIKA. Access to the systems and servers on which

these systems operate takes place on the general principles set out in the "Manual [...]".

Explaining whether verification activities were undertaken in terms of the security of the IT environment that had been modified, PIKA indicated that the implemented change for Fortum was at the stage of testing completion - before the final validation by Fortum, and thus before implementation into production and final implementation of system security and a new database based on the solution […].

The production implementation phase and the completion of security implementation were planned for the period from [...] - [...] April 2020. At the time of finding a personal data breach of Fortum's customers, based on information provided by Fortum on [...] April 2020, the changes aimed at improving the operation of the system [...] were still under implementation (i.e. the stage of synchronization of the subsystem based on the solution [...] with the current environment [...]), thus the works performed by PIKA were not fully completed - the process of testing and feeding the newly created database was ongoing.

By letter of [...] April 2021, being a response to the request of the President of the Personal Data Protection Office of [...] March 2021, in the scope of indicating, inter alia, evidence of consultation between the Administrator and the Processor on the implementation of changes to the software that was the subject of the breach, PIKA indicated, inter alia, that Fortum did not consult PIKA on the implementation of software changes. The Processor further submitted that Fortum had reported a problem in the operation of the software [...] and expected it to be resolved. Knowing the technical reason, PIKA proceeded to solve the problem, and Fortum did not "consult the technical method and details of changes in the software in this case".

By letters of [...] July 2021, PIKA and Fortum were informed that the proceedings had been extended to include the possibility that Fortum, as a data controller, would breach its obligations under Art. 28 sec. 1 and art. 28 sec. 3 of the Regulation 2016/679.

By letter of [...] September 2021, Fortum supplemented the previously presented materials with additional explanations, according to which it commissioned an external entity to analyze the "incident" and provide recommendations in order to minimize the risk of a repeat incident of a similar nature. As explained by Fortum in the above-mentioned in a letter of [...] September 2021, on the basis of the presented recommendations, modifications were made to both the technical infrastructure and additional elements of approval and confirmation of the "modernization works in the application production environment" were introduced. The letter was also accompanied by a report on the data leakage monitoring conducted for the period from [...] June 2020 to [...] August 2020, according to which no data about Fortum customers whose confidentiality was breached in

the Internet and Darknet appeared in the result of the event of [...] April 2020.

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 violation of the rights or freedoms of natural persons of varying probability and seriousness, the controller implements appropriate technical and organizational measures for the processing to be carried out 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) Regulation 2016/679. The implementation of technical and organizational measures should rely on the administrator implementing relevant provisions, rules for the processing of personal data in a given organization, but also regular reviews of these measures, and, if necessary, updating previously adopted safeguards. The principle of integrity and confidentiality, expressed in art. 5 sec. 1 lit. f) Regulation 2016/679, in addition to the above-mentioned Art. 24 sec. 1 of Regulation 2016/679, also specify other provisions of this legal act, i.e. Art. 25 sec. 1 and art. 32 sec. 1 and 2.

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 violating 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.

From the content of art. 32 sec. 1 of Regulation 2016/679 shows that the administrator is obliged to apply technical and organizational measures corresponding to the risk of violating the rights and freedoms of natural persons with a different probability of occurrence and the severity of the threat. The provision specifies that when deciding on technical and

organizational measures, the state of technical knowledge, implementation cost, nature, scope, context and purposes of processing as well as the risk of violating the rights or freedoms of natural persons with different probability and severity should be taken into account. It follows from the above-mentioned provision that the determination of appropriate technical and organizational measures is a two-stage process. First of all, it is important to determine the level of risk related to the processing of personal data, taking into account the criteria set out 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. These arrangements, where applicable, in accordance with lit. b) and d) of this Article, should include measures such as the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services, and regular testing, measurement and evaluation of the effectiveness of technical and organizational measures to ensure the security of processing.

Art. 32 sec. 2 of Regulation 2016/679 provides that 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.

It should be pointed out that the basic security measure aimed at protecting against unauthorized access to personal data is the establishment of appropriate security measures for databases and IT systems used to process personal data. Providing access to authorized users and preventing unauthorized access to systems and services is one of the standard security elements, which is indicated, among others, by PN-EN ISO / IEC 27001: 2017-06 standard. According to Art. 32 sec. 1 of Regulation 2016/679, one of the factors to be taken into account when selecting the appropriate technical and organizational measures is the state of technical knowledge, which should be assessed taking into account market conditions, in particular the availability and market acceptability of a given technical solution. Guidelines specifying this subject are provided by the applicable standards and norms, in particular ISO standards, which are also subject to constant reviews and changes conditioned by technological progress.

In accordance with the PN-EN ISO / IEC 27002: 2017-06 standard, it is recommended to avoid the use of data containing data identifying a person or other confidential data as test data. If personal identification data is used in testing, it is advisable to protect all sensitive details and context by deleting or modifying them. Above the standard allows the use of real data for testing purposes, but these data should be subject to special protection. First of all, when real data is used for testing

purposes, the same access control procedures should be used in the tested applications as those used in production systems. Art. 32 sec. 1 lit. a) of Regulation 2016/679 indicates the pseudonymisation of personal data as a mechanism that can guarantee an adequate level of data security, and from recital 29 of Regulation 2016/679 it follows that pseudonymisation of personal data may reduce the risk for data subjects and help controllers and processors to fulfill their data protection obligation. At the same time, it was noted that the introduction of pseudonymisation does not serve to exclude other data protection measures. It should also be noted that pseudonymization is also mentioned in Art. 25 sec. 1 of Regulation 2016/679, which requires the data controller to implement appropriate technical and organizational measures both at the stage of determining the processing methods and during the processing itself. Therefore, both Regulation 2016/679 and good practices specified in ISO standards indicate to controllers and processors possible solutions that may be applied by them when making changes to IT systems in which personal data are processed. It should be emphasized that pseudonymisation of data is an effective security measure to ensure data confidentiality. An unauthorized person who came into possession of pseudonymised data, e.g. as a result of a breach of personal data protection, is not able to assign them to a specific person without having additional information about that person. However, neither the Administrator nor the Processor used this solution when deciding, as part of introducing changes to the [...] service, to supply the newly created database based on the solution [...] with actual personal data of Fortum's customers, which, in combination with the lack of using other effective security measures, as described below, led to a breach of personal data protection, which resulted in a breach of the confidentiality of more than 95,000 data. people.

In complex explanations, PIKA indicated that "each system created based on [...], on which PIKA solutions are built, is subject to the implementation of the so-called "Hardening", involving, inter alia, on implementing […]. Systems PIKA Sp. z o.o. are monitored 24/7 with host and network monitoring tools. (...). The machine with the [...] application was in the process of being implemented, so not all of the above-mentioned functionalities were implemented at the moment of the event ". As indicated by PIKA in its explanations of [...] August 2020, at the moment of finding a personal data breach of Fortum's customers, based on the information provided by it on [...] April 2020, changes aimed at improving the operation of the system [.. .] were still in the process of implementation (ie the synchronization stage), thus the work performed by PIKA was not fully completed - the process of testing and database supply was in progress.

