Warsaw, on 08

February

2023

Decision

DKN.5131.50.2021

Based on Article. 104 § 1 of the Act of June 14, 1960 Code of Administrative Procedure (Journal of Laws of 2022, item 2000, as amended), in connection with Art. 7, art. 60, art. 101 and art. 103 of the Act of May 10, 2018 on the protection of personal data (Journal of Laws of 2019, item 1781), art. 57 sec. 1 lit. a) and h) and Art. 58 sec. 2 lit. d) and i) in connection with Art. 5 sec. 1 lit. f), art. 5 sec. 2, art. 24 sec. 1, art. 25 sec. 1, art. 28 sec. 1 and 3, art. 32 sec. 1 and 2, as well as art. 83 sec. 1-3 and art. 83 sec. 4 letter 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 EU L 119 of 04.05.2016, p. 1, Official Journal of the EU L 127 of 23.05.2018, p. 2 and Official Journal of the EU L 74 of 4.03.2021, p. 35) hereinafter referred to as: "Regulation 2016/679", after conducting administrative proceedings initiated ex officio regarding the processing of personal data by: (...) K. P. conducting business activity under the name: "(...)" with the place of business in S. at ul. (…) (as the data controller) and (…) M. H. conducting business activity under the business name: "(...)" with the place of business in Z. at ul. (…) (as a processor), President of the Personal Data Protection Office,

1) stating a violation by (...) K.P. conducting business activity under the business name: "(...)" with the place of business in S. at ul. (…), art. 5 sec. 1 lit. f), art. 5 sec. 2, art. 24 sec. 1, art. 25 sec. 1, art. 28 sec. 1 and 3 and art. 32 sec. 1 and 2 of Regulation 2016/679, consisting in the failure to implement appropriate technical and organizational measures to ensure the security of personal data, resulting in a violation of their confidentiality and accountability, and in the lack of verification of the processing entity whether it provides sufficient guarantees for the implementation of appropriate technical and organizational measures so that the processing meets the requirements Regulation 2016/679 and protected the rights of data subjects,

a. imposes on (…) K.P. conducting business activity under the business name: "(...)" with the place of business in S. at ul. (…), for violation of Art. 5 sec. 1 lit. f), art. 5 sec. 2, art. 25 sec. 1, art. 28 sec. 1 and 3 and art. 32 sec. 1 and 2 of Regulation 2016/679, an administrative fine of PLN 33,012 (in words: thirty-three thousand and twelve zlotys), b. orders K.P. conducting

business activity under the business name: "(...)" with the place of business in S. at ul. (…) adjustment of the personal data processing operation by ceasing to entrust the processing of personal data (…) M. H. conducting business activity under the name: "(...)" with the place of business in Z. at ul. (...) based on a contract for entrusting the processing of personal data, (...) which does not contain the elements indicated in art. 28 sec. 3 lit. c), letter e) and ... f) Regulation 2016/679;

2) stating a violation by (...) M. H. conducting business activity under the business name: "(...)" with the place of business in Z. at ul. (…), art. 32 sec. 1 and 2 and art. 32 sec. 1 and 2 in connection with art. 28 sec. 3 lit. c) and f) of Regulation 2016/679, consisting in the failure to implement appropriate technical and organizational measures to ensure the security of personal data, including ensuring their confidentiality, imposes on (...) M. H. conducting business activity under the name: "(...)" with the place of business in Z. at ul. (...), an administrative fine of PLN 472.- (in words: four hundred and seventy-two zlotys).

Justification

On [...] December 2020, the President of the Office for Personal Data Protection, hereinafter also referred to as the "President of the Personal Data Protection Office" or the "supervisory authority", received a notification of a personal data breach under Art. 33 sec. 1 of Regulation 2016/679, sent by (...) K.P. conducting business activity (related to risk assessment and estimation of incurred losses and, among others, activities of insurance brokers) under the name: "(...)" with the place of business in ,S. at ul. . (...), hereinafter also referred to as the "Administrator" or "(...)", which was registered under the signature (...). In accordance with the content of sections 4A and 4E of the personal data breach notification form sent on that day (hereinafter referred to as: "Form No. (...)"), the reported breach consisted in the loss of data confidentiality in connection with the operation of the computer virus W (...) identified as a tool to (…). In box 2F of form No. (...), in the place intended to indicate another entity participating in the processing of personal data affected by the violation, the Administrator indicated the data of the processing entity - (...) M. H. running a business under the name: "(...)" with the place of performance activity in Z. at ul. (...), hereinafter referred to as "Processing Entity" or "(...)" or "ASI", dealing (as indicated in this box) with comprehensive IT services. The form No. (...) also indicated that the breach was found on [...] December 2020 and concerned the personal data of approx. 800 people (former and current clients of the Administrator) in terms of their: names, surnames, dates of birth, addresses of residence or stay, PESEL registration numbers, e-mail addresses and telephone numbers.

Notwithstanding the foregoing, on [...] December 2020, the President of the UODO became aware of a breach of the protection of personal data contained, among others, in in insurance policies concluded in the period from May 2015 to November 2020

with various insurance companies that were publicly available on IT resources belonging to the Administrator - at the address (...) in the domain (...), where among the disclosed files there were supposed to be documents such as: results of oncology tests, copies of contracts and insurance policies with customer data, photos of vehicles taken for insurance purposes, documents from the personal data security audit, security policy, as well as a file with access data to the Administrator's network resources. Such an incident was described on [...] December 2020 on the website (...). In connection with obtaining this information (as well as the lack of certainty whether it concerns a personal data breach reported on [...] December 2020), the supervisory authority contacted the Administrator on [...] December 2020. , based on Article. 58 sec. 1 lit. a) and e) of Regulation 2016/679, for appropriate explanations. In a letter received by the local Office on [...] December 2020, the Administrator confirmed that the personal data breach notification made on [...] December 2020 concerns the same event described by the portal (...) in the publication of [...] December 2020 under the title (...), and further explained that the notification was made during the verification activities (when the actual number of injured people, the scope of the disclosed data and any other circumstances of the event) and that during its completion it was incorrectly indicated that it was a complete/one-off notification, while it was supposed to be a preliminary notification. Included in this letter were a form supplementing the notification of a personal data breach (hereinafter referred to as: "Form No (...)"). In the extensive explanations contained in the above-mentioned in writing and in the attachments thereto, the Administrator indicated, among others, that: 1) on [...] December 2020, at 12:30 pm, on two administrator's computers in a time interval of 15 minutes, a prompt from the program appeared several times antivirus (...) informing about file infection by a computer virus: W (...), which was immediately informed (...) M. H. (ASI), which concluded a contract with the Administrator (...);2) The Processing Entity immediately started to perform checking activities, which ended with the identification of the virus as a tool for (…);3) around 14:00, the third party informed the Administrator's employee by phone that documents belonging to (...) were made public in the domain (...), including insurance policy documents - after receiving this information, the Processing Entity carried out checks and confirmed the publication of the files;4) access to the public database was blocked at 14:40 on the same day, i.e. [...] December 2020;5) as a result of the explanatory proceedings, it was established that the breach started in November 2020 and concerned 2,494 people; these data were in the working folder (from the server (...), which is made available in the local network for the Administrator's employees working on the docx, xlsx, pdf documents contained therein), in various types of documents, the oldest of which were dated back even to 1993 year - mostly constituting insurance policies of natural persons

(insurance data came from May 2015 to the date of the incident); the scope of the data provided regarding the Administrator's clients (former and present) differed in individual cases, and the data belonged to the following categories: names, surnames, address of residence or stay, PESEL registration number, e-mail address, series and number of ID card, telephone number and health data;6) on [...] December 2020, a website was launched (...) containing a message about the above-mentioned 7) the authentication data contained in one of the published files did not allow access to any resources used at the time of finding the violation or at the time of providing clarifications (these data allowed access to old servers - changed to new ones before the personal data protection violation occurred); 8) due to the circumstances surrounding the breach, it can be assumed with high probability that the reason for the replication of data from the server (...) was a hacking activity consisting in illegally obtaining logins and passwords used to configure the servers (...) and (...);9) the suspicion that a crime has been committed has been reported to the Police.

To the above the letter, which was received by this Office on [...] December 2020, also included, among others: 1) "Agreement (...)" (constituting part of Annex No. (...)) concluded for an indefinite period between the Administrator and the Processing Entity on (...) February 2015, the subject of which is the provision by (...) to (...) of IT support services consisting (in accordance with § (...), in particular in system administration (...) (current administrative activities) and other services in accordance with (...) related to the ongoing operation of IT systems; moreover, in § (...) of this agreement (...) he declared that he had the knowledge, experience and necessary skills for the proper performance of the subject of the agreement, and in § (...) he undertook to that the activities covered by the subject of this agreement will be performed with due diligence, according to the best knowledge and experience; the "Agreement (...)" concluded on (...) April 2020 between the above-mentioned entities was also attached to this agreement - in the agreement this, hereinafter referred to as: "Agreement (...)" (which, in accordance with § (...), replaced all previous arrangements regarding the processing of personal data related to the above-mentioned The cooperation agreement, in particular the agreement on entrusting the processing of personal data concluded on the basis of the legal status that is no longer in force), however, the elements referred to in art. 28 sec. 3 lit. c), e) and f) of Regulation 2016/679; 2) "Policy (...)" (constituting Appendix No. (...)) introduced by the Administrator on [...] April 2020, from which Appendix No. (...), i.e. the Instruction (...), it results, among others, that at the point of contact of the Data Administrator's computer network with the public network, there are applied (...), preventing unauthorized access from outside to its resources, as well as allowing control of the flow of data (chapter (...) of the above-mentioned Instructions);3) content of

the message - notification of a breach of personal data protection published on the website (...) (Appendix No. (...));4) protocol of a breach of personal data protection No. (...) drawn up by the Administrator in on [...] December 2020 (constituting Appendix No. (...));5) System/device test report of [...] December 2020 (constituting Appendix No. (...)) prepared by the Processing Entity from which it follows, among others, that: - the user reported a problem: (quote): "prompt from the program (...) about the emergence of viruses", - the problem was removed (HDD scanning + installation (...)), - it was recommended to return particular attention to messages from (...) containing attachments and coming from unknown senders, - the remarks include (quote): "HDD scan (...). Removed remaining threats, uninstalled (…)".

In the above in the letter received by the local Office on [...] December 2020 and in the attachments thereto, the Administrator also indicated: 1) that the entity providing hosting services to the Administrator is (...) sp. z o.o. with its registered office in Ł. (box 2F of form No. (...)) - hereinafter also referred to as (...); 2) what actions have been taken to minimize the risk of recurrence of such events in the future (quote): "Immediately after detecting a breach, all computers and servers (...) were rescanned for detecting the presence of viruses using new software (...), which was installed on all computers in place of the previous program. Then, in order to significantly improve security, the data was transferred to the newly purchased IT infrastructure in the form of: (...), (...) purchased together with the implementation and staff training service. Full backups are also made using the software (…). An audit in the field of IT security is currently being carried out. Recommendations that will be presented after the audit will be implemented"; additional security measures are also indicated in box 9B of form No. (...) (change of access passwords to e-mail boxes, servers (...), user accounts in the system (...) on all computers, scanning all computers and servers (...) for the presence of viruses by means of software (...));3) when and how the controller and processors involved in the processing of the data to which the breach relates regularly tested, measured and assessed the effectiveness of technical and organizational measures to ensure the security of personal data being processed in IT systems affected by the breach - in this respect, it was indicated that this was done (quote): "(...) by performing ongoing updates of workstations, updates of server firmware (...) and anti-virus scanning. ASI regularly tested, measured and assessed the effectiveness of technical measures to ensure the security of personal data being processed in the IT systems affected by the breach.

