THE CHAIRMAN OF PERSONAL DATA PROTECTION

Warsaw, on 17

of December

2020

DECISION

DKN.5130.1354.2020

Based on Article. 104 § 1 and art. 105 § 1 of the Act of 14 June 1960 Code of Administrative Procedure (Journal of Laws of 2020, item 256, as amended), art. 7 sec. 1, art. 60, art. 101 and art. 103 of the Personal Data Protection Act of May 10, 2018 (Journal of Laws of 2019, item 1781) and art. 57 sec. 1 lit. a, art. 58 sec. 2 lit. i, art. 83 sec. 1-3, art. 83 sec. 4 lit. a and art. 83 sec. 5 lit. and in connection with art. 5 sec. 1 lit. f, art. 24 sec. 1, art. 25 sec. 1, art. art. 28 sec. 1, art. 28 sec. 3 lit. h, 32 sec. 1 lit. b and lit. d, art. 32 sec. 2, art. 33 paragraph 1, art. 34 sec. 1 of the Regulation of the European Parliament and of the EU Council 2016/679 of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46 / EC (general regulation on data protection) (Journal of Laws UE L 119 of 04/05/2016, p. 1, as amended), after conducting administrative proceedings regarding the violation of the provisions on the protection of personal data by ID Finance Poland Sp. z o.o. in liquidation with its seat in Warsaw at ul. Hrubieszowska 6A, President of the Office for Personal Data Protection

1) finding a breach by ID Finance Poland Sp. z o.o. in liquidation with its seat in Warsaw at ul. Hrubieszowska 6A, the provisions of Art. 5 sec. 1 lit. f, art. 25 sec. 1, art. 32 sec. 1 lit. b, art. 32 sec. 1 lit. d and art. 32 sec. 2 of the Regulation of the European Parliament and of the EU Council 2016/679 of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46 / EC (general regulation on data protection) (Journal of Laws UE L 119 of 04/05/2016, p. 1, as amended), hereinafter referred to as "Regulation 2016/679", consisting in the failure to implement by ID Finance Poland Sp. z o.o. in liquidation based in Warsaw, both in the design phase of the processing process and during the processing itself, appropriate technical and organizational measures corresponding to the risk of violation of the ability to continuously ensure confidentiality, integrity, availability and resilience of the personal data processing system, as well as ensuring the ability to efficiently and quickly finding a breach of personal data protection and ensuring regular assessment of the effectiveness of these measures, which resulted in unauthorized access to the

processed personal data by third parties, imposes on ID Finance Poland Sp. z o.o. in liquidation, an administrative fine in the amount of PLN 1,069,850.00 (one million sixty-nine thousand eight hundred and fifty zlotys);

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

JUSTIFICATION

ID Finance Poland Sp. z o.o. in liquidation (hereinafter also referred to as: the "Company" or "administrator") [...] March 2020 and additionally [...] March 2020, reported to the President of the Personal Data Protection Office (hereinafter also referred to as the "President of the Personal Data Protection Office") a breach of data protection personal customers of the Company, which has been registered under the number DKN.5130.1354.2020.

The subject of the Company's activity is granting financial loans with the use of the moneyman.pl website. In the notification, the Company indicated that the breach took place on [...] March 2020 and was found on [...] March 2020 as a result of confirmation of information regarding the possibility of unauthorized access to data, received from a third party. The breach concerned problems related to the operation of the server on which the personal data of 218,657 people were processed. In the supplementary notification of [...] March 2020 and in the letter of [...] March 2020, the Company specified that the data included 140,699 of the Company's customers (the original number was related to, inter alia, the number of records in the database, and not the number of natural persons to whom these data relate) who, after [...] January 2018, have fully or partially completed the registration process on moneyman.pl, and the data included: name and surname, level of education, e-mail address , employment data, e-mail address of the person to whom the client wants to recommend the loan, earnings data, marital status data, telephone number (landline, mobile, previously used telephone number), PESEL number, nationality, tax identification number, password, place of birth, correspondence address, registered address, telephone number to the place of work and bank account number. The erroneous operation of the server was related to its restart by the processor - IDFT based in M. na B., which, under the contract of [...] March 2018, was entrusted with the processing of the above-mentioned data in order to provide hosting services. During the server restart, the settings of the software responsible for the server's security were reset, as a result of which the personal data on the server was publicly available. The database on this server was downloaded and deleted by an unidentified third party, which applied to the Company to pay remuneration in return for its return. The report indicated that, in order to remedy the breach and minimize the negative impact on data subjects, customers and potential customers had been informed that their login passwords had been reset. In order to minimize the risk of a

recurrence of the breach, e.g. firewall operation has been restored. At the same time, it was indicated that, in the opinion of the Company, there is a high risk of violating the rights or freedoms of natural persons to whom the data relates. In the supplementary notification, the Company announced that these persons were notified of the infringement on [...] March 2020 via e-mail and text messages (the content of the notification was attached to the supplementary notification).