In the explanations of [...] August 2020, PIKA also informed that the order to create a server for the base operating on the

basis of the solution [...] was transferred to a person with appropriate qualifications, the order also indicated that the implementation of the transmission security postulate is performed by an appropriate configuration [...], which was also indicated in the content of the internal order (Annex 4 to the above-mentioned explanations by PIKA). However, the analysis of the content of the indicated order does not confirm the explanations of PIKA. The presented documentation does not contain any evidence that the configuration was commissioned [...]. It is only an order to create a virtual server with the […] application. The order does not explicitly require to configure […]. PIKA did not provide any evidence that it had verified the correctness of the execution of the order. The verification of the execution of this order was also not verified by the Administrator. It should be noted that as the cause of the breach of personal data protection, PIKA indicated an error in the initial configuration of the new server consisting in [...].

As indicated, among others, by PN-EN ISO / IEC 27001: 2017-06 standard, safety functions should be tested during development works. In the facts of the case at hand, PIKA received a report of incorrect (slow) operation of the system [...]. In connection with the above-mentioned with the application, it started working on the implementation of the changes. It entrusted one person with the creation of a new server based on the […] solution, and then started feeding the database with real data from Fortum's customers. Despite the fact that the newly created database was supplied with actual personal data, at the stage of development works, PIKA did not test the security functions, which consequently led to a breach of the confidentiality of personal data of over 95,000 clients of the Administrator, in the case of which, due to the scope of the data disclosed, the risk of the violation of the rights or freedoms of natural persons in connection with the violation of the protection of personal data was high.

Explaining in the course of the proceedings what are the procedures for introducing changes to IT systems provided to data controllers in response to the demand signaled by them, PIKA indicated that it has specific policies and procedures for actions to introduce changes in IT systems, and basic documents in this regard are: "Instruction [...]", "Policy [...]", "Principles [...]" and "Principles [...]". In the event of changes to the systems, as explained by PIKA, individual departments of the IT department are required to record all changes made to the systems in internal systems supporting project management and their control. The main tools are: a) project and change management system […], b) documentation system […], c) repository management system […]. The order for Fortum was submitted in the […] system, as proof of which PIKA provided appropriate printouts from this system. The analysis of the "Instructions [...]" and "Policy [...]" showed that these documents do not contain detailed

provisions on how to make changes to IT systems used to process personal data, e.g. the need to create a test environment or adequate protection of actual data of the administrator's clients, if they are used to test the introduced changes, or the rules for controlling the correctness of the implementation of individual stages of the project. On the other hand, the presented printouts from the […] system are in fact orders for performing specific activities. On their basis, it is impossible to confirm that the implemented changes were implemented in accordance with predetermined rules ensuring the security of personal data. In the opinion of the President of the Personal Data Protection Office, the recording of work carried out for the benefit of the Processor's contractors in internal project management support systems cannot be considered a sufficient measure ensuring the security of personal data processing, as the various stages of implementing changes are not sufficiently documented. This may lead to the freedom to choose the solutions used, or, as in the case at hand, not to define all the required safeguards, which consequently led to a breach of personal data protection. In the content of the Policy [...] referred to by PIKA, however, it was indicated that "the following standards apply as supplementary requirements: a. ISO / IEC 27001 - Information technology - Security techniques - Information security management systems - Requirements, b. ISO / IEC 27002 - Information technology - Security techniques ". In connection with the above, in the absence of detailed provisions in PIKA's internal procedures regarding the method of introducing changes to IT systems, these changes should be made in accordance with the best practices specified in the above-mentioned ISO standards, which, as has been shown above, was not carried out in the event of changes to the system [...], resulting in the possibility of unauthorized entities to collect personal data, the administrator of which is Fortum.

In the actual state of the case, the breach of personal data protection (data leakage) occurred as a result of an error of one employee of the Processing Entity who, in his opinion, is appropriately qualified to perform this task, who by configuring a new server operating on the basis of the solution [...], not [...], as a consequence, a secure communication channel was not ensured between Fortum's servers used to process personal data.

In the opinion of the President of the Personal Data Protection Office, the technical and organizational measures applied by PIKA met the requirements specified in Art. 32 sec. 1 and 2 of Regulation 2016/679. The steps of implementing changes to Fortum's reported service performance problem [...] did not follow strictly defined procedures. During the process of making changes to the system, actual personal data of the Administrator's customers were used, and the effectiveness of the security measures applied was not verified before the changes to the above-mentioned changes were submitted to Fortum. system to

solve the problem with its performance. The safety functions were not tested during the work carried out for this purpose. In breach of the above-mentioned obligations under Art. 32 sec. 1 and 2 of Regulation 2016/679 and acting contrary to the above. ISO standards, PIKA acted against the provisions of its own "Policy [...]", which refers to these standards. PIKA also acted against the contract for entrusting the processing of personal data, in which it undertook, inter alia, to implement pseudonymization of data. In specifying the security measures it will apply to protect personal data, PIKA disregarded, in particular, the above-mentioned provision of Regulation 2016/679, the obligation to take into account the state of technical knowledge when defining them. As the doctrine indicates, “The need to take into account the state of technical knowledge can be understood as the need to apply measures that reflect the current security standards. This requirement can be read as the need to apply solutions currently considered effective, but not to use outdated solutions, commonly assessed as not ensuring security "(Fajgielski Paweł, Commentary to the Regulation No. 2016/679 on the protection of individuals with regard to the processing of personal data and on free movement of such data and repealing Directive 95/46 / EC (General Data Protection Regulation), [in:] General Data Protection Regulation. Personal Data Protection Act. Comment). There is no doubt that the current security standards are set, among others, by ISO standards. Consequently, it should be considered that PIKA has not applied appropriate technical and organizational measures to ensure the security of the personal data of the Administrator's clients being processed, in particular with regard to the use of actual data of the above-mentioned persons for the purposes of making changes to the system [...] without pseudonymising them and against the principles resulting from ISO standards, to which it refers in its internal documentation on the protection of personal data.

The processing entity failing to meet the requirements set out in the provisions of art. 32 sec. 1 and 2 of Regulation 2016/679, which has already been demonstrated above, he did not take actions under Art. 28 sec. 3 lit. c) and f) of Regulation 2016/679, pursuant to which the processor takes all measures required under Art. 32 and taking into account the nature of the processing and the information available to him, helps the controller to fulfill the obligations set out in art. 32–36.