Then, on [...] January 2021, the supervisory authority asked the Administrator pursuant to art. 58 sec. 1 lit. a) and e) of Regulation 2016/679 for additional explanations. To the response to this request (which was received by the local Office on [...]

January 2021), the Administrator attached the originally prepared by the Processing Entity (on [...] December 2020) description of the infringement (from which it resulted that (quote): "Due to the circumstances accompanying the breach found, I suppose that the reason for the replication of data from the server (...) is an activity bearing the features of a hacker's activity, consisting in illegal access by means of the W virus (...) to possession of logins and passwords used for server configuration (...)"), and also indicated, among others, that (quote): 1) "As a result of the breach of personal data protection, proceedings were conducted to clarify the circumstances of its occurrence, as a result of which it was established that there was no security breaches (…). The reason for the breach of personal data protection was the replication of the files of the internal work resource to the server (…)";2) »As a result of the breach of personal data protection, the directory "(...)" was placed in the domain (…). The "(...)" directory is one of its subdirectories. In the protocol on the breach of personal data protection No. (...) of [...].12/2020 and in the Notification of a breach of personal data protection - Supplementary/amending notification of [...].12/2020, all personal data are described subject to infringement, i.e. those stored in the "(...)" directory and all its subdirectories, e.g. in the "(...)"" directory; 3) "Placing data in the above-mentioned locations was in no way intended or intentional, and occurred as a result of unplanned data replication."

The letter also contains a detailed description of the infringement (quote): "In order to determine the circumstances of the infringement (...), he obliged ASI (M.H.) to explain them (...). Accepting the analysis carried out by ASI and the described events (...), he assumed that the main cause of the breach was the described virus and its consequences, i.e. logins and passwords used for configuration and administration used in (...) servers (...) and the server (...) were stolen. (…) having confidence in ASI, he referred to this information in the personal data breach notification, supplementary notification and in previous correspondence with the President of the UODO. Aware of the seriousness of the infringement and aiming at its reliable explanation (...) not wanting to base his knowledge only on the analysis performed by ASI, he established cooperation with the company (...) commissioned an audit of the IT infrastructure. The auditor (...) analyzed the incident and questioned that the main cause of the personal data breach was the operation of the W virus (...). In cooperation with ASI (M.H.), they established the following circumstances of the incident: In the fourth quarter of 2020 (...), in connection with the intensifying COVID-19 pandemic, commissioned ASI (M.H.) to provide its employees with the possibility of remote work. Due to the specific nature of the tasks performed and the need for close cooperation between employees when creating documentation for customer service, there was a need to separate a common work resource containing a file repository and make it available

to employees. For this purpose, a server was used (...) by separating the resource to which the files were copied. The resource was made available in the local network and made available remotely by using the server built into (...), which was secured with encryption (...). In addition, the mechanism (…) was used for additional protection of the shared resource by means of its replication to a separate local server (…). Considering the structure of the locally shared resource located in the directory (...) and the structure of the locally replicated resource located in the directory (...) and comparing it to the structure of the resource located on the server (...) the only possible reason for the situation was the incorrect configuration of servers (…) made by ASI during the implementation of remote work. (…) during the personal data breach, he had the system (…) and (…) installed on all workstations and did not use other IT systems".

In addition, the Administrator, in the letter of [...] January 2021, indicated that (quote) "At the request of (...), the audit company analyzed the system logs, determining that there were several data downloads by unauthorized persons, i.e. one intentionally downloading all available files from a shared resource on the server (...), several files (...) of an internal nature and several partial lists of shared files (index headers)". The administrator, referring to the report on the audit of the security and organization of the IT infrastructure (constituting Annex No. (...) to the letter), also indicated the details of the findings made by the auditing company in this regard.

In the above in writing (date of receipt: [...] January 2021) (...) also explained that (quote): "Before the infringement (...) he did not perform penetration tests. Reports on tests of the correct operation of IT systems and devices on behalf of (...) were performed by ASI (M. H.)" (copies of reports on monthly tests were attached to the above-mentioned letter), and also that (quote): "The tests were carried out immediately after the occurrence of violation by a professional external entity (…), during the audit of the security and organization of the IT infrastructure". The letter additionally shows that the Administrator, after the breach occurred, took a number of other actions aimed at minimizing the risk of such breaches in the future (including implementing (...) allowing for the elimination of work directly on docx, xlsx, pdf files (...)) .

To the letter of [...] January 2021, the Administrator attached, as mentioned above, a report issued on [...] January 2021 on the audit of the security and organization of the IT infrastructure carried out on [...] December 2020 - [...] January 2021 (hereinafter: "Report No. (...)"), in which segment A (regarding the examination of the existing state of the IT infrastructure and data protection organization) it was indicated that the task of the first audit specifying the zero state of the organization after the incident was performed on [...]-[...] December 2020 and that the audited entity, after the incident, has already taken its own,

independent identification and corrective measures, including testing for the presence of viruses, limited analysis logs and workstation reconfigurations. Despite this, Segment A of Report No. (...) includes a number of recommendations proving irregularities in this area (due to the lack of appropriate safeguards for the confidentiality of data on one of the network devices, the persons conducting the audit gained access to directories of files containing personal data - including special category data). In the section summarizing this segment of the report, it was indicated, among others, that (quote): "The conducted study and the relatively low level of technical and organizational security measures showed the need to strengthen the work of the IT specialist who supports (...). We point out the need to conduct an internal analysis of the possibility of supporting the current work of an IT specialist with an additional asset with a specialization in network service configuration."

In segment B of Report No. (...) (regarding the examination of the condition of the IT infrastructure after the implementation of corrective and corrective actions) it was indicated that on January [...]-[...], 2021, a second audit was carried out as an audit of the supervision of the implementation level corrective and corrective actions and determination of the level of involvement of the company's management and owners in minimizing the effects of the incident and breach. It stated that the audited organization, prior to the breach, had undertaken its actions in good faith (similarly to the IT person serving it, who - as stated in the report: "acted in full conviction of the correctness of its activities and full care for the interests of its principal"), and currently consistently takes corrective, corrective and risk minimizing actions so that in subsequent periods it is not exposed to another security incident or breach. It was also found that the implementation of corrective actions in the IT area and the organization of new security measures as of the day of the second audit was in progress, at a highly advanced level.

Segment C of Report No. (...) (regarding the examination of the log file in the context of a security incident and data protection breach) indicated that it was established that making available on the server (...) in the directory (...) backup files of the internal drive of the (...) organization took place after the change of hosting from the company (...) to (...), i.e. after [...] November 2020. Based on the information collected, the entity conducting the audit hypothesized that the public disclosure of data was not intentional, but the result of a configuration error as well as an attempt to maintain the continuity of the organization's operations in the situation of pandemic restrictions. Attention was drawn to the principles of automatic mechanisms operating on the Internet, i.e. the operation of automated scanning tools (search engine robots), which, despite not informing third parties about private information on the server, found it, indexed it and presented it in search results. It was also indicated that already on [...] November 2020, there was a deliberate download of the available files (a comprehensive copy of the shared resources

was made (...)).

On [...] February 2021, the President of UODO asked (...) for further clarifications. In the letter received by the local Office on [...] February 2021, the administrator stated that (quote): "Works related to the configuration of the server (...), carried out by ASI during the implementation of remote work, began in on [...].11.2020. The server configuration change (...) took place after the disclosure of the fact of making personal data public, i.e. on [...].12.2020.". In addition, the Administrator, responding in the same letter to other questions asked by the supervisory authority, confirmed the implementation (...), while explaining that working directly on docx, xlsx and pdf files was limited to the necessary minimum (total elimination of working directly on files in these formats is not possible due to the correspondence received by the Administrator from external entities). In addition, the Administrator, when asked whether: - before signing the contract with processing entities [footnote: which was, among others, (…) M. H.] checked whether they 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, indicated that each entity with which it plans to establish cooperation is always checked in terms of reliability and real possibility of performing the ordered services, including guaranteeing the security of information provided to him, and also that before establishing cooperation with (...) M. H., the Administrator checked his education and skills; - processing entities provided the administrator with all information necessary to demonstrating compliance with the obligations set out in art. 28 of Regulation 2016/679 and enabled the administrator or an auditor authorized by the administrator to conduct audits, including inspections, and whether such audits or inspections were carried out by (...), declared that (quote): "(...) M. H. (...) performs (…) ASI function. In accordance with the concluded contract (...) (Appendix No. (...) to the letter of [...].12.2020), the processing of personal data carried out by him takes place as part of the infrastructure (...) on the terms indicated in the internal documentation and procedures. (...) has never identified the processing carried out by ASI in a manner inconsistent with the adopted internal procedures. (…) M. H. is subject to the same ongoing control in this respect as other employees (…)".

To the above letter received by the local Office on [...] February 2021, the Administrator attached, among others Report issued [...] February 2021 on the audit of the security and organization of the IT infrastructure carried out from [...] December 2020 to [...] February 2021 (hereinafter referred to as: "Report No (...) ") containing an assessment of the security level after the third supervision audit, which shows, among others, that the audited organization ensures, as of the assessment date (i.e. [...] February 2021), the correct level of data protection, information and privacy protection of persons individuals and their clients.

Segment B1 of Report No. (...) (regarding the examination of the condition of the IT infrastructure after the implementation of the next cycle of corrective and corrective actions as at the date of the third supervision audit) indicated that during the third audit it was found that the organization had taken and implemented all corrective and corrective actions available to it in order to obtain the maximum level of security and minimize the risk of another incident or breach, and also that as a result of the activities described in this segment, it has achieved the intended goals and a satisfactory, correct level of technical and organizational security.

In response to the call for clarification (of [...] March 2021), which was received by the local Office on [...] April 2021, the Administrator (asked about the method of checking education and skills (...) M. H.), indicated that (quote): "(...) has been cooperating directly with (...) M.H. since 2010. The level of knowledge and skills (...) of M.H. were verified during an interview conducted in 2010 before establishing cooperation. It was held in the same way as job interviews of employees - direct conversation, answers to questions, oral presentation of one's experience. (…) there are no objections to the quality and timeliness of the services provided by (…) M.H.. The cooperation is very good, which has built high inter-organizational trust over the years. In 2016, during the implementation of (...) solutions aimed at adapting activities to the provisions of the GDPR, (...) M. H. presented a certificate confirming knowledge of the provisions and principles of personal data protection, and also drew attention to the nature of his cooperation with the Processing Entity (quote .): "This is direct cooperation, all activities that are performed by (...) M.H. on information processed by (...) are carried out in the IT environment (...). Therefore, all procedures, rules, safeguards, etc. used by (...) M.H. are those that have been implemented and are used by (...). This is reflected in the provisions of the personal data processing agreement concluded by (...) with (...), which was presented to the President of the Office for Personal Data Protection in the letter of [...] December 2020 (Appendix No. (...))".

Then, in a letter of [...] April 2021, the President of UODO asked the Processing Entity for clarification. (...) provided them in a letter received by the local Office on [...] May 2021, and the letter states, inter alia, that: - the infringement arose as a result of the replication of the internal work resource (...) on virtual server located at the address (...), which was caused by incorrect configuration of servers (...); - the launch of the virtual server, to which the data to which the breach relates was replicated, took place on [...] November 2020 - according to the logs on the server, the first data was replicated on [...] November 2020, and access to the database was blocked on [...] December 2020 at 14:40, i.e. immediately after it was made public; - (quote): "(...) regularly tested, measured and assessed the effectiveness of technical and organizational measures to ensure the

security of personal data processed in IT systems (...). All IT systems were regularly updated to eliminate possible errors and tested for vulnerability using anti-virus and anti-malware software, with copies of system/device test reports dated [...] November 2020 attached to the letter as evidence. . and dates indicating that they were carried out after its occurrence (i.e. [...] and [...] December 2020); it was also noted that (...) he actively participated in the tests carried out by an external entity during the IT infrastructure security audit; - (quote): "A local copy was made between the working folder on the server (...) and the server (...). Files intended for archiving were compressed, the archive was password protected. In addition, regular anti-virus and anti-malware scanning of stored files was carried out through the internal mechanisms of the server (...)" - it was indicated that a copy was also once a week transferred from the server (...) to the company's server (...), and after the breach occurred, as a result conducted analyzes and IT security audits, the backup procedure was modified (a new backup system based on different software was implemented - storage of copies on the server was abandoned (...)). The processing entity also assured that it regularly tested backup copies (it also indicated the relevant procedures in this regard).