In connection with the above, in a letter of [...] March 2020, the President of the Office for Personal Data Protection called ID Finance Poland Sp. z o.o. incl. down:

transfer of the content of the entrustment agreement with the processing entity involved in the processing that the breach relates to,

forwarding the content and date of any correspondence addressed to the Company from third parties with knowledge of the violation in question,

a detailed description of the personal data breach, description of its finding and presentation of the procedure for identifying and reporting data protection breaches, also in the context of the relationship with the processor,

indication of the time, channel and content of other correspondence addressed to data subjects in connection with the violation,

provide an assessment of the effectiveness of reaching the data subjects by e-mail about the breach and how the Company provides data subjects with effective provision of additional information about the breach as part of the hotline and e-mail address referred to in a notification addressed to these persons,

indication of whether and which the Company and the processor have adopted technical and organizational security measures in accordance with art. 24 and art. 25 of Regulation 2016/679,

clarification whether, when and how the controller and the processor regularly tested, measured and assessed the effectiveness of technical and organizational measures to ensure the security of personal data processed in ICT systems.

In response, by letter dated [...] March 2020, the Company provided extensive explanations regarding the event itself, including a copy of the correspondence conducted by the Company. The explanations were also accompanied by the full text of the entrustment agreement with attachments, concluded in Warsaw on [...] March 2018 between ID Finance Poland sp. Z o.o. based in Warsaw and the limited liability company "IDFT" with its seat in M. na B. (hereinafter also referred to as the "processor"). The submitted documents also included: The procedure for reporting a breach of personal data protection

introduced by order No. [...] of [...] May 2018 of the Management Board of the Company; Instruction on detailed rules for the security and management of the IT system […]; a number of internal procedures and documents used by the Company and the processor as an element of the security and personal data protection system. In addition, in her explanations, she described in detail the technical and organizational measures applied by both the Company and the processor.

According to the collected evidence, the chronology of events was as follows:

[...] February 2020 at [...] an employee of the processor restarted one of the servers used by the Company. The reboot was due to resource monitoring data that made the server believe that the server was not functioning optimally. After the reboot, the processor did not verify the correctness of the security configuration. The indicated date is appropriate for the time when the infringement occurred. In the preliminary and supplementary notification, the Company had no knowledge of the exact circumstances of the event. This information was provided by the Company in a letter of [...] March 2020 following an analysis by the processor on [...] March 2020.

[...] March 2020 at […] The company received the first signal of irregularities from an independent cybersecurity consultant - […]. In an e-mail in English, addressed both to the main e-mail address of the Company and the e-mail address of the Data Protection Officer, the researcher indicated that he had discovered a server with publicly available data of the Company's customers using the moneyman.pl website. The message in question constitutes attachment No. [...] to the letter of the Company of [...] March 2020.

[...] in March 2020, the data protection officer sent the above-mentioned message incl. to the company's finance director with a request for contact to the company's IT service - IDFT. The Company's Finance Director on the same day sent the above-mentioned a message to the director of IDFT with a comment suggesting that it may be a phishing scam. A copy of this message was received, among others, by the operational director of the Company. The activities of the Company's finance director, according to the administrator, were aimed at determining whether the received information is reliable and whether the reply poses a threat to the security of the Company's IT resources.

[...] in March 2020, the company's chief financial officer again approached the director of IDFT to determine whether the information provided had been verified. On the same day, IDFT restarted the server, but its configuration, taking into account the correct protection of the environment, was still incorrect.

[...] in March 2020, an undetermined third party downloaded and deleted the Company's database, leaving information with a

ransom demand.

[...] March 2020 at [...], the editor of the website trustanatrzeciastrona.pl contacted the Company by e-mail, pointing to the breach of personal data protection in question and the IP address of the server the breach concerns. On the same day, this information was provided, inter alia, to to the company's finance director.

[...] in March 2020, the company's finance director provided the above-mentioned message to the director of IDFT and the President of the Management Board of the Company.

[...] March 2020 at [...], the company's finance director received an e-mail (attached to the company's letter of [...] June 2020) from the director of IDFT with the information about the identification of the problem and noted that previously this entity had not dealt with such situation. IDFT employees determined that the breach of confidentiality of personal data processed on the Company's server occurred as a result of incorrect configuration of the firewall after the server restart, i.e. one of the ports remained open. The unauthorized data collection was confirmed, the scale of the breach was determined and remedial actions were taken, i.e. the correct configuration of the server was restored (port closure) and the passwords of the moneyman.pl users were reset. The company has also verified all the servers it uses to determine whether the data processed on these servers is safe. The verification showed that the Company is not threatened with such a risk, in particular with regard to unauthorized access. On the same day, the Company made an initial notification of a personal data breach to the President of the Data Protection Office.

[...] in March 2020, the Company re-verified all used servers. The conclusions of the verification were the same as those of [...] March 2020.

[...] in March 2020, the Company sent to the District Prosecutor's Office in Warsaw a notification of suspicion of a crime committed by an unknown perpetrator in connection with the event of [...] March 2020 (file reference number [...]).

In the context of the notification of the data subjects, the Company indicated that on [...] March 2020, it sent an SMS with the following text: "[o] retrieval of the MoneyMan password was successful. The new password is (…) ", thus indicating the content of the new password. On [...] March 2020, it sent out emails to users with identical content. Another e-mail containing the full content of the notification with the scope of information indicated in art. 34 sec. 2 of Regulation 2016/679 it sent [...] March 2020. By text message of [...] March 2020 addressed to data subjects, the Company informed that "(...) the last password change was carried out automatically and was due to security reasons . More on www.moneyman.pl (...) ". [...] in March 2020,

the Company posted information on the breach on the moneyman.pl home page and created dedicated tabs, in which it clarified the information provided in the text message of [...] March 2020 and information on the breach of personal data protection. Relevant screenshots are attached to the explanations.