According to the material collected in the course of the administrative procedure, it should be reiterated that the Processing Entity started its activities as a result of the Administrator's notification regarding the slow operation of the digital archive. After conducting an internal analysis of the increase in system performance, he commissioned the creation of a new server for a database based on the […] solution for Fortum. After creating the indicated solution, he did not verify whether the appropriate configuration was made [...], which was to ensure the security of data transmission of the new server with other ICT elements

of the entire Fortum environment used to process personal data. Then, he fed the newly created database with actual personal data of the Administrator's clients. Due to the fact that the change implemented for Fortum was in the process of being implemented, not all security measures applied by the processor to ensure the security of data processing were implemented at the time of the event causing a personal data breach. Therefore, there is no doubt that the Processor did not exercise due diligence in its conduct in this regard, which in turn proves that, when carrying out the order for Fortum, it did not take all measures required under Art. 32 of Regulation 2016/679 and did not help the Administrator to fulfill the obligation specified in this provision.

As part of the security measures applied, the administrator, in turn, indicates the storage agreement between him and PIKA along with accompanying services of [...] February 2016, where, according to his explanations, in Annex No. 2 "[...]" to the above-mentioned of the agreement, in point 1.3. describes the procedure for implementing changes to the system. At the same time, the Administrator argued that the procedure was not applied by PIKA in the case in question. The Processing Entity did not provide the Administrator with the concept of changes or functional and technical designs. It should be noted, however, that in accordance with the Annex 2 to the contract, referred to by Fortum, the development of the abovementioned documentation regarding changes in the systems is prepared by the Processing Entity at the request of the Administrator. The administrator, however, did not provide documentation that would indicate that it required the Processor to present such documentation in relation to the changes introduced in the service [...], which resulted in a breach of personal data protection.

Fortum additionally indicated that the practice of the Administrator's IT area (based on [...]), for the implemented implementations, requires the involvement of an application system engineer in such consultations, who accepts the proposals within his / her powers or submits for verification to appropriate internal IT services. As Fortum pointed out in its explanations, at least to protect the interests of the Administrator and the Processor, the work plan presented as part of the implementation should be approved and then followed, leading to the approval of the acceptance tests. Only after their approval by a system engineer, any modification can be introduced productionally, and thus made available to the Administrator's employees.

It should be emphasized that the Administrator, despite the procedures in place and knowledge of how, in accordance with commonly used practices, the implementation of changes in IT systems should proceed, at no stage of implementation has supervised whether the implementation actually takes place in accordance with generally applicable standards, data processing entrustment agreement. personal data or a storage agreement (document archive) with accompanying services.

The presented documentation shows that on [...] April 2020, the Administrator reported to the Processor the need to improve the operation of the digital archive [...]. After receiving information on the implementation of the new solution on [...] April 2020, the Administrator informed that the system is currently working properly, and any comments will be forwarded to PIKA after "extended testing".

Responding to the inquiry of the President of the Personal Data Protection Office regarding regular testing, measurement and evaluation of the effectiveness of technical and organizational measures to ensure the security of the processed personal data in the IT systems affected by the breach, Fortum indicated that "taking into account the cause and nature of the incident, according to the Administrator, regular testing, measuring and evaluating the effectiveness of technical and organizational measures to ensure the security of the processed data would not prevent a breach that took place and resulted from the implementation of a one-off modification ".

It should be emphasized that under Art. 32 sec. 1 lit. d) of Regulation 2016/679 results in the obligation to regularly test, measure and evaluate the effectiveness of technical and organizational measures to ensure the security of processing. Conducting reviews and updating of implemented solutions are also a requirement formulated directly in Art. 24 sec. 1 of the Regulation 2016/679, as well as resulting from art. 25 sec. 1 of Regulation 2016/679, creating an obligation to ensure privacy protection in the design phase (privacy by design) and obliging the controller to implement appropriate technical measures both at the stage of determining the processing methods and at the stage of the processing itself. The administrator's implementation of technical and organizational measures is not a one-off activity, but should take the form of a process where the administrator reviews and, if necessary, updates the previously adopted security measures. Consequently, one cannot agree with Fortum's statement that testing, measuring and evaluating the effectiveness of technical and organizational measures to ensure the security of the processed data would not prevent a breach in this case, because such an evaluation should be applied not only to technical but also organizational measures, i.e. procedures implemented by the Administrator regarding the processing of personal data, including procedures for making changes to IT systems used to process personal data. Regular evaluation of the above-mentioned procedures, as required by Art. 32 sec. 1 lit. d) of Regulation 2016/679, would allow the Administrator to verify whether such a procedure is effective, i.e. whether it ensures that appropriate measures are taken to ensure the protection of personal data during the process of making changes to the IT system, whether it is complied with at all by persons responsible for carrying out these changes, as well as identifying any gaps in it. It should be

emphasized once again that regular testing, measurement and evaluation of the effectiveness of technical and organizational measures to ensure the security of the processed data, including the procedures used, also serves to ensure the fulfillment of the Administrator's obligation referred to in art. 25 sec. 1 of Regulation 2016/679, i.e. ensuring that the protection of personal data is taken into account, inter alia, in the design phase, which also applies to any changes made to the IT systems used to process personal data.

In the factual state of the case, in the opinion of the President of the Personal Data Protection Office, verification by the Controller of the manner in which the Processor implements changes aimed at improving the operation of the system processing personal data ([...]), in accordance with the procedure adopted by Fortum, would significantly reduce the risk of gaining access by unauthorized persons to the data processed in this system, and thus would minimize the risk of violating the rights or freedoms of natural persons whose data is processed by Fortum, because the breach of personal data protection occurred as a result of a simple error consisting in failure to apply the basic security measure, which is the establishment of [...] to ensure secure communication, which should be tested and detected during the process of implementing changes to the IT system processing personal data. The Administrator's compliance with this procedure would undoubtedly also allow him to state that in the process of making changes to the system [...] the actual personal data of Fortum's clients were used by PIKA (without pseudonymisation), which, in view of the failure to apply other effective security measures, as mentioned above, may mean a high risk of violation of the rights or freedoms of these persons in the event of a breach of personal data protection (which actually took place). As a result of the above, Fortum did not act to ensure the security of its customers' personal data, which it was required to do in accordance with the above-mentioned provisions of Regulation 2016/679 as the data controller.

It should also be emphasized that Fortum is not exempt from the fulfillment of these obligations by using the services of a processor. Responsibilities in this respect rest primarily with the data controller. By analyzing the actions, and the actual lack of actions of the Administrator in this regard, it can be concluded that it was more important for him to increase the efficiency of the system [...] as quickly as possible than to ensure an adequate level of security of personal data processed using this system.