Then, on [...] June 2021, the supervisory authority asked the Processing Entity for further explanations. (...) provided them in a letter received by the local Office on [...] June 2021 - it indicates the software used to eliminate possible errors and test the IT systems used for vulnerability (both before the occurrence of a personal data protection breach as well as after). The Processing Entity also stated in this letter that testing the effectiveness of the technical measures used was carried out cyclically - once a month - during the tests of the entire IT infrastructure.

In connection with the above, on [...] November 2021, the President of the UODO instituted ex officio administrative proceedings against the Administrator (letter reference: (...)), as well as against the Processing Entity (letter reference: (...)) regarding the infringement the provisions of art. 5 sec. 1 lit. f), art. 5 sec. 2, art. 24 sec. 1, art. 25 sec. 1, art. 32 sec. 1 and 2, art. 28 sec. 1 and art. 28 sec. 3 of Regulation 2016/679, in connection with a breach of the protection of personal data contained, among others, in insurance policies concluded with various insurance companies, access to which was made available to unauthorized persons, reported to the President of the Personal Data Protection Office by (...) K.P. conducting business activity under the name: (...) - as the data controller - on [...] December 2020 and registered under number (...).

In addition, in the notifications of the initiation of proceedings, the President of the UODO, acting pursuant to art. 58 sec. 1 letter a) and e) of Regulation 2016/679, called on both of the above-mentioned entities for clarification. The administrator has been requested to indicate whether it has undertaken (as the administrator of the above-mentioned data) control activities

towards the Processor (e.g. audits, including inspections) aimed at verifying its compliance with its obligations under Art. 28 of Regulation 2016/679 (and if so, how often such activities were undertaken, how and what was their scope).

On [...] November 2021, the local Office received the Administrator's response to the above request for clarification. In it, he explained, among others, that (quote): "According to the concluded data processing entrustment agreement, the processing of personal data by (...) M. H. is carried out on the terms set out in the internal documentation and procedures (...). This means that (...) it is not possible to voluntarily shape organizational solutions related to the processing of personal data. The fact of concluding an agreement to entrust the processing of personal data results from the type of cooperation (b2b) and the inability to grant authorization to process personal data (as to other employees (...) employed under an employment contract). (…) he has never received information (even suspicions) that the processing of personal data is carried out by ASI in a manner inconsistent with the adopted internal procedures - which could justify detailed control activities".

In the reply received by this Office on [...] November 2021, the Processing Entity explained that (quote): "(...) (...) and I, acting as ASI, have consciously and intentionally never sent no files from the server (...) to the server in the company (...). By carrying out checks and eliminating potential sources of leakage on [...] December 2020, the actions taken concerned both the server in the company (...) and the server (...) in the company (...). Access to the disclosed data on the server (...) has been blocked and the server configuration (...) has been changed to the configuration preceding the possibility of remote work for employees (...). By making these changes on [...] December 2020, the incorrect configuration of the server was eliminated (...), i.e. the cause of the leak found on the basis of an audit of the IT infrastructure conducted by an external auditor, i.e. the company (...), in which the audit is also actively I participated". In this letter (...) M. H. (Processing Entity) also drew attention to his current health situation (which he also pointed out in the letter received by the local Office on [...] September 2022).

Then, on [...] February 2022, the supervisory authority requested clarifications from both the Administrator and the Processor. These entities were asked, inter alia, whether before performing activities aimed at ensuring access to files containing, among others, personal data of employees who are to work remotely, in connection with which the personal data protection has been breached, a risk analysis was carried out taking into account the risks associated with such activities (in order to identify threats and specify technical and organizational measures reducing the probability of their occurrence to the level of acceptable risk). The explanations provided in this regard by (...) in a letter received by the local Office on [...] February 2022 show that (quote) "On the basis of the "Agreement (...)" of (...) April 2020, which connects (...) with (...), (...) applies internal

regulations (...), including policy (…). This policy provides for the so-called a risk-based approach that requires constant identification and estimation of the level of risk related to the processing of personal data. All activities (...), including those related to the implementation of remote work, as well as any other activities undertaken as part of the IT infrastructure (...), which (...) supervises, were and are carried out with respect for this approach. Considering the above, activities aimed at providing access to files to employees (...) working remotely were carried out by (...) taking into account the risk associated with the implementation of such a solution. The technical and organizational measures used in this regard were subject to an analysis, prior to their implementation, taking into account the risks associated with remote work. In the assessment (...), adequate means of authorization and security of the remote work environment were used, in particular in this respect: - the server was used (...), with a resource to which the files were copied, - antivirus protection and protection against attacks were applied for the separated resource ,- the resource was made available in the local network and made available remotely by using the server built into (...), which was secured with encryption (...),- the mechanism (...) was used for additional protection of the shared resource by means of its replication on a separate local server (…). ,

In the opinion (...), as a result of the implemented solutions, the probability of the occurrence of threats related to the activities carried out has been reduced to the level of acceptable risk«.

In its explanations provided in this regard (in a letter with the date of receipt: [...] March 2022), the Administrator also drew attention to its use of a risk-based approach and to the Processing Entity's obligation to apply this approach, and then indicated that (quote): "(...) assumes that, in connection with this commitment, the technical and organizational measures used by ASI have been analyzed taking into account the risks associated with remote work, and the probability of these threats has been reduced to the level of acceptable risk".

In the summons of [...] February 2022 addressed to both of the above-mentioned entities, other questions were included, including: - whether the appropriate technical and organizational measures applied both before and after activities aimed at ensuring access to files containing, among others, personal data of employees who are to work remotely were tested for their adequacy and effectiveness, - whether the correctness (both the course and the result) of the actions taken to ensure access to files containing, among others, personal data of employees who are to work remotely (including: in terms of securing data against access by unauthorized persons) - immediately after their completion.

In this regard, the Processing Entity explained that it had checked the correctness of the actions taken to ensure access to files

containing, among others, personal data of employees (...) who are to work remotely, which is confirmed by the lack of objections of people working remotely, disclosed in the report on the tests of the IT system of [...] November 2020. The administrator also indicated that (...) this report was presented.

In addition, in their explanations (to the summons of [...] February 2022), both of these entities unanimously declared that, apart from the "Agreement (...)" concluded between (...) and (...) on (...) April 2020, no additional agreements were concluded in this regard. The administrator also indicated that the decision to undertake remote work was made by (...), and the method of carrying out activities aimed at providing access to files to employees who were to work was determined by ASI (as the person responsible for the IT infrastructure in (...)) and the data processing personal data by ASI as part of the above activities was carried out on the basis of an order (...).

On [...] March 2022, the President of UODO sent another request for clarification to the Administrator, to which (...) he replied in a letter received by the Office on [...] April 2022. This response shows that the notification of a personal data breach (in the form of two communications of [...] and [...] and [...] December 2020) will be published on the website (...) until the end of the proceedings in question.

In addition, from the latest explanations of ASI and the Administrator (received respectively on [...] and [...] November 2022 and which constituted a response to the supervisory authority's calls for explanations aimed at a thorough examination of the role of (...) M. H. in the process of processing personal data) it follows that (...) M. H. was never employed by the Administrator and processed personal data only on the basis of an agreement to entrust the processing of personal data (and not on the basis of an authorization to process them). (...) also indicated that (...) M. H. had been cooperating with him from the beginning as an external specialist, and (...) M. H. explained that during this cooperation he also provided services to other entities (e.g. in the field of comprehensive services in the field of IT). These explanations and the findings indicate its autonomous role in the processing of clients' personal data (...).

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

Article 5 of Regulation 2016/679 formulates the rules regarding the processing of personal data that must be respected by all administrators, i.e. entities that individually or jointly with others determine the purposes and methods of personal data processing. However, before discussing these rules to the extent necessary in the case in question, attention should be paid to

the status of (...) being an insurance broker, i.e. the function of the administrator performed by him in relation to the data of former and current customers contained in the disclosed files. At this point, reference should be made to the provisions of the Act of December 15, 2017 on insurance distribution (Journal of Laws of 2022, item 905, as amended), i.e.:

1. article 4 sec. 4, according to which the insurance broker, as part of its brokerage activity, performs activities in the field of insurance distribution on behalf of or for the client, hereinafter referred to as "brokerage activities in the field of insurance",

2nd article 4 sec. 1, which states that insurance distribution means activities performed exclusively by an insurance distributor (i.e. an insurance company, an insurance agent, an agent offering ancillary insurance or an insurance broker) consisting in: 1) advising, proposing or performing other preparatory activities aimed at concluding insurance contracts or insurance guarantee contracts;2) concluding insurance contracts or insurance guarantee contracts on behalf of the insurance company, on behalf of or for the client or directly by the insurance company;3) providing assistance by an insurance intermediary (i.e. insurance agent, agent offering ancillary insurance, broker insurance company and reinsurance broker who distribute insurance or reinsurance for remuneration) in the administration and performance of insurance contracts or insurance guarantee contracts, also in cases for compensation or benefit,

3. article 27 sec. 1 and 2, according to which the client grants the insurance broker, in writing, a power of attorney to perform brokerage activities in the field of insurance on behalf of the customer, and the broker provides the insurance company with this power of attorney at the first activity belonging to brokerage activities in the field of insurance; (Thus, the broker acts on behalf of and on behalf of its client on the basis of the power of attorney granted, but - what is worth noting - this mandate is not directed at the processing of personal data),

4. article 32 sec. 3, which states that the insurance broker: 1) keeps confidential the information obtained in connection with the performance of brokerage activities in the field of insurance, and this obligation is incumbent on the insurance broker also after termination of the contractual relationship with the principal; 2) provides the insurance company and the client with each request, permission to perform brokerage activities in the field of insurance; 3) keeps a register of claims and claims; 4) keeps documentation regarding brokerage activities in the field of insurance, in particular powers of attorney to perform brokerage activities in the field of insurance on behalf of the client and documents regarding the broker's remuneration, by a period of 10 years from the date of termination of cooperation with the client.

The above provisions define the tasks and obligations of the insurance broker and the rules for providing services to clients.

The broker's activities for the client may consist in performing all or only some activities in the field of insurance distribution, e.g. collecting and analyzing insurance options available on the market, consulting, submitting and liquidating claims, negotiating with insurance companies as to the amount of benefits related to specific claims. Performing activities by the insurance broker that are covered by the catalog of tasks indicated, among others, in in article 4 sec. 1 point 3 above of the Act on Insurance Distribution, would argue for treating the broker - in the scope of processing personal data for this purpose - as the data controller. Such a status of a broker also results from other obligations of the broker specified in the provisions of the above-mentioned act (obligation to keep information secret or to keep documentation regarding the brokerage activity). A similar position has been taken many times by the President of the Personal Data Protection Office. In addition (as indicated by the supervisory authority in one of the decisions it issued), the need to recognize the insurance broker as the controller of personal data is also determined by the scope of competences specified in the above-mentioned of the act, expert knowledge, confirmed by a permit and an entry in the register of brokers, as well as the fact of being responsible for actions while performing brokerage activities.

In accordance with art. 5 sec. 1 lit. f) of Regulation 2016/679, personal data must be processed in a manner that ensures adequate security of personal data, including protection against unauthorized or unlawful processing and accidental loss, destruction or damage, using appropriate technical or organizational measures ("integrity and confidentiality "). This principle is specified in further provisions of the regulation.