Explaining the effectiveness of the breach notification reaching the data subjects, the company presented a detailed table which is a report listing the dates, channels, type of information and data concerning the receipt of the message. As indicated, the table shows that only 4% of entities could not receive information about the infringement provided by e-mail.

Referring to the effectiveness of providing information to data subjects using the telephone number and e-mail address indicated in the notifications, the Company explained that it had delegated additional employees to the Call Center department, informed employees on how to communicate with data subjects , prepared for them answers to basic questions asked by customers in connection with a breach of the protection of their personal data, withheld debt collection calls for a period of three days to facilitate customer contact and on [...] March 2020, suspended the sale of new loans to ensure effective servicing the affected customers.

As it results from the submitted explanations, in the notification of the infringement, the Company indicated that the database in question was not the main database of the Company's customers and potential customers. The company, in a letter of [...] March 2020, explained that the database contained data of the Company's customers who, after [...] January 2018, had fully or partially completed the registration process. In addition, it clarified the scope of the data categories. This database, as the Company points out, by mistake contained passwords of the MoneyMan.pl portal users, which were stored in plain text. In the main (production) database, passwords are stored in an implicit form.

In a letter of [...] May 2020, the President of the Personal Data Protection Office notified the Company of the initiation of administrative proceedings, the subject of which is the possibility of the Company, as a data controller, violating the obligations arising from the provisions of Regulation 2016/679 in the scope of obligations under Art. 5 sec. 1 lit. f, art. 24 sec. 1, art. 25 sec. 1, art. 28 sec. 1, art. 28 sec. 3 lit. h, art. 32 sec. 1, art. 32 sec. 2, art. 33 paragraph 1 and art. 34 sec. 1. In the notification, the President of the Personal Data Protection Office called on the Company to submit additional explanations, including down: explaining why the database concerned by the violation in question also mistakenly stored user passwords in plain text and what was the role of this database, since the passwords are stored in an encrypted form in the main production database of the Company;

indication of what verification procedures of the processing entity in terms of its compliance with the requirements of Regulation 2016/679 were carried out by the administrator before the conclusion of the data processing outsourcing agreement, as well as whether the Company exercised the right to control pursuant to art. 28 sec. 3 lit. h of Regulation 2016/679;

clarification of the circumstances related to the event that led to the breach of personal data protection.

In response to the notice of initiation of the procedure, by letter of [...] June 2020, the Company indicated that the main purpose of the existence of the database affected by the infringement was to develop and test a script examining the behavior of moneyman.pl users during and after logging into the customer panel (behavioral analysis). The implementation of such functionality was aimed at increasing data security and minimizing the risk of attacks, identity theft and financial fraud. The company indicated that due to the working nature of this functionality and the access of a limited number of people, the database was not encrypted at the right moment. At the same time, she emphasized that the ultimately applied security measures should be identical to those applied in the main base. As can be seen from these explanations, the personal data in the main (production) database is not covered by the personal data breach and despite the deletion of data on [...] March 2020, the administrator still had data that allowed him to notify data subjects about breach of personal data protection.

Referring to the verification of the processor in terms of its compliance with the requirements of Regulation 2016/679, the Company indicated that, guided by the need to ensure the correct and professional configuration of servers, it decided to entrust the performance of these tasks to a specialized entity such as IDFT, guided by, inter alia, his extensive experience in servicing entities from the financial sector, highly qualified employees and a comprehensive approach to customer service. In 2018, IDFT was audited in terms of the Company's services in accordance with the provisions of Regulation 2016/679. The results of this audit constitute an attachment to the letter of [...] June 2020. The company also indicated that IDFT had completed the tasks referred to in the above-mentioned document. Referring to the implementation of the right of control under Art. 28 sec. 3 lit. h of Regulation 2016/679, the Company indicated that the processor immediately provided the administrator with information on the event of [...] February 2020, as well as throughout the term of the entrustment agreement, telephone calls, teleconferences and mutual, direct visits were held regularly. In addition, the processor replied to the Company as part of a detailed questionnaire verifying compliance with contractual provisions. The completed questionnaire is attached to the letter of [...] June 2020.

In a letter of [...] June 2020, the Company specified that IDFT applied a firewall to the server affected by the breach, which could define network protection policies, traffic filtering, etc. This solution should be considered sufficient to protect the database against violation if its protection features were not unknowingly disabled due to a human error of running an inappropriate configuration script. One of them ([…]) contained a policy reset command for further manual configuration, while another ([…]) did not require any further manual steps. According to the information provided by the processor, the person who made the error had previously been trained in cybersecurity rules and had performed similar tasks regularly for a long time. Moreover, the above-mentioned the person was familiar with the server restart procedure, which in practice boils down to the use of a specific script, according to the supervisor's command. As part of activities aimed at minimizing the likelihood of a similar event in the future, scripts requiring manual configuration were abandoned and the server reset procedure was modified, which was attached to the letter of [...] June 2020.

As a result of the analysis of the information contained in the response to the letter informing about the initiation of the procedure, the President of the Office for Personal Data Protection, in a letter of [...] September 2020, asked the Company for clarification whether the audit of the processor carried out in connection with the entry into force of Regulation 2016 / 679 included procedures related to starting new servers, their configuration, resetting and final verification whether technical and organizational measures respond to threats to the data being processed. In a letter of [...] June 2020, the Company indicates that the person who made the error had been performing similar tasks on a regular basis for a long time, therefore the President of the Personal Data Protection Office called on the Company to indicate whether it saw the risks associated with the use of script launching procedures to configure the firewall.