It should be emphasized that the Administrator indicated in the course of the proceedings that in the current practice of the Processor introducing changes to Fortum systems, such changes were introduced according to a previously agreed work plan, tested by Fortum in a test environment and only then implemented for production. In the storage agreement between the

parties with accompanying services of [...] February 2016, the Administrator also ensured itself the possibility of requesting changes in IT systems, presentation by the Processor of the concept of these changes as well as functional and technical designs. In the event of making changes to the system that led to the infringement being the subject of the proceedings, the Administrator contented himself only with notifying the Processing Entity of the need to make modifications, not requesting any drafts of these changes or taking any actions to verify or in the process of making changes in the the system ensures the security of personal data processing of its clients.

The material collected in the case also confirms that, prior to the initiation of administrative proceedings, the Administrator did not carry out audits, including inspections, at the processor to verify that PIKA correctly fulfills its obligations under Regulation 2016/679. The possibility of carrying out such audits, including inspections, results from Art. 28 sec. 3 lit. h) Regulation 2016/679, pursuant to which the contract for entrusting the processing of personal data is to provide that the processor provides the administrator with all information necessary to demonstrate compliance with the obligations set out in this article and allows the administrator or auditor authorized by the administrator to carry out audits, including inspections, and contributes to them. Therefore, this provision gives the administrator certain tools, the use of which can ensure that the processing of data subject to entrustment will be in accordance with the provisions of Regulation 2016/679, and the administrator will avoid liability for their violation. It should be emphasized that the performance of audits by the controller in the processor, including inspections, should be treated as one of the most important security measures to be applied by the controller in order to properly fulfill its obligations under Art. 32 sec. 1 of Regulation 2016/679. The controller should have knowledge of whether and how the entity entrusted with the processing of personal data meets the requirements set out in Regulation 2016/679 when using the services of the processor. There is no doubt that the most effective way for the controller to ensure this knowledge is to carry out appropriate audits, including inspections, on the processor. However, Fortum did not apply such security measures, which in turn contributed to a breach of personal data protection. Moreover, the use of the above-mentioned funds is related to the obligation of the data controller under Art. 28 sec. 1 of Regulation 2016/679, which means that its implementation is also to confirm whether the processor continues to guarantee 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.

Failure to carry out audits, including inspections, in the processing entity also means a violation of the provision of art. 25 sec.

1 of Regulation 2016/679. This provision obliges to implement appropriate technical and organizational measures, not only when specifying the methods of processing, but also during the processing itself. Continuity, inscribed in the analyzed obligation, may in practice manifest itself, inter alia, in in the need to ensure regular monitoring of the applied safeguards and to conduct constant supervision over the processor through, for example, audits and inspections referred to in art. 28 sec. 3 lit. h) Regulation 2016/679.

In the opinion of the President of the Personal Data Protection Office, the technical and organizational measures applied by Fortum only to a very limited extent met the requirements specified in Art. 32 of Regulation 2016/679, due to the fact that Fortum did not enforce PIKA's performance of the provisions connecting their agreements, did not adhere to its own practice of implementing changes in the IT environment based on internal regulations and did not verify the Processor in the scope of activities aimed at improving the operation of the service [...]. It should be emphasized that ensuring the supervision and monitoring of development works on systems commissioned by external entities by the data controller is one of the basic organizational measures that should be effectively implemented by the controller in order to ensure the security of personal data in accordance with the requirements of Regulation 2016/679, in in particular when these works use, instead of test (fictitious) data, actual personal data of its clients (without subjecting them to pseudonymization) and a model security element, which is indicated, inter alia, by PN-EN ISO / IEC 27001: 2017-06 standard. As a consequence of Fortum's failure to apply the above principles, foreseeable risks have not been adequately minimized and limited in time to processing. It should be recognized that the application of appropriate security standards with regard to introducing changes to IT systems used to process personal data, including their verification in terms of security, and in particular meeting the requirements under Art. 24 sec. 1, art. 25 sec. 1 and art. 32 sec. 1 and 2 of Regulation 2016/679, as well as effective verification of the Processor's actions in this respect, would significantly reduce the risk of unauthorized access to the personal data of the Administrator's clients, and thus minimize the risk of violating the rights or freedoms of natural persons whose data is provided by the Administrator processed, i.e. making data available to unauthorized recipients.

At this point, reference should be made to the judgment of the Provincial Administrative Court in Warsaw of August 26, 2020, file ref. II SA / Wa 2826/19, in which the Court indicated that "The measures adopted are to be effective (...)" and "(...) technical and organizational activities are the responsibility of the personal data administrator, but cannot be selected in a manner completely free and voluntary, without taking into account the degree of risk and the nature of the personal data protected. ",

as well as the judgment of this court of January 19, 2021, file ref. II SA / Wa 702/20 that "Personal data should be processed in a manner ensuring appropriate security and confidentiality, including protection against unauthorized access to them and equipment used for their processing and against unauthorized use of these data and equipment (recital 39 of Regulation 2016/679) ".

Therefore, the findings do not provide a basis for stating that the technical and organizational measures used by the Administrator and the Processor to ensure the security of personal data were adequate to the state of technical knowledge, implementation costs and the nature, scope, context and purposes of processing, which consequently did not ensure effective implementation of data protection principles. Consequently, in the opinion of the President of the Personal Data Protection Office, both Fortum and PIKA have not implemented appropriate technical and organizational measures to ensure the security of processing of personal data contained in the IT system subject to modification, which constitutes a breach of Art. 32 sec. 1 and 2 of Regulation 2016/679.

Moreover, it should be noted that the obligations to implement appropriate technical and organizational measures to ensure that the processing takes place in accordance with this Regulation and to provide the processing with the necessary safeguards to meet the requirements of this Regulation have been imposed on the data controller (and only on the data controller). the provisions of Art. 24 sec. 1 and art. 25 sec. 1 of Regulation 2016/679. Due to the fact that Fortum does not apply adequate security measures, as mentioned above, it should be considered that the Administrator has also breached these provisions of Regulation 2016/679. The consequence of their violation is the necessity to state that the confidentiality principle expressed in Art. 5 sec. 1 lit. f) Regulation 2016/679. Pursuant to Art. 5 sec. 1 lit. f) of Regulation 2016/679, data should be "processed in a manner ensuring adequate security of personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, by appropriate technical or organizational measures". It should be emphasized that the correct and effective protection of data was raised in Regulation 2016/679 to the rank of a general principle, which proves that the issue of ensuring the confidentiality of data should be treated in a special and priority manner by the data controller. Meanwhile, as already shown in the justification of this decision, both Fortum and PIKA did not implement appropriate technical and organizational measures to ensure the security of personal data processing, which led Fortum to breach their confidentiality due to a breach of personal data protection, i.e. a breach of the principle of referred to in Art. 5 sec. 1 lit. f) Regulation 2016/679.