In accordance with art. 5 sec. 2 of Regulation 2016/679, the administrator is responsible for compliance with the provisions of para. 1 and must be able to demonstrate compliance with them ("accountability"). As indicated in the Guidelines 07/2020 on the concepts of controller and processor contained in the GDPR (hereinafter referred to as: Guidelines 07/2020) of the European Data Protection Board (quote): "The purpose of including the principle of accountability in the GDPR and making it its main principle was to emphasize that data controllers must implement appropriate and effective measures and be able to demonstrate compliance with the regulations. The principle of accountability has been clarified in art. 24 (…). The accountability principle is also reflected in art. 28, which specifies the obligations of the administrator when using the services of the processing entity."

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

administrator implements appropriate technical and organizational measures so that the processing takes place in accordance with this regulation and to be able to demonstrate it . These measures are reviewed and updated if necessary. This means that the controller, when assessing the adequacy of security, should take into account the factors and circumstances regarding processing (e.g. type, method of data processing) and the risk associated with it. At the same time, the implementation of appropriate safeguards is an obligation that is a manifestation of the implementation of the general principle of data processing - the principle of integrity and confidentiality, set out in art. 5 sec. 1 lit. f) Regulation 2016/679. The implementation of technical and organizational measures should consist in the controller's implementation of relevant provisions, rules for the processing of personal data in a given organization, but also in regular reviews of these measures, and, if necessary, in updating previously adopted security measures. The principle of integrity and confidentiality, expressed in art. 5 sec. 1 lit. f) of 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.

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

Pursuant to Art. 28 sec. 1 of Regulation 2016/679, if the processing is to be carried out on behalf of the administrator, he uses only the services of such processing entities that provide sufficient guarantees for the implementation of appropriate technical and organizational measures so that the processing meets the requirements of this regulation and protects the rights of data subjects. In accordance with art. 28 sec. 3 Regulation 2016/679, processing by the processor takes place on the basis of a contract or other legal instrument that is subject to Union law or Member State law and binds the processor and the controller, specify the subject and duration of processing, the nature and purpose of processing, the type of personal data and categories of data subjects, obligations and rights of the administrator. This agreement or other legal instrument provides in particular that the processor: a) processes personal data only on the documented instructions of the administrator - which also applies to the

transfer of personal data to a third country or an international organization - unless such an obligation is imposed on it by Union law or the law of a state the Member State to which the processor is subject; in this case, before starting the processing, the processing entity informs the controller of this legal obligation, unless this law prohibits the provision of such information due to important public interest; b) ensures that persons authorized to process personal data have committed themselves to secrecy or are subject to the relevant statutory obligation of secrecy; c) take all measures required under Art. 32;d) complies with the terms of use of the services of another processor referred to in sec. 2 and 4;e) taking into account the nature of the processing, as far as possible, helps the controller through appropriate technical and organizational measures to meet the obligation to respond to the requests of the data subject in the exercise of his rights set out in Chapter III;f) taking into account the nature of processing and the information available to him, helps the administrator to fulfill the obligations set out in art. 32-36; g) upon completion of the provision of processing services, depending on the controller's decision, deletes or returns all personal data to him and deletes any existing copies thereof, unless Union or Member State law requires the storage of personal data; h) provides the controller with all information necessary to demonstrate compliance with the obligations set out in this article and enables and contributes to the administrator or an auditor authorized by the administrator to conduct audits, including inspections.

In connection with the obligation set out in the first paragraph, point h) the processor immediately informs the controller if, in its opinion, the instruction given to it constitutes a breach of this Regulation or other provisions of the Union or a Member State on data protection.

From the content of art. 32 sec. 1 of Regulation 2016/679 shows that the controller and the processor are required to apply technical and organizational measures corresponding to the risk of violating the rights and freedoms of natural persons with different probability of occurrence and severity of the threat. The provision specifies that when deciding on technical and organizational measures, the state of technical knowledge, the cost of implementation, the nature, scope, context and purposes of processing as well as the risk of violating the rights or freedoms of natural persons with different probability and severity should be taken into account. The quoted provision shows that the determination of appropriate technical and organizational measures is a two-stage process. First of all, it is important to determine the level of risk associated with the processing of personal data, taking into account the criteria indicated in art. 32 of Regulation 2016/679, and then it should be determined what technical and organizational measures will be appropriate to ensure a level of security corresponding to this

risk. These arrangements, if applicable, in accordance with point b) and d) of this article should include measures such as the ability to continuously ensure the confidentiality, integrity, availability and resilience of processing systems and services, and regularly test, measure and evaluate the effectiveness of technical and organizational measures to ensure the security of processing.

Article 32 sec. 2 of Regulation 2016/679 provides that when assessing whether the level of security is adequate, the risk related to processing is taken into account, in particular resulting from accidental or unlawful destruction, loss, modification, unauthorized disclosure or unauthorized access to personal data sent , stored or otherwise processed.

The provisions of Regulation 2016/679 therefore impose certain obligations in the field of ensuring the security of processed personal data on both controllers and processors. In accordance with art. 32 sec. 1 and 2 of Regulation 2016/679, both types of these entities are required to adopt appropriate technical and organizational measures to ensure a level of security corresponding to the risk associated with the processing of personal data. In the case in question, it is therefore first necessary to check whether the relevant entities, before taking actions aimed at introducing changes to the IT system, properly conducted the above-mentioned two-stage process, i.e.: 1) whether they analyzed the risk associated with such actions, as the separation of a joint working resource containing a file repository and making it available to employees in the local network and remotely is an action introducing a change in the current course of the personal data processing process and as such should be preceded by detailed analyzes in terms of determining the impact of this activity on the security of data processed in the system,2) whether (based on the above-mentioned analysis) determined and applied technical and organizational measures to ensure the level of security of personal data processed in this system corresponding to this risk (and also whether they verified whether the data was effectively secured in the location to which they were replicated).

In order for the risk analysis to be carried out properly, it is necessary to fully understand the structure of all elements of the data processing system, both for the processing itself and its protection against - in this case - unauthorized access. It should also be emphasized that any changes to the IT systems used to process personal data require the data controller, as well as the processor, to first verify whether the risk analysis carried out so far takes into account the risks associated with this activity. If not, it is their duty to carry out such an analysis to identify these threats and define security measures reducing the probability of their occurrence to the level of acceptable risk. As indicated by the Provincial Administrative Court in Warsaw in the judgment of September 3, 2020, file ref. II SA/Wa 2559/19, regulation 2016/679 "(...) introduced an approach in which risk

management is the foundation of activities related to the protection of personal data and is a continuous process. Entities processing personal data are obliged not only to ensure compliance with the guidelines of the above-mentioned regulation through a one-time implementation of organizational and technical security measures, but also to ensure the continuity of monitoring the level of threats and ensuring accountability in terms of the level and adequacy of the introduced security measures. This means that it becomes necessary to be able to prove to the supervisory authority that the solutions introduced to ensure the security of personal data are adequate to the level of risk, as well as take into account the nature of the organization and the mechanisms used for processing personal data.

The consequence of this orientation is the resignation from lists of requirements in the field of security imposed by the legislator, in favor of self-selection of security measures based on threat analysis. The administrators are not provided with specific security measures and procedures. The administrator is to independently conduct a detailed analysis of the conducted data processing processes and perform a risk assessment, and then apply measures and procedures that will be adequate to the assessed risk."

In the light of the aforementioned judgment of the Provincial Administrative Court in Warsaw, it should be emphasized that risk analysis and risk management are processes that require the cooperation of all interested parties and as such require, above all, planning, organizing, managing and controlling resources used for processing, carrying out the processing activities themselves, and examining and detecting possible vulnerabilities and vulnerabilities. In particular, it is necessary to analyze the impact of each change on the level of security of the processed data. Consequently, before taking any actions, including introducing changes to the existing data processing process aimed at providing employees with remote access to files, the data controller and processing entity should exercise the utmost caution, and before implementing the change itself, they should define the rules its implementation, especially in the context of ensuring an appropriate level of security of the processed data, and check whether the operation was completed successfully not only in terms of system efficiency, but also in terms of meeting the requirements of the law (including the provisions of Regulation 2016/679 imposing obligations in the field of ensuring an appropriate level of data security). However, in the present case, such a targeted analysis was not carried out, limiting itself only to general assumptions. This is indicated by the explanations of the Processing Entity, which assured that it applies internal regulations (...), including, among others, Policy (...) providing for a risk-based approach (requiring constant identification and estimation of the level of risk related to the processing of personal data) and that (quote): "(...)

activities aimed at providing access to files to employees (...) working remotely were carried out by (…) taking into account the risk associated with the implementation of such a solution". The Processing Entity also noted that (quote): "The technical and organizational measures used in this regard were subject to an analysis, prior to their implementation, taking into account the risks associated with remote work. (…) In the assessment (…), as a result of the implemented solutions, the probability of the occurrence of threats related to the activities carried out has been reduced to the level of acceptable risk". In its explanations, the Administrator also indicated its use of a risk-based approach and the Processor's obligation to apply this approach, and then explained that (quote): "(...) assumes that in connection with this commitment, the ASI technical and organizational measures have been analyzed taking into account the risks associated with remote work, and the probability of these threats has been reduced to the level of acceptable risk." When assessing the correctness of the actions of the Administrator and the Processing Entity in the above context, it should be emphasized that the analysis in question is performed by both of these entities, and not only by the Processing Entity, hence the Administrator's arguments are unfounded here (this obligation cannot rest only on the Processing Entity).

The findings made in this case allow us to assume that the Administrator and the Processor performed an insufficient analysis of the risk related to the actions taken to provide access to personal data to employees working remotely (including: they did not conduct a risk analysis related to finding personal data in an unsecured location), while its proper conduct would allow for the selection of appropriate security measures. For the proper implementation of the second stage of the above-mentioned process, since the necessary condition is the correct execution of the first stage preceding it. In the case of the above the work undertaken by (...) in the case in question, the risk of unintended replication of data and placing them in a location accessible to unauthorized persons had to be taken into account. Taking this risk into account, entities on which obligations are imposed pursuant to Art. 32 sec. 1 and 2 of Regulation 2016/679, could decide, for example, to set access passwords to folders containing personal data or to subject files containing such data to encryption or pseudonymization. This would avoid a breach of personal data protection even in the event of accidental sharing of copied files with unauthorized persons.

In the case in question, the Administrator limited himself to instructing the Processing Entity to make changes to the system aimed at providing access to personal data to employees working remotely, assuming that the Processing Entity will take into account the general principles of operation resulting from the above. Policy (...) (i.e. a risk-based approach), will analyze the risk associated with such activities and select appropriate technical and organizational measures to ensure the security of this

data. However, the obligations in this regard rest on both the Administrator and the Processing Entity, and the fact of taking action by one of them does not affect the release of the other from the obligations imposed on them by the provision of art. 32 sec. 1 and 2 of Regulation 2016/679. The findings made in this case do not allow to assume that the Administrator has taken steps to implement the two-stage process referred to in the above-mentioned recipe. Also, the Processing Entity did not demonstrate, in a way that did not raise serious doubts, the correctness of its actions - in particular, it did not verify the correctness of the process of changes made to the system (it was only checked whether employees had access to the data). As mentioned above, (...) indicated in a letter (received by the local Office on [...] February 2022) that in its opinion (quote): "(...) adequate means of authorization and security of the remote environment were used work, in particular in this respect: - the server was used (...) by separating the resource to which the files were copied, - antivirus protection and protection against attacks were applied for the separated resource, - the resource was made available in the local network and made available remotely by using the built-in in (...) the server (...), which was secured with encryption (...), - a mechanism was used (...) for additional protection of the shared resource by means of its replication to a separate local server (...)".