The company, in response of [...] September 2020, indicated that the script application procedures were also checked during the semi-annual internal audits and assessed as adequate. The human error that caused the breach could not be predicted and avoided despite taking into account various risk factors. As the company points out, the normal scenario of the proceeding was automatic script execution, which ensured that all security measures were applied. The incident occurred in connection with a manual reboot of the server where the predefined settings were not triggered.

In these facts, the President of the Personal Data Protection Office considered the following.

Article 5 of Regulation 2016/679 lays down the rules for the processing of personal data that must be respected by all administrators, i.e. entities that independently or jointly with others determine the purposes and methods of personal data

processing. Pursuant to Art. 5 sec. 1 lit. f of Regulation 2016/679, personal data must be processed in a manner ensuring adequate security of personal data, including protection against unauthorized or unlawful processing and accidental loss, destruction or damage, by appropriate technical or organizational measures ("confidentiality and integrity") . Further provisions of the regulation make this principle more specific.

Pursuant to Art. 24 sec. 1 of Regulation 2016/679, taking into account the nature, scope, context and purposes of processing as well as the risk of violating the rights or freedoms of natural persons of varying probability and seriousness, the controller implements appropriate technical and organizational measures to ensure that the processing takes place in accordance with this Regulation and to be able to demonstrate it. These measures are reviewed and updated as necessary.

Pursuant to Art. 25 sec. 1 of Regulation 2016/679, both when determining the methods of processing and during the processing itself, the controller implements appropriate technical and organizational measures designed to effectively implement data protection principles (taking into account data protection at the design stage).

From the content of Art. 32 sec. 1 of Regulation 2016/679 shows that the administrator is obliged to apply technical and organizational measures corresponding to the risk of violating the rights and freedoms of natural persons with a different probability of occurrence and the severity of the threat. The provision specifies that when deciding on technical and organizational measures, the state of technical knowledge, implementation cost, nature, scope, context and purposes of processing as well as the risk of violating the rights or freedoms of natural persons with different probability and severity should be taken into account. It follows from the above-mentioned provision that the determination of appropriate technical and organizational measures is a two-stage process. In the first place, it is important to determine the level of risk related to the processing of personal data, taking into account the criteria set out in Art. 32 of Regulation 2016/679, and then it should be determined what technical and organizational measures will be appropriate to ensure the level of security corresponding to this risk. These arrangements, if applicable, in accordance with lit. b and d of this article, should include measures such as the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services as well as regular testing, measurement and evaluation of the effectiveness of technical and organizational measures to ensure the security of processing.

Pursuant to Art. 32 sec. 2 of Regulation 2016/679, the administrator, when assessing whether the level of security is appropriate, takes into account in particular the risk associated with the processing, in particular resulting from accidental or

unlawful destruction, loss, modification, unauthorized disclosure or unauthorized access to personal data sent, stored or otherwise processed.

Pursuant to the wording of Art. 33 paragraph 1 of Regulation 2016/679, in the event of a breach of personal data protection, the controller shall, without undue delay - if possible, no later than 72 hours after finding the breach - notify the supervisory authority, unless the breach is unlikely to result in a breach risk the rights or freedoms of natural persons.

The provisions of Regulation 2016/679 oblige both controllers and processors to adopt appropriate technical and organizational measures to ensure a level of security corresponding to the risk related to the processing of personal data. It also follows from the above-mentioned provisions and recital 87 of Regulation 2016/679 that the Regulation required the adoption of the above-mentioned measures to immediately find a breach of personal data protection. This is decisive for determining whether the obligations under Art. 33 paragraph 1 and art. 34 sec. 1 of Regulation 2016/679.

The obligation to notify the supervisory authority about the breach and the deadline for its submission is related to the moment when the controller "detects" the breach of personal data protection. The Article 29 Working Party, in the guidelines on reporting personal data breaches pursuant to Regulation 2016/679, adopted on October 3, 2017, last amended and adopted on February 6, 2018 (hereinafter: breach reporting guidelines), indicates that the controller finds a breach as soon as it has obtained reasonable certainty that a security incident leading to the disclosure of personal data occurred. However, this issue should be considered in relation to the controller's obligation to maintain the ability to quickly and effectively identify any breaches to ensure that appropriate action can be taken. In some cases, it may take time to determine whether personal information has been disclosed. In this context, however, emphasis should be placed on prompt investigation of the incident in question to determine whether a personal data breach has actually occurred and, if so, take remedial action and, if necessary, report the breach.