Pursuant to Art. 28 sec. 1 of Regulation 2016/679, if the processing is to be carried out on behalf of the controller, he or she uses only the services of such processors that provide sufficient guarantees to implement appropriate technical and organizational measures to ensure that the processing meets the requirements of this Regulation and protects the rights of data subjects.

In the case in question, the Administrator indicated that prior to the conclusion of the data processing agreement, he had not verified the Processor. Fortum has been cooperating with PIKA for many years and so far there have been no security incidents. In addition, as indicated by the Administrator, PIKA is a market leader in the field of services provided and represents a high standard in the field of archiving and digitization. Therefore, the administrator considered it sufficient to sign a personal data processing outsourcing agreement with the arrangements set out in the appendix to this agreement.

Before the commencement of the administrative procedure in question, the Administrator did not exercise the right of control referred to in Art. 28 sec. 3 lit. h) of Regulation 2016/679, in terms of PIKA's provision of the measures required under Art. 32 of Regulation 2016/679. Only after the breach of personal data security has been identified and the administrative proceedings in this case have been initiated, the Administrator sent the Processor a questionnaire for the processor, which is the first element of the process of verification of the processors.

In the facts of the case at hand, it should be indicated that since the processing is to be performed 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. Long-term cooperation of the parties, not supported by periodic, systematic audits or inspections, does not guarantee that the processor will correctly perform the tasks required by law and resulting from the entrustment agreement concluded. The existing, positively assessed cooperation may only be a starting point when verifying whether the processor provides 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. The requirement specified in Art. 28 sec. 1 of Regulation 2016/679 absolutely applies to every data administrator who, as part of his business, uses the resources or services of the processor during the processing of personal data. The mere signing of a contract for entrusting the processing of personal data without proper assessment of the processor cannot be considered as the fulfillment of the obligation to conduct a procedure to verify the processor in terms of its

compliance with the requirements of Regulation 2016/679. The obligation to carry out such an assessment also does not exempt the fact of many years of cooperation and use of the services of a given processor before May 25, 2018, i.e. before the application of Regulation 2016/679.

In the case at hand, the Controller did not carry out such verification, but only a positive assessment of the processor, which was the result of the cooperation so far, during which, as he explained, there were no security incidents. However, the consequence of failure to perform this assessment is Fortum's breach of the requirement set out in Art. 28 sec. 1 of Regulation 2016/679.

When applying the provisions of Regulation 2016/679, it should be borne in mind that the purpose of this regulation (expressed in Article 1 (2)) is to protect the fundamental rights and freedoms of natural persons, in particular their right to the protection of personal data, and that the protection of natural persons in connection with the processing of personal data is one of the fundamental rights (first sentence of Recital 1). In case of any doubts, e.g. regarding the performance of obligations by administrators - not only in a situation where there has been a breach of personal data protection, but also when developing technical and organizational security measures to prevent them - these values should be taken into account in the first place.

Bearing in mind the above findings, the President of the Personal Data Protection Office, exercising his powers specified in art. 58 sec. 2 lit. and 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 this Regulation, an administrative fine under Art. 83 sec. 4 lit. a) and sec. 5 lit. a) of Regulation 2016/679, having regard to the circumstances established in the proceedings in question, stated that in the case in question there were premises justifying the imposition of administrative fines on the Administrator and the Processor.

Pursuant to Art. 83 sec. 4 lit. a) Regulation 2016/679, breach of the provisions on the obligations of the controller and the processor referred to in art. 8, 11, 25–39 as well as 42 and 43 are subject to, pursuant to para. 2 an administrative fine of up to EUR 10,000,000, and in the case of a company - up to 2% of its total annual worldwide turnover from the previous financial year, whichever is higher.

Pursuant to Art. 83 sec. 5 lit. a) Regulation 2016/679, breach of the provisions on the basic principles of processing, including the terms of consent, as referred to in art. 5, 6, 7 and 9 are subject to, in accordance with para. 2 an administrative fine of up to EUR 20,000,000, and in the case of a company - up to 4% of its total annual worldwide turnover from the previous financial

year, whichever is higher.

Art. 83 sec. 3 of Regulation 2016/679, on the other hand, provides that if a controller or processor intentionally or unintentionally infringes several provisions of this Regulation in the same or related processing operations, the total amount of the administrative fine shall not exceed the amount of the penalty for the most serious infringement.

In the present case, an administrative fine was imposed on Fortum for violation of Art. 25 sec. 1, art. 28 sec. 1, art. 32 sec. 1 and 2 of Regulation 2016/679 on the basis of the above-mentioned Art. 83 sec. 4 lit. a) of Regulation 2016/679, and for the violation of Art. 5 sec. 1 lit. f) Regulation 2016/679 - pursuant to art. 83 sec. 5 lit. a) of this regulation. At the same time, a fine in the amount equivalent to PLN 1,080,000. EUR imposed on Fortum jointly for breach of all the above provisions - pursuant to Art. 83 sec. 3 of Regulation 2016/679 - does not exceed the amount of the fine for the most serious violation found in the present case, i.e. violation of Art. 5 sec. 1 lit. f) Regulation 2016/679, which pursuant to Art. 83 sec. 5 lit. a) of Regulation 2016/679 is subject to an administrative fine of up to EUR 20,000,000, and in the case of an enterprise - up to 4% of its total annual worldwide turnover from the previous financial year.

Administrative fine imposed on PIKA for violation of Art. 32 sec. 1 and 2 of the Regulation 2016/679 is based on Art. 83 sec. 4 lit. a) of Regulation 2016/679.

When deciding to impose an administrative fine on Fortum, 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. The nature and gravity of the infringement (Article 83 (2) (a) of Regulation 2016/679). When imposing the penalty, it was important that the infringement of the provisions of Regulation 2016/679, imposing obligations on the controller to apply appropriate technical and organizational measures in order to ensure the security of the processed personal data, it had an impact on the breach of data confidentiality over 95 thousand. Administrator's clients. The breach of personal data protection found in the present case, consisting in allowing unauthorized persons access to personal data, is of considerable importance and serious nature, as it may lead to material or non-material damage to the data subject, and the probability of their occurrence is high. In addition, the risks arising from the wide range of data affected by the breach, the large number of data subjects as well as the large-scale and professional nature of data processing should be taken into account. It should be emphasized that there is still a high risk of unlawful use of their personal data in relation to persons whose data has been

violated, because the purpose for which unauthorized persons took action resulting in the violation of personal data protection is unknown. Data subjects may therefore still suffer material damage, and the breach of confidentiality of data itself also constitutes non-pecuniary damage (harm). The data subject may, at the very least, feel the fear of losing control of their personal data, of identity theft or identity fraud, and finally of financial loss.