The selection of the above technical and organizational measures additionally (apart from the above-quoted explanations of the Administrator and the Processing Entity) proves that the risk analysis (related to the separation of a new resource and sharing files therein with employees working remotely) does not take into account the possibility of unintentional data replication and their placement in a location unsecured against access unauthorized persons. These measures were not adequate to this type of risk. They did not include, for example, encryption of the copied data, which was mentioned earlier in the justification for this decision, or securing file folders (or the files themselves) with access passwords.

It is obvious that when selecting technical and organizational measures, their effectiveness should be verified taking into account the current technical capabilities as well as potential threats. Measures that were appropriate in the past do not have to remain effective in changed circumstances. It should also be remembered that measures, even appropriately selected to the current possible risk of personal data breach, should be regularly tested. These activities (consisting in constant verification of the adequacy and effectiveness of the selected measures and regular testing of those already used) constitute - as a certain whole - the implementation of the obligation provided for in Art. 32 sec. 1 lit. b) Regulation 2016/679 (ability to ensure confidentiality at all times).

In the situation of separating a common working resource containing a repository of files (and thus: personal data contained

therein) and making it available to employees in the local network and remotely, it seems clear that tests should be carried out regarding the security measures used both before and after making this data available in a new location. Their proper conduct would have made it possible to detect the resulting error, i.e. making the resource unprotected against access by unauthorized persons also available in the wrong location, which was the direct cause of the personal data breach. The obligation to conduct such tests, in accordance with Art. 32 sec. 1 lit. d) of Regulation 2016/679, rests with both the processing entity and the data controller. The administrator provided the supervisory authority with information on the manner in which he and (...) M.H. involved in the processing of the data affected by the breach regularly tested, measured and assessed the effectiveness of technical and organizational measures to ensure the security of personal data being processed in IT systems whose the infringement concerns. As mentioned above, (...) in a letter received by the local Office on: - [...] December 2020, he indicated that the testing was carried out (quote): "(...) by performing current updates of the station working hours, server firmware updates (…) and virus scanning. ASI regularly tested, measured and assessed the effectiveness of technical measures to ensure the security of personal data being processed in the IT systems affected by the breach"; - [...] January 2021, stated that (quote): "Before the breach occurred (...) did not perform penetration tests. Reports on tests of the correct operation of IT systems and devices on behalf of (...) were performed by ASI (M. H.)", and also that (quote): "The tests were carried out immediately after the breach by a professional external entity (...), during the security audit and organization of IT infrastructure".(...) (in a letter received by the local Office on [...] May 2021) he explained that (quote): "(...) regularly tested, measured and assessed the effectiveness of the measures technical and organizational requirements to ensure the security of processed personal data in IT systems (...). All IT systems were regularly updated to eliminate possible errors and tested for vulnerabilities using anti-virus and anti-malware software" and provided copies of system/device test reports with the dates: [...] November, [...] and [...] December 2020, and also indicated that he actively participated in tests carried out by an external entity during the IT infrastructure security audit.

The above explanations do not prove regular testing of the technical and organizational measures used to protect the processed personal data in the event of changes to the Administrator's systems. Performing monthly tests (including verification in the following scope: in the case of servers: (...), and in the case of computers: (...)) seems to be too general and does not allow detecting errors such as the one in this case (unintended replication of data). As already indicated, the correct selection of technical and organizational measures, taking into account possible risks, and regular testing, including also

verification of the correctness of changes made to the systems, would allow in this situation to avoid a breach of personal data protection. It should be assumed that the obligations of entities participating in the processing of personal data should not end with the above-mentioned a two-stage process, i.e. conducting a risk analysis and applying appropriate technical and organizational measures to ensure the security of the processed personal data. As a consequence of this assumption, it should be stated that both the Administrator and the Processor should have verified whether personal data was effectively made available only in the intended location, and whether it is properly secured against access by unauthorized persons. The lack of such verification, due to the failure to implement any technical and organizational measures aimed at securing personal data (e.g. by using a password required to open all files or folders of files containing personal data) located in new locations where the data was made available, resulted in the infringement in question. Activities in the field of implementing appropriate technical measures were carried out only after the breach of personal data protection in question occurred.

In the light of the above findings, it should be stated that the lack of action by both the Administrator and the Processing Entity to conduct a risk analysis for the purposes of the change regarding the data processed in the IT system, determine and apply adequate technical and organizational measures to ensure data security during this operation and verification of the effectiveness of the correctness of the changes made, resulted in a violation of Art. 32 sec. 1 and 2 of Regulation 2016/679. Properly conducted testing as part of the implementation of the requirement of Art. 32 sec. 1 lit. d) should also cover the replicated resource and allow for verification whether the selection of the introduced security measures (which should be tested for their effectiveness already at the stage of implementing this solution) was appropriate. Meanwhile, e.g. as a result of inadequate verification of the correctness of the actions taken, neither the Administrator nor the Processing Entity realized for about three weeks that there had been an unintentional publication of personal data of 2,494 people - the violation was detected by accident (due to the suspicion of infecting the system with a virus) and as a result simultaneous information provided by a third party. Irregularities in this area obviously also affect the assessment of the Administrator's and the Processor's fulfillment of their obligation under Art. 32 sec. 1 lit. b) Regulation 2016/679 (ability to ensure confidentiality at all times).

Discussing the obligations arising from art. 32 sec. 1 lit. d), it should also be noted that the Administrator conducted audits of the security status and organization of the IT infrastructure, as part of which the activities of the Processing Entity were assessed, only after identifying a breach of personal data security - unfortunately, this action was delayed. It should also not be

forgotten that the controller's supervision over the activities of the processor is an important organizational measure aimed at protecting the security of the processed personal data.

It should also be pointed out that the obligations to implement appropriate technical and organizational measures to ensure that the processing is carried out in accordance with Regulation 2016/679 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 controller data) by the provisions of art. 24 sec. 1 and art. 25 sec. 1 above-mentioned regulation. Due to the Administrator's failure to apply adequate security measures, as mentioned above, it should be considered that he also violated these provisions of Regulation 2016/679. The consequence of their violation is the need to state that the confidentiality principle expressed in art. 5 sec. 1 lit. f) of Regulation 2016/679, as well as the accountability principle referred to in Art. 5 sec. 2 of Regulation 2016/679, obliging the administrator to comply with the rules resulting from art. 5 sec. 1 of Regulation 2016/679 and demonstrating this compliance. The above is confirmed by the decision of the Provincial Administrative Court in Warsaw of February 10, 2021, ref. II SA/Wa 2378/20: "The accountability principle is therefore based on the controller's legal responsibility for the proper fulfillment of duties and imposes on him the obligation to demonstrate, both to the supervisory authority and to the data subject, evidence of compliance with all data processing principles."

Similarly, the issue of the principle of accountability is interpreted in the judgment of August 26, 2020 by the Provincial Administrative Court in Warsaw, reference number II SA/Wa 2826/19: "Taking into account all the standards of Regulation 2016/679, it should be emphasized that the administrator has considerable freedom in terms of the security measures used, but at the same time is responsible for violating the provisions on the protection of personal data. The principle of accountability directly implies that it is the data controller who should demonstrate, and thus prove, that he complies with the provisions set out in Art. 5 sec. 1 of Regulation 2016/679".

In view of the above, that the Administrator and the Processor have failed to fulfill the obligations imposed on each of them, as specified in art. 32 sec. 1 and 2 of Regulation 2016/679 in the field of risk analysis and the selection of appropriate technical and organizational measures to ensure the security of the processed data, it is worth making an additional in-depth analysis of certain aspects of the relationship between these two entities (including in the context of Article 32(1) and Article 28 section 3 of Regulation 2016/679), i.e. whether the activities of the Processing Entity were carried out in accordance with the established procedures (and if not, whether the Administrator provided the Processing Entity with information on how to introduce changes

to the IT system), in how the rights and obligations of the above were shaped entities in this regard and whether the Administrator has properly verified whether the Processing Entity guarantees the proper performance of its tasks.

In the explanations received by this Office on [...] February 2021, the Administrator indicated, inter alia, that in accordance with the concluded contract for entrusting the processing of personal data, the processing of personal data by the Processor takes place as part of the infrastructure (...) on the terms set out in the internal documentation and procedures, and also that in this respect it is subject to the same ongoing control as the Administrator's employees. Unfortunately, the "Policy (...)" (constituting Annex No. (...) to the letter received by the local Office on [...] December 2020) does not contain detailed provisions on how to make changes to the IT systems used to process personal data . In particular, it has not been specified that the entity making any changes to this system is required to verify the correctness of the actions taken or control (current and as-built) in the scope of securing personal data being processed against access by unauthorized persons. From the annex to the above of the Policy, i.e. from the Instruction (...), it only follows that at the point of contact of the Data Administrator's computer network with the public network, there are (...) devices that prevent unauthorized access from outside to its resources, and also allow control of the flow of data (chapter (...) of the above-mentioned Instruction), which in the analyzed case seems insufficient. This lack is also accompanied by the fact that the Administrator has not been shown to supervise the activities undertaken by the Processor in order to enable employees to work remotely and (as already mentioned in the earlier part of this justification) to verify the correctness of the process of changes made in its systems.

The explanations provided by the Administrator at the request of [...] February 2022 show that the decision to introduce changes was made by the Administrator, and the method of carrying out activities aimed at providing access to files to employees who are to work was determined by the Processing Entity (as a person responsible for the IT infrastructure in (...)). It should be noted that in the case in question, the breach of personal data protection (data leakage) occurred as a result of an error by the Processing Entity, which, by separating a new resource for employees (...) who are to work remotely, unintentionally replicated data in the Administrator's domain, which data was not protected against unauthorized access.

Meanwhile, in accordance with the wording of art. 28 sec. 1 of Regulation 2016/679, if the processing is to be carried out on behalf of the administrator, he 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 persons whose data applies. The implementation of this principle is ensured by

the introduction in art. 28 sec. 3 of Regulation 2016/679, the obligation to conclude an agreement between the administrator and the processing entity specifying the subject and duration of processing, the nature and purpose of processing, the type of personal data and the categories of data subjects, the obligations and rights of the administrator, which agreement contains in particular the elements indicated in lit. a)-h) of this provision. In the considered facts, the Agreement (...) concluded between the Administrator and the Processing Entity on [...] April 2020 did not, however, contain the elements indicated in art. 28 sec. 3 lit. c), e) and f). However, this agreement in § (...) specified (in reference to the obligation provided for in Article 28(3)(a) of Regulation 2016/679) that in connection with entrusting the processing of personal data (...) undertakes to process personal data only on the basis of this agreement or on another documented instruction of the Administrator, which is considered to be an instruction sent in writing or electronically.

In accordance with art. 28 sec. 3 lit. a) of Regulation 2016/679, the processor processes personal data only on documented instructions from the controller - which also applies to the transfer of personal data to a third country or an international organization - unless such an obligation is imposed on it by Union law or the law of the Member State to which the processor is subject; in this case, before starting the processing, the processing entity informs the controller of this legal obligation, unless the law prohibits providing such information due to important public interest. Article 28 par. 3 lit. c) of Regulation 2016/679 requires the processor to take all measures required under Art. 32. Pursuant to Art. 28 sec. 3 lit. e) of Regulation 2016/679, the processing entity, taking into account the nature of the processing, shall, if possible, help the controller through appropriate technical and organizational measures to meet the obligation to respond to the requests of the data subject in the exercise of his rights set out in Chapter III. Pursuant to art. 28 sec. 3 lit. f) of Regulation 2016/679, taking into account the nature of the processing and the information available to it, the processing entity helps the controller to meet the obligations set out in art. 32 - 36.