It should therefore be assumed, as indicated by the Article 29 Working Party in the Breach Notification Guidelines, that after receiving the first information about a potential personal data breach, from an individual, from another source or after detecting a security incident itself, the controller may conduct a short-term investigation to determine whether a given infringement has actually taken place. While, until the conclusion of these proceedings, the controller cannot be considered to have identified a breach, it should be expected that the preliminary proceedings should begin as soon as possible and lead to a determination as soon as possible with a reasonable degree of certainty whether in a given case a breach actually occurred. violations, then

a more detailed analysis of the incident can be performed. However, in case of any doubts, in particular taking into account the nature and scope of the processed data and the risk related to e.g. accidental disclosure, the controller should notify the supervisory authority of the breach, even if such caution could turn out to be excessive. Recital 85 of Regulation 2016/679 explicitly states that one of the reasons for reporting a breach is the limitation of the related harm to individuals, as evidenced by the provisions cited above, which specify the principle of confidentiality in Art. 5 sec. 1 lit. f of the Regulation 2016/679, obliging the processing of personal data in a manner ensuring their appropriate security. As indicated in the Breach Reporting Guidelines, when assessing the risk that may arise from a breach, the controller should take into account the impact of the breach on the rights and freedoms of individuals and the likelihood of their occurrence.

In the e-mail of [...] March 2020, received by the Company, a fragment of information was presented containing the personal data of the user of the moneyman.pl website, which, in the sender's opinion, is located in the Company's IT infrastructure. This fragment was a partial reflection of the structure of the data categories with their values. Among them was, among others PESEL number, e □ mail address and user ID. While in this letter the sender did not indicate the IP address of the server, the incorrect configuration of which led to a breach of personal data protection, in the opinion of the President of the Personal Data Protection Office, the controller did not undertake a detailed analysis and take into account the information contained in this message suggesting that the entire customer database may be made available. Companies. Adopting at least such a perspective should make the Company aware of the scale of the potential breach and the negative consequences for its customers that may or have already occurred. Having the above-mentioned information should be an incentive to try to obtain additional information from the sender with due care and to undertake verification activities also on their own. For example, whether the indicated information regarding this one exemplary person actually relates to one of the Company's clients and should not be a reason for taking more intensified actions in cooperation with the processor. Unauthorized disclosure of the scope of personal data (indicated in the description of the facts) may undoubtedly result in a high risk of violating the rights or freedoms of natural persons to whom such data relates. In connection with the above, ensuring adequate security of such data should be the subject of special care of the administrator, and each signal about possible irregularities should be thoroughly analyzed.

In the opinion of the President of the Personal Data Protection Office, the administrator, after receiving the message of [...] March 2020, did not follow the above-mentioned rules. This is indicated, inter alia, by its redirection by the company's finance

director to the director of IDFT with a short comment questioning the sender's intentions and pointing to the so-called "Smart phishing". While the Company rightly sent the message to the processing entity and based its belief that it was necessary to notify the supervisory body only after confirming its credibility, it does not appear from the evidence that the controller would take other actions to quickly and effectively identify the infringement, apart from directing [...] March 2020 a short question to the director of IDFT. If there are circumstances indicating that this information cannot be verified quickly and effectively, taking into account the risk to the rights and freedoms of natural persons, the Company should report the breach to the supervisory authority without undue delay.

The delay, which, according to the President of the Personal Data Protection Office, was committed by the administrator between [...] March 2020 and [...] March 2020, when he received another signal about the infringement, led to its escalation. The server's vulnerability, detected on [...] March 2020 by an unknown person, resulted in the collection of personal data of 140 699 of the Company's customers, their deletion and leaving a ransom-demand message. Only after the [...] March 2020 message of [...] March 2020 was sent to the director of IDFT, which indicated the legal obligations incumbent on the Company regarding the date of notification of the supervisory authority, both the Company and the processor undertook intensified verification activities and countermeasures. According to the explanations of the Company, it was not until [...] March 2020 that the IT team of the processor found the causes of the problem after it checked the e-mail of [...] March 2020. This leads to the obvious conclusion that it took about 10 days. In addition, as the Company indicated, it was only from [...] March 2020 that the Company's data protection officer began collecting information about the breach.

Although the Company repeatedly in its explanations in the letters of [...] March 2020 and [...] June 2020, the processor referred to the fact that the processor immediately provided information to the Company about individual events, including on [...] February 2020 r., the collected material shows that this information was provided in an intensified manner and on the initiative of the Company only after [...] March 2020.

According to the letter of [...] June 2020, the Company has not found any similar irregularities in the past that led to a data protection breach. At the same time, she indicated that the server restart, as a standard procedure, was repeatedly performed. Also, the director of IDFT in an e-mail of [...] March 2020 indicated that so far such serious events had not taken place. In the opinion of the President of UODO, the lack of events of a similar nature cannot, however, lull the administrator's vigilance and justify the lack of appropriate actions on his part between [...] March 2020 and [...] March 2020.

The lack of a quick response from the processor does not remove the responsibility of the controller for finding a personal data breach, as the ability to detect breaches, remedy them and report them in a timely manner should be seen as a key element of technical and organizational measures, including any data security policy. . In the opinion of the President of the Personal Data Protection Office, the company, despite the immediate transmission of a signal of irregularities to the processing entity, did not take its actions in an appropriate manner. The circumstances of the case clearly indicate that the controller briefly analyzed the message of [...] March 2020, did not take it seriously and did not oblige the processor to do the same. Undertaking a proper analysis and intensified contact with the processing entity already on [...] March 2020, in which the Company learned about the first irregularities, in the opinion of the President of the Personal Data Protection Office, would allow to find a breach of data protection much faster (as was done after the message received from the editor of one of the websites) and potentially minimize the risk to the rights and freedoms of the Company's customers, including avoiding the event that took place on [...] March 2020.