2. The degree of Fortum's liability, taking into account the implemented technical and organizational measures (Article 83 (2) (d) of Regulation 2016/679). The arrangements made by the President of the Personal Data Protection Office allow the conclusion that the Administrator, despite the contract concluded with the Processor, adopting appropriate internal regulations and knowledge of how to implement changes in IT systems, did not fulfill his obligations in the field of supervision over the processing entity during the implementation of changes in the IT system used to process personal data, which consequently led to freedom of action by the Processing Entity, i.e. implementing changes in the IT system without prior appropriate testing of the applied security measures and supplying an additional database with actual personal data of Fortum customers, during the test phase of the implemented solution. The lack of any supervision over the process of implementing changes in the IT system in which personal data was processed results in a high degree of the Administrator's responsibility for violating the confidentiality of personal data.

3. Relevant earlier violations of the provisions of Regulation 2016/679 (Article 83 (2) (e) of Regulation 2016/679) - Previous violations of the provisions of Regulation 2016/679 by Fortum were found in the scope of Art. 6 2016/679, (case no .: DS.523.3241.2020; decision date: 30 December 2020, case no .: DS.523.3072.2020; decision date: December 30, 2020, case no .: DS 523.3067.2020; date of issue of the decision: December 30, 2020, case no .: DS.523.3144.2020; date of issue of the decision: December 30, 2020, case no .: DS.523.3331.2020; date of issue of the decision: 30 December 2020, case no .: DS.523.3626.2020; decision date: 31 December 2020, case no .: DS.523.3208.2020; decision date: 28 December 2020) - in these cases The President of the Personal Data Protection Office issued a reminder to Fortum. In the WP253 Guidelines, the Article 29 Working Party indicates that this criterion is intended to assess the business history of the infringer, therefore "Supervisory authorities should take into account the fact that the scope of such an assessment may be quite broad, as any type of breaches of the regulation, even if different from the one currently being investigated by the supervisory authority, could be 'relevant' to the assessment as it could indicate a general level of insufficient knowledge or a disregard for data protection rules. '

4. Categories of personal data concerned by the infringement (Article 83 (2) (g) of Regulation 2016/679). Personal data accessed by an unknown and unauthorized third party do not belong to the special categories of personal data referred to in in art. 9 of the Regulation 2016/679, however, their wide scope, i.e. name and surname, address of residence or stay, PESEL number, type, series and number of an identity document, e-mail address, telephone number and the number and address of the collection point, and contract data (e.g. date and contract number, fuel type, meter number) is associated with a high risk of violating the rights or freedoms of individuals affected by the violation. It should be emphasized that, in particular, unauthorized disclosure of such a data category as a PESEL number (in combination with a first and last name) may have a real and negative impact on the protection of the rights or freedoms of natural persons. PESEL number, i.e. an eleven-digit numeric symbol, uniquely identifying a natural person, containing the date of birth, serial number, gender and a control number, and therefore closely related to the private sphere of a natural person and also subject to exceptional protection as a national identification number under Art. 87 of Regulation 2016/679 is a data of a special nature and requires such special protection. When determining the amount of the administrative fine imposed on Fortum, the President of the Personal Data Protection Office took into account the following premises as mitigating circumstances: 1. Duration of the infringement (Article 83 (2) (a) of Regulation 2016/679) - the President of UODO considers the duration of the infringement of the provisions of Regulation 2016/679 to be a mitigating circumstance. According to the information obtained by the supervisory authority in the course of the administrative procedure, the newly created database, supplied with actual data of Fortum's customers, remained unprotected against unauthorized access on [...] - [...] April 2020, i.e. for 5 days.2. Unintentional nature of the violation (Article 83 (2) (b) of Regulation 2016/679) - the President of the Personal Data Protection Office did not find in this case any deliberate actions of the Administrator leading to the violation of the provisions of Regulation 2016/679. 3. Actions taken to minimize the damage suffered by the data subjects (Article 83 (2) (c) of Regulation 2016/679) - in this case, the Administrator did not find any damage to property on the part of the persons affected by the infringement. It should be pointed out that immediately after disclosure of the breach of personal data protection, Fortum took steps, as a result of which the reason for the breach was quickly determined and the data was secured against further breaches, i.e. before being collected by other unauthorized entities. The decision indicates as an aggravating circumstance that data subjects may still suffer material damage, and the breach of data confidentiality itself is also a non-pecuniary damage (harm), but taking quick steps to protect the data from being downloaded by others unauthorized entities should be assessed as a mitigating circumstance, because, in the opinion of

the President of the Personal Data Protection Office, a narrowing of the group of entities that may illegally download the data of the Administrator's customers should be considered as actions taken to minimize the damage suffered by the data subjects. 4. The degree of cooperation with the supervisory authority in order to remove the breach and mitigate its possible negative effects (Article 83 (2) (f) of Regulation 2016/679). In the course of the proceedings, in connection with the request of the President of the UODO, Fortum sent data subjects notifications about the breach of their personal data, containing all required under Art. 34 sec. 2 of Regulation 2016/679, information. 5. Any other aggravating or mitigating factors applicable to the circumstances of the case, obtained directly or indirectly from the infringement, financial benefits or losses avoided (Article 83 (2) (k) of Regulation 2016/679). In the course of these proceedings, the President of the Personal Data Protection Office did not state that Fortum obtained any financial benefits or avoided any financial losses by committing the infringement punishable by the penalty. In the course of the proceedings, Fortum provided extensive explanations precisely indicating at what stage of the process of implementing changes to the IT system an error occurred, as a result of which a personal data breach occurred. The fact that the President of the Office applied to Fortum in the present case by the President of the Office of sanctions in the form of an administrative fine, as well as its amount, was not affected by other sanctions specified in Art. 83 sec. 2 of Regulation 2016/679 circumstances, that is: 1. The way in which the supervisory authority learned about the breach (Article 83 (2) (h) of the Regulation 2016/679) - the President of the Personal Data Protection Office found the breach as a result of the notification of the breach of personal data protection by The Administrator, however, due to the fact that the Administrator, by making this notification, only fulfilled the legal obligation incumbent on him, there are no grounds to recognize 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 2016/679 Wp. 253 "The supervisory authority may become aware of a breach as a result of investigations, complaints, press articles, anonymous indications 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. Mere compliance with this obligation by an administrator cannot be interpreted as a weakening / mitigating factor ".2. Compliance with previously applied measures in the same case, referred to in Art. 58 sec. 2 of Regulation 2016/679 (Article 83 (2) (i) of Regulation 2016/679) - in this case no measures were previously applied to Fortum, referred to in Art. 58 sec. 2 of Regulation 2016/679. 3. Application of approved codes of conduct pursuant to Art. 40 of the Regulation 2016/679 or approved certification mechanisms pursuant to Art. 42 of Regulation 2016/679 (Article 83 (2) (j) of Regulation 2016/679) -

Fortum does not apply approved codes of conduct or approved certification mechanisms referred to in the provisions of Regulation 2016/679.