Based on the explanations provided by the Administrator and the Processing Entity, it is impossible to confirm that the implemented changes were implemented in accordance with predetermined rules ensuring the security of personal data - technical and organizational measures to ensure this security were not specified either in the general regulations implemented by the Administrator or in an appropriate agreement concluded with the Processing Entity. Moreover, the instruction to make changes to the IT system (...) in order to enable its employees to work remotely was not provided by the Administrator together with any instructions as to the methods of ensuring the security of the processed data. On the contrary: the Processing Entity

was to decide on the method of their implementation. The freedom to choose the solutions used by the Processing Entity, combined with the lack of implemented procedures for checking the correctness of the activities undertaken in this regard, resulted in a breach of personal data protection.

In view of the above (i.e. finding that the Processing Entity was left to decide how to perform activities in the field of introducing changes to the IT system), it should be additionally analyzed whether such action by the Administrator could result from reasonable certainty as to the competence of the Processing Entity. In the case in question, the Administrator indicated that cooperation with the Processing Entity began long before the entry into force of the provisions of Regulation 2016/679 (i.e. from 2010). The explanations submitted by (...) in this regard also show that the verification of the Processing Entity's competences was not formalized (it consisted in conducting a conversation), the cooperation is direct, and the services provided by ASI within its framework do not raise the Administrator's objections as to their quality and punctuality. Referring to the aforementioned of the Administrator's explanations, it should be indicated that: - in the previous legal status, on the basis of the Act of August 29, 1997 on the Protection of Personal Data (Journal of Laws of 2016, item 922), other requirements were defined for the processing entity, and other have been in force since May 25, 2018, i.e. from the date of application of Regulation 2016/679. Therefore, the cooperation so far, positively assessed, 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 controller who, as part of his business, uses the resources or services of the processing entity when processing personal data. It should be emphasized that the obligation to carry out such an assessment is not relieved by the fact of long-term cooperation and use of the services of a given processing entity before May 25, 2018, i.e. before the entry into application of Regulation 2016/679. The administrator did not carry out such verification, limiting itself to a positive assessment of the Processing Entity, which is the result of the existing cooperation established before the application of the provisions of Regulation 2016/679. The consequence of not making this assessment is the violation of the requirement set out in Art. 28 sec. 1 of Regulation 2016/679. It should be noted that the mere signing of an agreement to entrust the processing of personal data without making an appropriate assessment of the processor cannot be considered as the implementation of the obligation to carry out the procedure verifying the processor in terms of compliance with the requirements of Regulation 2016/679; - long-term cooperation of the parties not supported by

periodic, systematically conducting audits or inspections does not guarantee that the processing entity will correctly perform the tasks required by law and resulting from the concluded entrustment agreement. It should be noted here that the Agreement (...) connecting the Administrator and the Processing Entity from (...) April 2020 contains provisions regarding the right (...) to control the compliance of personal data processing by (...) and its obligation to answer the Administrator's questions regarding issues related to this processing - these activities could therefore have been carried out before the personal data protection breach occurred.

The issue of criteria for evaluating the processor was also discussed by the European Data Protection Board. As indicated in the Guidelines 07/2020, referring to the content of art. 28 sec. 1 and recital 81 of Regulation 2016/679, (quote): »The controller is (...) responsible for assessing the adequacy of the guarantees provided by the processor and should be able to prove that he seriously considered all the elements provided for in the GDPR. The guarantees "provided" by the processor are those that the processor is able to demonstrate to the satisfaction of the administrator, because these are the only guarantees that the administrator can effectively take into account when assessing the fulfillment of its obligations. This will often require the exchange of relevant documentation (e.g. privacy policy, terms of service, register of processing activities, documentation management policy, information security policy, external data protection audit reports, recognized international certificates such as ISO 27000 standards). The administrator's assessment of whether the guarantees are sufficient is a form of risk assessment, which largely depends on the type of processing entrusted to the processing entity and must be made individually for each case, taking into account the nature, scope, context and purposes of processing, as well as threats to the rights and freedom of individuals. (…) The controller should consider the following elements (…) to assess whether the guarantees are sufficient: expertise (e.g. technical knowledge of security measures and data breaches); credibility of the processor; resources of the processor. The reputation of the processor in the market may also be an important factor that controllers should consider. In addition, adherence to an approved code of conduct or certification mechanism may be used as an element to demonstrate sufficient assurances. (…) The obligation to use only the services of processors "providing sufficient guarantees" contained in art. 28 sec. 1 of the GDPR is a continuous obligation. It does not end when the contract or other legal act is concluded by the controller and the processing entity. Rather, the controller should verify the processor's guarantees at appropriate intervals, including, where appropriate, through audits and inspections (…)«.

To sum up the previous argument, it should be noted that the circumstances of placing the data in an unsecured location were

related to the actions taken to make these data available for the administrator's internal needs related to the organization of remote work, while the Processing Entity started its activities as a result of the Administrator's order that did not specify either the manner of performing the outsourced activity or security measures to be followed. Moreover, when carrying out this process, the Processing Entity did not exercise due diligence - changes in the IT system were not made on the basis of specific procedures, and the correctness of their course was not verified after (or during) their implementation. Therefore, the Processing Entity did not meet the requirements set out in the provisions of Art. 32 sec. 1 and 2 of Regulation 2016/679 - did not take actions under Art. 28 sec. 3 lit. c) and f) of Regulation 2016/679, according 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 administrator to fulfill the obligations set out in art. 32-36. When evaluating the actions taken by the Processing Entity, it should be taken into account not only that the § (...) "Agreement (...)" concluded between the Administrator and the Processing Entity states that (...) has undertaken that the activities covered by the subject of this will perform the contract with due diligence, according to the best knowledge and experience, but also the fact that the Report No. (...) conducted by an external auditor shows that the Processing Entity acted confident in the correctness of its activities.

The above leads to the conclusion that the reasons for the breach in question should also be sought in improper organization and management of the process of implementing new solutions in the IT infrastructure or making changes to it. It should be pointed out that the Administrator, at any stage of the introduced changes, did not supervise whether these changes actually proceed correctly and whether the processed personal data are protected against access by unauthorized persons (such supervision is an organizational measure to ensure the security of the processed personal data). As already mentioned in the earlier part of this justification, Art. 32 sec. 1 lit. d) of Regulation 2016/679, there is an obligation to regularly test, measure and evaluate the effectiveness of technical and organizational measures to ensure the security of processing. Reviewing and updating the implemented solutions are also a requirement expressly formulated in art. 24 sec. 1 of Regulation 2016/679, as well as resulting from Art. 25 sec. 1 of Regulation 2016/679, creating the obligation to ensure the protection of privacy in the design phase (privacy by design) and imposing an obligation on the controller to implement appropriate technical measures both at the phase of determining the processing methods and at the phase of processing itself (it should be emphasized again that the obligations set out in the provisions of Article 24(1) and 25(1) of Regulation 2016/679 are solely the responsibility of the administrator). The implementation of technical and organizational measures by the administrator is not a one-off action,

but should take the form of a process under which the administrator reviews and, if necessary, updates the previously adopted security measures. Such an assessment should cover not only technical measures, 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 for personal data processing. Regular assessment of the above. procedures, in accordance with the requirement resulting from art. 32 sec. 1 lit. d) of Regulation 2016/679, would allow the Administrator to verify whether these procedures do not show any shortcomings, and if not, whether such a procedure is effective, i.e. whether it ensures that appropriate actions are taken to ensure the protection of personal data during the process of making changes in the IT system and whether it is observed at all by persons responsible for carrying out these changes.

In the case in question, in the opinion of the President of the UODO, the Administrator's verification of the method of implementation by the Processing Entity of changes in the IT system in which personal data were processed would significantly reduce the risk of unauthorized persons gaining access to data processed in this system, and thus minimize the risk of violation the rights or freedoms of natural persons whose data are processed by (...), because the personal data protection violation occurred as a result of a simple error consisting in unintentional data replication, which should have been detected during the process of implementing changes in the IT system processing personal data. The result of the above omission was the lack of action (...) to ensure the security of the personal data of his clients, which he was obliged to do in accordance with the above-mentioned provisions of Regulation 2016/679, as the data controller. It should also be emphasized that the fact of using the services of a processing entity does not release the Administrator from fulfilling these obligations. The obligations in this regard rest primarily with the data controller. Analyzing the actions (and, in fact, the lack of actions of the Administrator in this regard), it can be concluded that he limited himself to notifying the Processor of the need to make modifications, without taking any actions to verify whether the security of processing personal data of his clients was ensured in the process of making changes to the system .

The material collected in the case also confirms that before the initiation of administrative proceedings, the Administrator did not carry out audits, including inspections, in the processing entity in order to check whether (...) properly fulfills its obligations under Regulation 2016/679 (including whether it ensures the application measures required under Article 32 of that Regulation). The possibility of conducting such audits, including inspections, results from Art. 28 sec. 3 lit. h) of Regulation 2016/679, according to which the personal data processing agreement is to provide that the processor provides the controller

with all information necessary to demonstrate compliance with the obligations set out in this article and enables the controller or an auditor authorized by the controller to conduct audits, including inspections, and contributes to them. Therefore, this provision gives the administrator some tools, the use of which can ensure that the processing of entrusted data will comply with the provisions of Regulation 2016/679, and the administrator will avoid liability for their violation. It should be emphasized that the controller's performance of audits, including inspections, in the processing entity should be treated as one of the most important security measures that the controller should apply in order to properly fulfill its obligations under Art. 32 sec. 1 of Regulation 2016/679. The controller should, when using the services of the processing entity, know whether and how the entity entrusted with the processing of personal data meets the requirements set out in Regulation 2016/679. There is no doubt that the most effective way for the controller to ensure this knowledge is to conduct appropriate audits, including inspections, in the processing entity. However, she did not apply such security measures, which consequently contributed to the occurrence of a personal data protection breach. Moreover, the use of the above 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 (before the audit carried out as a result of the breach of personal data protection in question), 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 determining the processing methods, but also during the processing itself. Continuity inherent in the analyzed obligation may therefore in practice manifest itself, among others, in in the need to ensure regular monitoring of the security measures applied and to conduct constant supervision over the processing entity through e.g. audits and inspections referred to in art. 28 sec. 3 lit. h) Regulation 2016/679.

In the opinion of the President of the UODO, the technical and organizational measures used by the Administrator met the requirements set out in Art. 32 of Regulation 2016/679, due to the fact that he did not implement appropriate procedures to ensure the security of the processed data in the process of changes made to the IT system in which these data are processed, and did not supervise the Processing Entity in the scope of activities carried out to make the resource available employees to work remotely. It should be emphasized that the supervision and monitoring of development work on systems commissioned to

external entities by the data controller is one of the basic organizational measures that the controller should effectively implement in order to ensure the security of personal data in accordance with the requirements of Regulation 2016/679.

As a consequence of (…) not applying the above rules, the foreseeable risks have not been properly minimized and limited during processing.

It should be recognized that the application of appropriate security standards in the field of introducing changes to IT systems used to process personal data, including their verification in terms of security, and in particular meeting the requirements of 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 Processing Entity's activities in this regard, 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, 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 adopted measures are to be effective (...)" and "(...) activities of a technical and organizational nature are the responsibility of the personal data administrator, but cannot be selected in a way completely free and voluntary, without taking into account the degree of risk and the nature of the protected personal data", 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 that ensures their appropriate security and appropriate 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)'.

To sum up, the findings do not give grounds to conclude 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 ensured effective implementation of data protection principles. As a consequence, in the opinion of the President of the UODO, both (...) and (...) did not implement appropriate technical and organizational measures to ensure the security of processing personal data contained in the IT system subject to modification, which constitutes a violation of Art. 32 sec. 1 and 2 of Regulation 2016/679.