In the document presented by the Company, entitled "Procedure for reporting personal data breaches", point [...] indicates that its purpose is to create a mechanism ensuring timely notification of a personal data breach. Point […], which is the personal data breach notification scheme, indicates that the role of the Data Protection Officer is to analyze the incident and identify the breach and assess the risk for individuals. In point […] there is an incident analysis procedure, in which the data protection officer, as a coordinator, verifies and analyzes the incident, involving all units related to a potential data protection breach. In point [...], there are examples of catalogs of events subject to the obligations under Art. 33 and 34 of Regulation 2016/679. In addition to these elements, the document contains many general statements that can be derived directly from the provisions of Regulation 2016/679.

Thus, with their actions, despite the awareness of the events that may result in a breach of personal data protection (the procedure refers to, for example, an incorrect operation of an IT system or a human error), the message from [...] March 2020 was treated by the Company without due diligence. seriousness and contrary to the above-mentioned the procedure and the provisions of Regulation 2016/679, the purpose of which is to create a mechanism ensuring timely notification of a breach of personal data protection. This is evidenced by the question of the data protection officer to one of the employees and the company's finance director to contact the IT team of the processor and the suggestion of the company's finance director in a message to the director of IDFT, indicating the so-called "Smart phishing". The contract for entrusting the processing of

personal data of [...] March 2018 in the context of data protection breaches, only in § [...] contains specific obligations of IDFT in the event of a breach of personal data protection, however, their wording and interpretation, in the opinion of the President of the Personal Data Protection Office, is already related to the established breach.

Both the explanations of the Company and the documents presented by it do not present the procedure of finding a violation. While such a procedure is not explicitly required by any of the provisions of Regulation 2016/679, as indicated in the infringement guidelines and as it results from the provisions of Regulation 2016/679, the controller is obliged to efficiently and quickly identify a data protection breach, and such the procedure can significantly facilitate this.

From the response to the request to indicate how the controller regularly tested, measured and assessed the effectiveness of technical and organizational measures to ensure the security of personal data in the IT systems affected by the breach, it does not appear that the aforementioned procedure for reporting breaches was approvals verified in terms of its effectiveness.

In view of the above, the Company, when assessing the first signal of irregularities, did not take into account - in the opinion of the President of the Personal Data Protection Office - the risk related to the processing of personal data resulting from the accidental disclosure of personal data, which constitutes a violation of Art. 32 sec. 2 of Regulation 2016/679. The evidence collected in the course of these proceedings is also the basis for stating that the Company has failed to fulfill its obligation to ensure the processing of personal data in a manner ensuring their appropriate security from the moment it received the first signal of irregularities, which constitutes a breach of the confidentiality principle expressed in Art. 5 sec. 1 lit. f of the Regulation 2016/679. It also failed to implement appropriate technical and organizational measures for the effective implementation of the above-mentioned data protection rules, which constitute a violation of Art. 25 sec. 1 of Regulation 2016/679 and the effective and quick finding of the infringement, which constitutes an infringement of Art. 24 sec. 1 of Regulation 2016/679. In the opinion of the President of the Personal Data Protection Office, the Company did not regularly assess the effectiveness of these measures, which constitutes a breach of Art. 32 sec. 1 lit. d of Regulation 2016/679. Thus, between [...] March and [...] March 2020, its actions contributed to the failure to ensure the ability to continuously ensure confidentiality, integrity, availability and resilience of processing systems and services, which constitutes a violation of Art. 32 sec. 1 lit. b of the Regulation 2016/679.

In connection with the explanations relating to the regular testing, measurement and evaluation by the administrator of the effectiveness of technical and organizational measures to ensure the security of personal data in the IT systems affected by

the breach, it should be noted that these explanations do not indicate that the Company acquires customer data service moneyman.pl after [...] January 2018 showed interest in the way in which user passwords are stored in an additional database, which is the subject of a breach. In the opinion of the President of the Personal Data Protection Office, the statement of the Company that the passwords of users were mistakenly stored in open text and due to the working nature of this functionality and the access of a limited number of people, the database was not "encrypted" at the right moment is incomprehensible in the opinion of the President of the Personal Data Protection Office. As indicated by the Company in the explanations of [...] March 2020 and [...] June 2020, the purpose of the existence of the database affected by the infringement was to develop and test a script examining the behavior of moneyman.pl users during and after logging into the customer panel (behavioral analysis). The President of the Personal Data Protection Office points out that the storage of passwords in IT systems in a classified form (e.g. by using a hash function, also known as hashing) is one of the most common measures to ensure the confidentiality of a password and limit its knowledge only to the person who uses it. In this way, the negative consequences related to the potential risk of using such a password by a person who unauthorized, in conjunction with other information, reads its content are limited. A person who knows the user's credentials for a particular service can freely access their account. It should be noted that in the case at hand such a situation could lead to, for example, identity fraud, damage to reputation or financial loss. In addition, the user could use the same username (e.g. e-mail address) and password on other websites. Taking into account the categories of data processed by the Company, ensuring the security of this data, it should take such circumstances into account in a special way, because the group of people who may be potentially interested in the obtained certificates for the purpose of unlawful use may be undefined and have negative consequences. for the rights and freedoms of data subjects. Although the use of the secret password storage mechanism does not completely eliminate the likelihood that an unauthorized person will reverse the process and obtain the password, its proper implementation causes the so-called attacks. cracking passwords turn out to be time-consuming and even impractical. The purpose of such a process is, inter alia, obtaining adequate time for taking remedial actions by both the controller and the data subject, especially in cases where the controller does not find a breach of personal data protection close to its actual occurrence, which took place in the case being the subject of this decision. Therefore, when deciding on such a solution, the administrator should assess whether the solutions used will actually fulfill their role. While the Company rightly indicates in its letter of [...] September 2020 that the relationship with the processor does not imply an obligation to constantly monitor the solutions applied, in the opinion of the President of the