When deciding to impose an administrative fine on PIKA, 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. Nature and gravity of the infringement (Article 83 (2) (a) of Regulation 2016/679). When imposing the penalty, the fact that the violation of the provisions of Regulation 2016/679, imposing on the Processor obligations to apply appropriate technical and organizational measures to ensure the security of the processed personal data, had an impact on the breach of data confidentiality of over 95,000. Administrator's clients. The breach resulted from the non-application by the Processor of the basic security rules, consisting in not securing personal data against access by unauthorized persons. The processing entity providing professional services, incl. in the field of providing IT systems and having appropriate knowledge in this regard, he did not apply the security rules, supplying the actual data of the administrator's clients to the database, which is not secured against unauthorized access. The breach of personal data protection found in this case, consisting in allowing unauthorized persons to access personal data, as a result of which the Administrator's customer database was downloaded, is of considerable importance and serious nature, as it may lead to property or non-property damage to the data subject. violated and the probability of their occurrence is high. In addition, the risks arising from the wide range of data affected by the breach, the large number of data subjects as well as the large-scale and professional nature of data processing should be taken into account. It should be emphasized that there is still a high risk of unlawful use of their personal data in relation to persons whose data has been violated, because the purpose for which unauthorized persons took action resulting in the violation of personal data protection is unknown. Data subjects may therefore still suffer material damage, and the breach of confidentiality of data itself also constitutes non-pecuniary damage (harm). The data subject may, at the very least, feel the fear of losing control of their personal data, of identity theft or identity fraud, and finally of financial loss.

2. The degree of responsibility, taking into account the implemented technical and organizational measures (Article 83 (2) (d) of Regulation 2016/679). The findings made by the President of the Personal Data Protection Office allow the conclusion that the Processing Entity, despite the adoption of appropriate internal regulations, did not fulfill its obligations in the scope of implementing changes in IT systems, which consequently led to the implementation of changes in the IT system without prior

testing of the applied security measures, feeding with actual personal data Fortum customers additional database in the test phase of the implemented solution. The Processor is directly responsible for the breach, and such gross negligence in the processing of personal data must be an aggravating circumstance in the case of a professional entity.

3. Categories of personal data affected by the breach (Article 83 (2) (g) of Regulation 2016/679). The personal data accessed by an unknown and unauthorized third party does not belong to the special categories of personal data referred to in Art. 9 of Regulation 2016/679, however, their wide scope, i.e. name and surname, address of residence or stay, PESEL number, type, series and number of an identity document, e-mail address, telephone number and number and address of the collection point, and contract data (e.g. date and contract number, fuel type, meter number) entails a high risk of violating the rights and freedoms of individuals affected by the violation. It should be emphasized that, in particular, unauthorized disclosure of such a data category as a PESEL number (in combination with a first and last name) may have a real and negative impact on the protection of the rights or freedoms of natural persons. PESEL number, i.e. an eleven-digit numeric symbol, uniquely identifying a natural person, containing the date of birth, serial number, gender and a control number, and therefore closely related to the private sphere of a natural person and also subject to exceptional protection as a national identification number under Art. 87 of Regulation 2016/679 is a data of a special nature and requires such special protection.

When determining the amount of the administrative fine imposed on PIKA, the President of the Personal Data Protection Office took into account the following premises as a mitigating circumstance:

1. Duration of the infringement (Article 83 (2) (a) of Regulation 2016/679) - the President of UODO considers the duration of the infringement of the provisions of the General Data Protection Regulation as a mitigating circumstance. According to the information obtained by the supervisory authority in the course of the administrative proceedings, the newly created database, supplied with actual customer data, remained unsecured against unauthorized access on [...] - [...] April 2020, i.e. for 5 days.

2. Unintentional nature of the infringement (Article 83 (2) (b) of Regulation 2016/679) - the President of the Personal Data Protection Office did not find in this case any deliberate actions of the Processor leading to the violation of the provisions of Regulation 2016/679.

3. Actions taken to minimize the damage suffered by data subjects (Article 83 (2) (c) of Regulation 2016/679) - in this case, the Administrator did not find any material damage to the persons affected by the infringement, however, it should be indicated, that immediately after the disclosure of a breach of personal data protection, before the initiation of administrative proceedings,

PIKA took steps as a result of which the reason for the breach was quickly determined and the data was secured against further breaches, i.e. before being collected by other unauthorized entities. The decision indicates as an aggravating circumstance that data subjects may still suffer material damage, and the breach of data confidentiality itself is also a non-pecuniary damage (harm), but taking quick steps to protect the data from being downloaded by others unauthorized entities should be assessed as a mitigating circumstance, because, in the opinion of the President of the Personal Data Protection Office, a narrowing of the group of entities that may illegally download the data of the Administrator's customers should be considered as actions taken to minimize the damage suffered by the data subjects.

4. Relevant previous infringements of the provisions of Regulation 2016/679 (Article 83 (2) (e) of Regulation 2016/679) - PIKA has not identified relevant previous infringements of Regulation 2016/679.

5. Any other aggravating or mitigating factors applicable to the circumstances of the case, achieved directly or indirectly as a result of the breach of financial benefits or avoided losses (Article 83 (2) (k) of Regulation 2016/679) - the President of the Personal Data Protection Office proceedings that by committing the infringement punishable by the penalty, PIKA obtained any financial gain or avoided any financial loss. In addition, immediately after the disclosure of the breach of personal data protection, PIKA took steps as a result of which the reason for the breach was quickly determined and the data was secured against further breaches. In the course of the proceedings, PIKA provided extensive explanations precisely indicating at what stage of the process of implementing changes in the IT system an error occurred, as a result of which the personal data protection was breached.

The fact that in this case the President of the Office applied to PIKA sanctions in the form of an administrative fine, as well as its amount, were not affected by other sanctions specified in Art. 83 sec. 2 of Regulation 2016/679 circumstances, that is:

1. The degree of cooperation with the supervisory authority in order to remove the breach and mitigate its possible negative effects (Article 83 (2) (f) of Regulation 2016/679). In the course of the proceedings, PIKA did not take any additional actions in connection with the instances of the authority. However, before the initiation of the proceedings, independent, spontaneous actions were taken by PIKA to remove the infringement. These activities were, however, autonomous; The President of the Personal Data Protection Office cannot treat them as undertaken in cooperation with the supervisory authority and therefore cannot assess the "degree" of this cooperation. However, these actions were considered above as a mitigating circumstance set out in Art. 83 sec. 2 lit. c of the Regulation 2016/679.