When making this summary, it is necessary to repeat the arguments contained in the previous part of the justification, which

show that the obligations to implement appropriate technical and organizational measures to ensure that the processing is carried out in accordance with Regulation 2016/679 and to provide the processing with the necessary safeguards to meet the requirements of this Regulation, were imposed on the data controller (and only on the data controller) by the provisions of Art. 24 sec. 1 and art. 25 sec. 1 of Regulation 2016/679. In the absence of (...) adequate security measures, as referred to above, it should be considered that the Administrator also violated these provisions of Regulation 2016/679. The consequence of their violation is the need 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, the data should be "processed in a manner that ensures adequate security of personal data, including protection against unauthorized or unlawful processing and accidental loss, destruction or damage, using appropriate technical or organizational measures". It should be emphasized that proper and effective data protection has been raised in Regulation 2016/679 to the rank of a general rule, which proves that the issue of ensuring data confidentiality should be treated in a special and priority way by the data controller. Meanwhile, as has already been demonstrated in the justification for this decision, both the Administrator and the Processor failed to implement appropriate technical and organizational measures to ensure the security of personal data processing, which led to a breach by (...) their confidentiality in connection with the occurrence of a personal data protection breach, i.e. violation of the principle referred to in art. 5 sec. 1 lit. f) Regulation 2016/679. As shown in this justification, the Administrator also violated the provision of art. 5 sec. 2 of Regulation 2016/679 (defining the principle of accountability) and the provision of art. 28 sec. 1 of Regulation 2016/679. In addition, the Entrustment Agreement concluded by the Administrator with the Processing Entity did not contain the elements specified in art. 28 sec. 3 lit. c), e) and f) of Regulation 2016/679, i.e. it did not specify that the processor: - takes all measures required under art. 32;- taking into account the nature of the processing, as far as possible, helps the controller through appropriate technical and organizational measures to meet the obligation to respond to the requests of the data subject in the exercise of his rights set out in Chapter III;- taking into account the nature of the processing and available information, helps the administrator to meet the obligations set out in art. 32-36.

Meanwhile, the Guidelines 07/2020 indicate that (quote): "Although the elements specified in Art. 28 of the Regulation constitute its core content, the contract should be a way for the controller and the processor to further explain how to implement these essential elements with detailed instructions", and that (quote): "In any case, the contract must cover all elements of Art. 28 sec. 3. At the same time, the contract should contain certain elements that may help the processor

understand the risks to the rights and freedoms of data subjects resulting from the processing: because the activity is performed on behalf of the controller, the controller often has a better understanding of the risks posed by processing because he is aware of the circumstances in which the processing takes place." The contract, on the other hand, should be made in writing, which was also emphasized in the above-mentioned Guidelines (quote): "(...) unwritten agreements (regardless of their degree of detail or effectiveness) cannot be considered sufficient to meet the requirements set out in Art. 28 GDPR".

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

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

In accordance with art. 83 sec. 4 lit. a) of Regulation 2016/679, violation of the provisions on the obligations of the administrator and the processing entity referred to in art. 8, 11, 25-39 as well as 42 and 43 are subject in accordance with sec. 2, an administrative fine of up to EUR 10,000,000, and in the case of an enterprise - up to 2% of its total annual worldwide turnover from the previous financial year, with the higher amount applicable.

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

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

In this case, an administrative fine against the Administrator was imposed for violation of Art. 25 sec. 1, art. 28 sec. 1 and 3, art. 32 sec. 1 and 2 of Regulation 2016/679 on the basis of the above-mentioned art. 83 sec. 4 lit. a) of Regulation 2016/679, while for violation of Art. 5 sec. 1 lit. f) and art. 5 sec. 2 of Regulation 2016/679 - pursuant to art. 83 sec. 5 lit. (a) of this regulation. At the same time, a penalty in the amount of the equivalent of EUR 7,000.00 imposed on the Processor jointly for violation of all the above provisions - pursuant to the provision of art. 83 sec. 3 of Regulation 2016/679 - does not exceed the amount of the fine for the most serious violation found in this case, i.e. violation of Art. 5 sec. 1 lit. f) and art. 5 sec. 2 of Regulation 2016/679, which, pursuant to Art. 83 sec. 5 lit. a) of Regulation 2016/679 is subject to an administrative fine of up to EUR 20,000,000, and in the case of an enterprise - up to 4% of its total annual worldwide turnover from the previous financial year.

Administrative fine imposed on the Administrator for violation of art. 32 sec. 1 and 2 and art. 32 sec. 1 and 2 in connection with art. 28 sec. 3 lit. c) and f) of Regulation 2016/679 is based on Art. 83 sec. 4 lit. a) Regulation 2016/679.

Moreover, it should be pointed out that pursuant to Art. 58 sec. 2 lit. d) of Regulation 2016/679, each supervisory authority has a corrective power in the form of ordering the controller or processor to adapt the processing operations to the provisions of this regulation, and, where appropriate, indicate the method and date.

When deciding to impose an administrative fine on (...), the President of the UODO - pursuant to art. 83 sec. 2 lit. a-k of Regulation 2016/679 - took into account the following circumstances of the case, aggravating and affecting the amount of the imposed financial penalty:

1. The nature, weight and duration of the infringement, taking into account the nature, scope or purpose of the given processing, the number of data subjects affected and the extent of the damage suffered by them (Article 83(2)(a) of Regulation 2016/679). In imposing the penalty, it was important that the violation of the provisions of Regulation 2016/679, imposing obligations on the administrator to apply appropriate technical and organizational measures to ensure the security of the processed personal data, had an impact on the breach of confidentiality of the data of 2,494 people. The breach of personal data protection found in this case, consisting in allowing unauthorized persons to access personal data, is of considerable

importance and serious in nature, as it may lead to material or non-material damage to the person whose data has been breached, and the probability of their occurrence is high. In addition, the risk arising from the wide range of data covered by the breach, the relatively large number of data subjects, as well as the relatively large scale and professional nature of data processing should be taken into account. It should be emphasized that in relation to persons whose data have been breached, there is still a high risk of unlawful use of their personal data, because the purpose for which unauthorized persons downloaded the mistakenly shared data is unknown, and it is also unknown whether to further share this data. Therefore, data subjects may still suffer material damage, and the breach of data confidentiality itself also constitutes non-material damage (harm). At the very least, the data subject may fear losing control of their personal data, identity theft or identity fraud, or financial loss. In addition, it should be emphasized that the infringement occurring in the situation in question had special circumstances - the Administrator, as an insurance broker, was obliged pursuant to Art. 32 sec. 3 point 1 of the Act of December 15, 2017 on insurance distribution (Journal of Laws of 2022, item 905, as amended) to keep secret information obtained in connection with the performance of brokerage activities in the field of insurance (which obligation remains with the insurance broker even after termination of the contractual relationship with the principal). In addition, the information obtained by the supervisory authority in the course of the administrative proceedings shows that the resource containing files containing personal data of the Administrator's former and current clients remained unprotected against access by unauthorized persons (which is tantamount to loss of their confidentiality) from [. ..] November 2020 to [...] December 2020, i.e. for [...] days. It should be assumed that the violation of Art. 5 sec. 1 lit. f), art. 5 sec. 2, art. 25 sec. 1 and 32 sec. 1 and 2 of Regulation 2016/679 lasted at least at the same time, and the infringement of Art. 28 sec. 1 and 3 of this regulation lasts at least from [...] April 2020 (i.e. from the date of signing by (...) the contract for entrusting the processing of personal data with the Processing Entity).

2. 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 UODO allow to conclude that the Administrator did not fulfill its obligations in the field of supervision over the Entity Processors during the implementation of changes in the IT system used for personal data processing, which consequently led to freedom of action by the Processing Entity, i.e. making changes to the IT system without conducting current and post-implementation control of the correctness of the actions taken and securing the processed personal data against access by persons unauthorized. 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 responsibility of the

Administrator for breaching the confidentiality of personal data.

3. Categories of personal data affected by the breach (Article 83(2)(g) of Regulation 2016/679). Personal data accessed by unknown and unauthorized third parties include, among others, the special categories of personal data referred to in article 9 of Regulation 2016/679. At the same time, their wide range (i.e. names and surnames, address of residence or stay, PESEL registration number, e-mail address, series and number of ID card, telephone number and health data, which data were included, among others, in insurance policies natural persons) is associated with a high risk of violating the rights or freedoms of natural persons affected by the breach. It should be emphasized that, in particular, unauthorized disclosure of such a category of data as the PESEL registration number (in conjunction with the name and surname) may have a real and negative impact on the protection of the rights or freedoms of natural persons. PESEL registration number, i.e. an eleven-digit numerical symbol, uniquely identifying a natural person, containing, among others, date of birth and gender designation, and thus closely related to the private sphere of a natural person and also subject, as a national identification number, to exceptional protection under Art. 87 of Regulation 2016/679, is data of a special nature and requires such special protection. The fact that the data provided also included health data further increases the risk of violating the protection of the rights or freedoms of natural persons to whom these data relate.

When determining the amount of the administrative fine imposed on (…), the President of the UODO took into account the following premises as mitigating circumstances:

1. 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 intentional actions of the Administrator leading to the violation of the provisions of Regulation 2016/679.

2. 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 material damage on the part of the persons affected by the breach. It should be pointed out that immediately after the disclosure of the breach of personal data protection, even before the initiation of administrative proceedings, (...) took steps as a result of which the data was quickly secured against further breaches, i.e. against downloading by further unauthorized entities, and it was also agreed, among others, reason for the breach by commissioning relevant audits to a third party. The decision indicated as an aggravating circumstance that data subjects may still suffer material damage, and the breach of confidentiality of data itself is also non-material damage (harm), but taking quick action to

protect the data from being downloaded by other unauthorized entities should be assessed as a mitigating circumstance, because in the opinion of the President of the UODO, narrowing down the group of entities that may illegally download the data of the Administrator's clients should be considered as actions taken to minimize the damage suffered by the data subjects. In addition, (...) sent to the data subjects (and of whom he is the administrator) notifications of a breach of their personal data, containing all the data required in accordance with art. 34 sec. 2 of Regulation 2016/679 information.

3. Relevant previous violations of the provisions of Regulation 2016/679 (Article 83(2)(e) of Regulation 2016/679) - no relevant previous violations of Regulation 2016/679 were found in (...).

4. Degree of cooperation with the supervisory authority in order to remove the infringement and mitigate its possible negative effects (Article 83(2)(f) of Regulation 2016/679) - the administrator provided exhaustive explanations to the supervisory authority's calls and involved an external entity in corrective and preventive measures (conducting an audit and introducing appropriate changes).

5. Any other aggravating or mitigating factors applicable to the circumstances of the case, such as financial benefits gained directly or indirectly in connection with the infringement or losses avoided (Article 83(2)(k) of Regulation 2016/679). The President of the UODO did not state in the course of these proceedings that by committing a breach subject to a penalty (...) she achieved any financial benefits or avoided any financial losses.

The fact that the President of the UODO applied sanctions in the form of an administrative fine in this case to the Administrator in this case, as well as its amount, was not affected by other ones indicated in art. 83 sec. 2 of Regulation 2016/679 circumstances, that is:

1. The manner in which the supervisory authority found out about the breach (Article 83(2)(h) of Regulation 2016/679) - the President of the UODO found the breach as a result of reporting a breach of personal data protection by the Controller, however, due to the fact that the Controller by making this notification, he was only fulfilling his legal obligation, there are no grounds to consider that this circumstance is a mitigating circumstance. The fact that the supervisory authority later received information about this breach from other sources is irrelevant in this case. In accordance with the Guidelines on the application and determination of administrative fines for the purposes of Regulation No. 2016/679 Wp. 253 "The supervisory authority may become aware of a breach as a result of proceedings, complaints, articles in the press, anonymous tips or notification by the data controller. Pursuant to the regulation, the controller is obliged to notify the supervisory authority of a breach of personal

data protection. The mere fulfillment of this obligation by the controller cannot be interpreted as a mitigating factor.'