Personal Data Protection Office, it is important that the controller, as part of the performance of obligations under Regulation 2016/679, performs regular verifying that the technical and organizational solutions used have not identified any weaknesses that may affect the risk of violating the rights or freedoms of data subjects, and the fact that data is processed by a processor does not remove this responsibility from the controller. In the opinion of the President of the Personal Data Protection Office, this constitutes a violation by the Company of Art. 25 sec. 1 of Regulation 2016/679. It should be indicated that the addressee of Art. 25 sec. 1 of Regulation 2016/679, it is only the controller who is obliged to both define the processing methods and during the processing itself, implement appropriate technical and organizational measures, such as pseudonymisation, designed to effectively implement data protection principles. It should be emphasized that the concept resulting from this provision is based on the proactive and preventive approach of the controller consisting in ensuring the security of personal data at every stage. The adoption of such solutions by the EU legislator aims to strengthen the confidentiality principle expressed in Art. 5 sec. 1 lit. f of the Regulation 2016/679, in order to ensure the necessary security of the processed data, corresponding to the risks related to their processing. The lack of actions of the administrator in this regard also constitutes a violation of Art. 24 sec. 1, art. 32 sec. 1 lit. d and art. 32 sec. 2 of Regulation 2016/679 by not taking into account the risk related to the processing of users' passwords in open form, which in the event of failure to apply other technical and organizational measures to ensure secure processing, in accordance with the above-mentioned the provisions of Regulation 2016/679, provides for the exposure of data subjects to increasing the risk of violating the rights or freedoms of natural persons in the event of a breach of the confidentiality of the data processed.

In the course of the administrative procedure, despite the irregularities identified by the President of the Personal Data Protection Office which had an impact on the breach of data protection and its late finding, the President of the Personal Data Protection Office did not find a breach of Art. 33 paragraph 1 of Regulation 2016/679. The content of this provision obliges the controller to notify the supervisory body about the breach of personal data protection after two cumulative conditions are met - the breach is identified, which results in the risk of violating the rights or freedoms of natural persons. / 679, the provisions of Regulation 2016/679 should be interpreted, inter alia, through the prism of the administrator's ability to efficiently and quickly identify a breach of personal data protection using technical and organizational measures. Thus, on this account, a breach of the obligations imposed on the Company was found. As a result, the President of the Personal Data Protection Office (UODO) discontinued the administrative proceedings regarding the violation of Art. 33 paragraph 1 of Regulation 2016/679, which

therefore does not constitute the basis for the administration of a fine.

Pursuant to the wording of Art. 34 sec. 1 of Regulation 2016/679, if the breach of personal data protection may result in a high risk of violation of the rights or freedoms of natural persons, the controller shall notify the data subject of such a breach without undue delay.

Again, reference should be made to the Breach Notification Guidelines, which indicate that when notifying individuals about a data breach, the controller should be transparent about this and provide information in an efficient and timely manner. When analyzing the meaning of the term "without undue delay" under this provision, it should be assumed that the beginning of the time limit for notifying data subjects is the moment of finding the infringement. The company, as already indicated in this decision, was late in finding the infringement on […] March 2020, which does not remove its liability for the risk of infringement of the rights or freedoms of data subjects resulting from the delay in finding the infringement. However, immediately after the belated finding, the Company, with the help of the processor, started the process of resetting users' passwords and took all necessary steps to inform data subjects efficiently and in a timely manner, including using the available information channels and exhaustively demonstrated the effectiveness of the notification delivery. As a result, the President of the Personal Data Protection Office (UODO) discontinued the administrative proceedings regarding the violation of Art. 34 sec. 1 of Regulation 2016/679, which therefore does not constitute the basis for the administration of a fine.

Pursuant to the wording of Art. 28 sec. 1 of Regulation 2016/679, if the processing is to be carried out on behalf of the controller, he or she uses only the services of such processors that provide sufficient guarantees for the implementation of appropriate technical and organizational measures to ensure that the processing meets the requirements of Regulation 2016/679 and protects the rights of persons whose data concern. Moreover, in accordance with par. 3 lit. h of this article, the controller has the power to obtain from the processor all information necessary to demonstrate compliance with the obligations set out in art. 28 of Regulation 2016/679 and has the power to conduct audits, including inspections.

With the above-mentioned the conducted analysis shows that the Company should be accused of failing to fulfill the obligations arising from the provisions of Art. 5 sec. 1 lit. f, art. 24 sec. 1, art. 25 sec. 1, art. 32 sec. 1 lit. b and d and art. 32 sec. 2 of Regulation 2016/679. However, it is impossible to agree with the position of the Company that its possible liability as an administrator should be considered only in the context of Art. 28 sec. 1 of Regulation 2016/679 and the answer to the question whether the guarantees provided to the controller by the processor were sufficient to justify the use of its services.