2. The way in which the supervisory authority found out about the breach (Article 83 (2) (h) of Regulation 2016/679) - the President of the Personal Data Protection Office found the breach as a result of the notification of the breach of personal data protection made by the Administrator. By making this notification, the Controller only fulfilled its legal obligation, there are no grounds to consider that this circumstance constitutes a mitigating circumstance for the Processor. In accordance with the Guidelines on the application and determination of administrative fines for the purposes of Regulation 2016/679 Wp. 253 "The supervisory authority may become aware of a breach as a result of investigations, complaints, press articles, anonymous indications 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. Mere compliance with this obligation by an administrator cannot be interpreted as a weakening / mitigating factor ".

3. Compliance with previously applied measures in the same case, referred to in Art. 58 sec. 2 of Regulation 2016/679 (Article 83 (2) (i) of Regulation 2016/679) - in this case, the measures referred to in Art. 58 sec. 2 of Regulation 2016/679.

4. Application of approved codes of conduct pursuant to Art. 40 of the Regulation 2016/679 or approved certification mechanisms pursuant to Art. 42 of Regulation 2016/679 (Article 83 (2) (j) of Regulation 2016/679) - PIKA does not apply the approved codes of conduct or approved certification mechanisms referred to in the provisions of Regulation 2016/679.

Taking into account all the above-mentioned circumstances, the President of the Personal Data Protection Office decided that the imposition of an administrative fine on the Administrator and the Processor is necessary and justified by the weight, nature and scope of the alleged infringements of the provisions of Regulation 2016/679. 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 stopping at an admonition (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 abovementioned entities in the future will not commit a similar negligence as in this case.

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

In the opinion of the President of the Personal Data Protection Office, an administrative fine imposed on Fortum in the amount of PLN 4,911,732 (in words: four million nine hundred eleven thousand seven hundred and thirty two zlotys), which is equivalent to EUR 1 080,000 (average EUR exchange rate from January 28, 2021 - 4.5479) PLN), 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.

In the opinion of the President of the Personal Data Protection Office, the penalty imposed on the Administrator is proportional both to the seriousness of the breach (resulting in a breach of one of the basic principles on which the personal data protection system is based in Regulation 2016/679 - the data confidentiality principle) and to the size of the Administrator, which is measured its turnover - should be considered inextricably linked with the effectiveness of the punishment and its dissuasive character.

In the course of the proceedings, Fortum presented the financial statements for 2020, according to which its net sales revenues amounted to PLN 2,789,815,141.52 (in words: two billion seven hundred eighty nine million eight hundred fifteen thousand one hundred and forty one PLN 52/100), which is the equivalent of EUR 613,429,306, 17 at the average EUR exchange rate of January 28, 2021. Considering the above financial results of Fortum, it should be stated that the administrative fine will not be excessively severe for it. It should be noted that the amount of the fine set by the President of UODO - PLN 4,911,732 - constitutes only 0.18% of its turnover achieved in 2020. At the same time, in the opinion of the President of UODO, the penalty in this amount will be effective (it will achieve the goal of punishing the Administrator for a serious infringement with serious consequences) and deterrent for the future (it will make the Administrator, in order to avoid further sanctions, pay due attention to the processing of personal data through and with the assistance of the Processor, while using the rights he is entitled to under the data processing agreement). A penalty of a lower amount for such a large entity as Fortum could be practically unnoticeable and could leave room for calculation if the costs of administrative fines for this organization would not be lower than the expenditure on personal data protection.

In view of the above, the President of the Personal Data Protection Office also points out that the administrative fine imposed on Fortum meets, in particular, the criterion of proportionality of the penalty within the meaning of the jurisprudence of the CJEU (under competition law and in relation to the decision of the European Commission, but which, in the opinion of the President of the Personal Data Protection Office, has a more general application): "[...] the principle of proportionality requires that acts of the institutions of the Union do not go beyond what is appropriate and necessary for the fulfillment of the legitimate

aims pursued by the rules concerned, and where there is a choice of more appropriate options, the least severe and the resulting inconvenience must not be excessive in relation to the objectives pursued […] (see judgment of 12 December 2012, Electrabel v Commission, T □ 332/09, EU: T: 2012: 672, paragraph 279) and the case-law cited therein) ”(see judgment of 26 October 2017, Marine Harvest ASA v EC, para. 580).

The above general considerations regarding the proportionality, effectiveness and dissuasiveness of the administrative fine imposed on Fortum also apply to the penalty imposed on PIKA.

In the course of the proceedings, PIKA presented the financial statements for 2020, according to which its net sales revenues in this financial year amounted to PLN 21,083,344.14 (in words: twenty one million eighty three thousand three hundred and forty four PLN 14/100), which is the equivalent of EUR 4 635 841.63 according to the average EUR exchange rate of January 28, 2021. In the opinion of the President of the Personal Data Protection Office, also the fine imposed against PIKA will not be excessively severe for this company. A fine in the amount of PLN 250,135 (in words: two hundred and fifty thousand one hundred and thirty five zlotys), which is the equivalent of EUR 55,000, also according to the average euro exchange rate of January 28, 2021, will only constitute 1.19% of the turnover achieved by PIKA in 2020. and only 0.55% of the maximum possible penalty. The President of UODO notes that the penalty imposed against PIKA may be relatively more severe for her than the penalty imposed on Fortum in the present case (1.19% compared to 0.18% of the annual turnover), nevertheless, in the opinion of the authority, it is justified by the fact that this action PIKA, characterized by a gross neglect of its obligations and applicable standards, has directly led to a breach of the protection of personal data, the administrator of which is Fortum, and consequently to a breach of the confidentiality of these data (for which - violation of Article 5 (1) (f) of Regulation 2016 / 679 - PIKA as a processor is not directly responsible, and the Administrator is responsible).

Summing up the above, in the opinion of the President of the Personal Data Protection Office, both administrative pecuniary penalties adjudicated in this case fulfill the conditions (the functions of penalties) referred to in Art. 83 sec. 1 of Regulation 2016/679, due to the importance of the infringements found in the context of the basic requirements and principles of Regulation 2016/679.

II. At the same time, on the basis of the evidence collected in the course of the proceedings, it should be stated that the remaining provisions of Regulation 2016/679, being the subject of this proceeding, have not been breached.

In terms of the possibility of violating Art. 34 sec. 1 of Regulation 2016/679, the proceedings became redundant due to the fact

that the Administrator, in the course of the proceedings, sent to data subjects notifications about the breach of their personal data, containing all required in accordance with art. 34 sec. 2 of Regulation 2016/679, information. Consequently, the proceedings had to be discontinued as far as Fortum could infringe Art. 34 sec. 1 of Regulation 2016/679.

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

2022-02-02