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

3. Application of approved codes of conduct under Art. 40 of Regulation 2016/679 or approved certification mechanisms under Art. 42 of Regulation 2016/679 (Article 83(2)(j) of Regulation 2016/679) - (…) 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 the Processor, the President of the UODO - pursuant to art. 83 sec. 2 lit. a-k of Regulation 2016/679 - took into account the following circumstances of the case, aggravating and affecting the amount of the imposed financial penalty:

1. The nature, gravity and duration of the infringement, taking into account the nature, scope or purpose of the given processing, the number of data subjects affected, and the extent of the damage suffered by them (Article 83(2)(a) of Regulation 2016/679). In imposing the penalty, it was important that the violation of the provisions of Regulation 2016/679, imposing obligations on the Processor to apply appropriate technical and organizational measures to ensure the security of the processed personal data, had an impact on the breach of confidentiality of the data of 2,494 people. The breach resulted from the Processor's failure to apply basic security rules consisting in failing to protect personal data against access by unauthorized persons. The processing entity providing professional services, e.g. in the field of operating IT systems and having appropriate knowledge in this area, he did not apply the security rules, e.g. without verifying the correctness of the processes being carried out. The violation of personal data protection found in this case, consisting in allowing unauthorized persons to access personal data, as a result of which, among others, the data of the Administrator's clients is of considerable importance and serious in nature, as it may lead to material or non-material damage to the person whose data has been breached, and the probability of their occurrence is high. In addition, the risk arising from the wide range of data covered by the breach, the relatively large number of data subjects, as well as the relatively large scale and professional nature of data processing should be taken into account. It should be emphasized that in relation to persons whose data have been breached, there is still a high risk of unlawful use of their personal data, because the purpose for which unauthorized persons downloaded the mistakenly shared data is unknown, and it is also unknown whether to further share this data. Therefore, data subjects may still suffer material damage, and the breach of data confidentiality itself also constitutes non-material damage

(harm). At the very least, the data subject may fear losing control of their personal data, identity theft or identity fraud, or financial loss. In addition, the information obtained by the supervisory authority in the course of the administrative proceedings shows that the resource containing files containing personal data of the Administrator's former and current clients remained unprotected against access by unauthorized persons (which is tantamount to loss of their confidentiality) from [. ..] November 2020 to [...] December 2020, i.e. for [...] days. It should be assumed that the violation of Art. 32 sec. 1 and 2 of Regulation 2016/679 lasted at least at the same time, and the infringement of Art. 32 sec. 1 and 2 in connection with joke. 28 sec. 1 and 3 of this regulation lasts at least from [...] April 2020 (i.e. from the date of signing by (...) the contract for entrusting the processing of personal data with the Processing Entity).

2. 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 us to conclude that the Processing Entity did not fulfill its obligations regarding the implementation of changes in IT systems , which consequently led to making changes to the IT system without conducting ongoing and post-execution control of the correctness of the actions taken and securing the processed personal data against access by unauthorized persons. The Processing Entity bears direct responsibility for the infringement, 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). Personal data accessed by unknown and unauthorized third parties include, among others, the special categories of personal data referred to in article 9 of Regulation 2016/679. At the same time, their wide range (i.e. names and surnames, address of residence or stay, PESEL registration number, e-mail address, series and number of ID card, telephone number and health data, which data were included, among others, in insurance policies natural persons) is associated with a high risk of violating the rights or freedoms of natural persons affected by the breach. It should be emphasized that, in particular, unauthorized disclosure of such a category of data as the PESEL registration number (in conjunction with the name and surname) may have a real and negative impact on the protection of the rights or freedoms of natural persons. PESEL registration number, i.e. an eleven-digit numerical symbol, uniquely identifying a natural person, containing, among others, date of birth and gender designation, and thus closely related to the private sphere of a natural person and also subject, as a national identification number, to exceptional protection under Art. 87 of Regulation 2016/679, is data of a special nature and requires such special protection. The fact that the data

provided also included health data further increases the risk of violating the protection of the rights or freedoms of natural persons to whom these data relate.

When determining the amount of the administrative fine imposed on the Processor, the President of the UODO took into account the following mitigating circumstances:

1. Unintentional nature of the infringement (Article 83(2)(b) of Regulation 2016/679) - the President of the UODO did not find in this case intentional actions of the Processing Entity leading to the state of violation of the provisions of Regulation 2016/679.

2. 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 breach, however, it should be indicated that immediately after the disclosure of the breach of personal data protection, even before the initiation of administrative proceedings, (…) he took steps as a result of which the data was quickly secured against further breaches, i.e. against downloading them by further unauthorized entities, and then participated in the relevant audits carried out by an external entity during which the reason for the infringement was established. The decision indicated as an aggravating circumstance that the data subjects may still suffer material damage, and the breach of confidentiality of data itself is also non-material damage (harm), but taking quick action to protect the data from being downloaded by other unauthorized entities should be assessed as a mitigating circumstance, because in the opinion of the President of the UODO, narrowing down the group of entities that may illegally download the data of the Administrator's clients should be considered as actions taken to minimize the damage suffered by the data subjects.

3. Relevant previous violations of the provisions of Regulation 2016/679 (Article 83(2)(e) of Regulation 2016/679) - no relevant previous violations of Regulation 2016/679 were found in (...).

4. Any other aggravating or mitigating factors applicable to the circumstances of the case, such as financial benefits achieved directly or indirectly in connection with the infringement or losses avoided (Article 83(2)(k) of Regulation 2016/679) - the President of the UODO did not state in in the course of these proceedings that by committing a punishable infringement, the Processing Entity has achieved any financial benefits or avoided any financial losses. In addition, immediately after the disclosure of the breach of personal data protection, the Processing Entity took steps, as a result of which the data was quickly secured against further breaches, and participated in carrying out the relevant above-mentioned audits by a third party. In the course of the proceedings, the Processing Entity provided extensive explanations indicating, inter alia, how the error occurred,

which resulted in a violation of personal data protection, and also drew attention to the state of its health, which objectively affects its financial situation.

The fact that the President of the UODO applied sanctions in the form of an administrative fine to the Processor in this case, as well as its amount, was not affected by other ones indicated in art. 83 sec. 2 of Regulation 2016/679 circumstances, that is:

1. Degree of cooperation with the supervisory authority to remove the infringement and mitigate its possible negative effects (Article 83(2)(f) of Regulation 2016/679). In the course of the proceedings, the Processing Entity did not take any additional steps in connection with the statements of the authority. However, prior to the initiation of the proceedings, independent actions were taken by (…) to remove the source of the infringement. These activities, however, were autonomous; The President of the UODO cannot treat them as taken in cooperation with the supervisory authority and therefore cannot assess the "degree" of this cooperation. However, these actions were taken into account above as a mitigating circumstance specified in Art. 83 sec. 2 lit. c of Regulation 2016/679.

2. The manner in which the supervisory authority found out about the breach (Article 83(2)(h) of Regulation 2016/679) - the President of the UODO found the breach as a result of reporting a breach of personal data protection made by the Administrator. When making this notification, the administrator only fulfilled the legal obligation imposed on him, there are no grounds to consider that this circumstance is a mitigating circumstance. In accordance with the Guidelines on the application and determination of administrative fines for the purposes of Regulation No. 2016/679 Wp. 253 "The supervisory authority may become aware of a breach as a result of proceedings, complaints, articles in the press, anonymous tips or notification by the data controller. Pursuant to the regulation, the controller is obliged to notify the supervisory authority of a breach of personal data protection. The mere fulfillment of this obligation by the controller cannot be interpreted as a mitigating factor.'

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

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

Taking into account all the circumstances discussed above, the President of the Personal Data Protection Office decided that the imposition of an administrative fine on the Administrator and the Processing Entity is necessary and justified by the weight

and nature and scope of the infringements of the provisions of Regulation 2016/679 alleged against these entities. It should be stated that the application of any other remedy provided for in Art. 58 sec. 2 of Regulation 2016/679, in particular, limiting oneself to a reminder (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 above-mentioned entities in the future will not commit similar negligence as in this case.

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

In the opinion of the President of the UODO, the administrative fine imposed on the Administrator in the amount of PLN 33,012 (say: thirty-three thousand and twelve zlotys), which is the equivalent of EUR 7,000 (average exchange rate of the euro of January 30, 2023 - PLN 4.7160), meets the established circumstances of this case, 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 UODO, the penalty imposed on the Administrator is proportional to both the severity of the infringement (resulting in the violation of one of the basic principles on which the personal data protection system in Regulation 2016/679 is based - data confidentiality) and the size of the Administrator, which size - measured its turnover - should be considered inseparable from the considerations of the effectiveness of the penalty and its deterrent nature.

In the course of the proceedings, the Administrator presented the financial statements, i.a. for 2021, according to which its net revenues from business activity amounted to PLN (...) (say: (...)), which is equivalent to (...), - euro at the average euro exchange rate of January 30, 2023. Considering the above-presented results financial (...), it should be stated that the adjudicated administrative fine will not be excessively severe for him. It should be pointed out that the amount of the fine set by the President of the UODO - PLN 33,012 - is only (...) % of its turnover achieved in 2021. At the same time, in the opinion of the President of the UODO, the fine in this amount will be effective (it will achieve the goal of punishing the Administrator for a serious infringement of consequences) and deterrent for the future (will cause the Administrator, in order to avoid further

sanctions, to pay due attention to the processing of personal data through and with the help of the Processing Entity, while using the rights it has under the data processing entrustment agreement). A fine in a lower amount for this entity could be imperceptible in practice and could leave room for calculating whether for this organization the costs of administrative fines would not be lower than the expenditure on personal data protection.

In view of the above, the President of the UODO also indicates that the administrative fine imposed on the Administrator meets, in particular, the criterion of proportionality of the fine as defined in the case law of the CJEU (on the basis of competition law and in relation to the decision of the European Commission, but which, in the opinion of the President of the UODO, is more generally applicable): "[...] the principle of proportionality requires that acts issued by Union institutions do not exceed the limits of what is appropriate and necessary to achieve the legitimate objectives pursued by the provisions, and where there is a choice between several appropriate solutions, the least onerous should be applied , and the resulting disadvantages must not be disproportionate 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 there)" (see judgment of 26 October 2017 in case T-704/14 Marine Harvest ASA v. EC, para. 580).

The above general considerations regarding the proportionality, effectiveness and dissuasive nature of the administrative fine imposed on the Administrator also apply to the fine imposed on the Processor.

In the course of the proceedings, the Processing Entity presented a financial statement for 2021, according to which its net revenues from business activity amounted to PLN (...) (in words: (...)) in this financial year, which is equivalent to (...) euro at the average euro exchange rate of January 30, 2023. In the opinion of the President of the UODO, also the fine imposed against (...) will not be excessively severe. The penalty in the amount of PLN 472 (in words: four hundred and seventy-two zlotys), which is the equivalent of EUR 100, also according to the average euro exchange rate of January 30, 2023, will constitute only (...) % of the turnover achieved by (...) in 2021 and only 0.001 % of the maximum possible penalty. The President of the UODO notes that the penalty imposed against (…) takes into account the special life situation (…) M.H.

Summarizing the above, in the opinion of the President of the UODO, both administrative fines imposed in this case meet the conditions (functions of penalties) referred to in Art. 83 sec. 1 of Regulation 2016/679, due to the importance of the violations found in the context of the basic requirements and principles of Regulation 2016/679.

Considering the above, the President of the Office for Personal Data Protection decided as in the operative part of this

decision.

Print article

Metadata

Provider:

Inspection and Infringement Department

Produced information:

John Nowak

2023-02-08

Entered the information:

Wioletta Golanska

2023-03-31 14:42:47

Recently modified:

Edith Magziar

2023-04-13 10:00:51