Obviously, this assessment, as the Company also points out, cannot be made only from the perspective of the incident itself, but from the perspective of the possibility of its occurrence and the possibility of a reasonable statement before the incident occurs that the guarantees are insufficient and the services of other IT experts should be used. The Company also rightly points out that Art. 28 sec. 1 of Regulation 2016/679 requires the use of processors that provide adequate guarantees of compliance, and not continuous monitoring of the solutions applied by this entity.

In the letters of [...] March, [...] June and [...] September 2020, the Company submitted extensive explanations and numerous documents that regulate the relationship between ID Finance Sp. z o.o. in liquidation and IDFT. From the point of view of the provisions of Art. 28 sec. 1 and art. 28 sec. 3 lit. h of Regulation 2016/679, the President of the Personal Data Protection Office, in the collected evidence, did not find any circumstances that would allow to conclude that IDFT did not provide sufficient guarantees for the security of personal data and did not provide the administrator with all information necessary to demonstrate compliance with the obligations set out in art. 28 of the Regulation 2016/679 or prevented the Company from carrying out audits, including inspections. As a result, the President of the Personal Data Protection Office (UODO) discontinued the administrative proceedings regarding the violation of Art. 28 sec. 1 and art. 28 sec. 3 lit. h of the Regulation 2016/679, which therefore does not constitute the basis for the administration of a fine.

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

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

The nature and gravity of the infringement taking into account the number of people injured (Article 83 (2) (a) of Regulation 2016/679) - when imposing the penalty, it was important that the number of people affected by the infringement was 140 699 (specified in the supplementary notification from [...] March 2020). In addition, the President of the Personal Data Protection

Office took into account that the event of [...] March 2020 caused a high risk of negative consequences in the future for data subjects, resulting from a wide range of data covered by the infringement, a large number of data subjects and undoubted bad will of the person that has obtained unauthorized access to data, as well as the large-scale and professional nature of data processing by the Company. It should be emphasized that in relation to the above-mentioned of persons, there is still a high risk of unlawful use of their personal data, because the purpose for which the person or unauthorized persons took action resulting in the infringement of personal data protection is unknown. The data subjects may therefore suffer material damage, and the very breach of data confidentiality is also non-pecuniary damage (harm). The data subject may, at the very least, feel the fear of losing control of their personal data, of identity theft or identity fraud, or of financial loss.

Duration of the infringement (Article 83 (2) (a) of Regulation 2016/679) - the collected evidence allowed the President of the Personal Data Protection Office to state that the Company did not take appropriate actions to quickly and efficiently identify the infringement, which resulted in confirmation of the irregularities reported [...] March 2020 only after about 10 days. The delay by the Company has a significant impact on the amount of the penalty imposed by the President of the Personal Data Protection Office, because, as indicated in the justification, appropriate, reliable analysis and intensification of contact with the processor already on [...] March 2020, in which the Company learned about the first irregularities, according to the President of the Personal Data Protection Office, would allow to find a breach of data protection much faster (as was done after the message received from the editor of one of the websites) and potentially minimize the risk to the rights and freedoms of the Company's clients, including avoiding an event that occurred [...] March 2020

At the same time, it should be pointed out that the duration of the breach consisting in the failure to implement appropriate organizational and technical measures to ensure the security of the personal data being processed, i.e. procedures allowing for quick identification of the breach and guaranteeing regular assessment of the implemented security measures, should be counted from the moment the Company introduces the breach reporting procedure protection of personal data, i.e. from [...] May 2018. However, in the case of a breach involving failure to take into account the risk related to the processing of users' passwords in an open form, which in the event of failure to apply other technical and organizational measures to ensure secure processing, in accordance with Regulation 2016/679, provides for the exposure of data subjects to an increased risk of violation of the rights or freedoms of natural persons in the event of a breach of the confidentiality of the processed data, this period should be counted from [...] January 20 18, i.e. from the date on which the Company's customers have fully or partially

completed the registration process at maneyman.pl.

3. Unintentional nature of the infringement (Article 83 (2) (b) of Regulation 2016/679).

Taking into account the findings in the case being the subject of this decision, it should be stated that the Company committed gross negligence resulting in a breach of the confidentiality of data, which took place on [...] March 2020. Thus, this is a significant circumstance aggravating the amount of the administrative penalty.

4. Categories of personal data affected by a breach of personal data protection (Article 83 (2) (g) of Regulation 2016/679) - data of the Company's customers who, after [...] January 2018, have fully or partially completed the registration process . The scope of the data that is the subject of the breach (specified in the letter of [...] March 2020) is as follows: name and surname, level of education, e-mail address, employment data, e-mail address of the person whom the client wants to recommend the loan, personal data regarding earnings, data on marital status, telephone number (landline, mobile, previously used telephone number), PESEL number, nationality, NIP number, password (mistakenly, as indicated by the Company, stored in open text), place of birth, correspondence address, registered address , telephone number to the place of work and bank account number. These data do not belong to the special categories of personal data referred to in art. 9 of the Regulation 2016/679, due to their sensitive nature, subject to special protection. However, their very wide scope is a significant circumstance aggravating the amount of the administrative penalty.

5. The high degree of responsibility of the controller (Article 83 (2) (d) of Regulation 2016/679) - Considering that the controller is legally obliged to identify the breach in an efficient and timely manner and, in certain situations, to immediately report the breach of personal data protection to the supervisory authority , the findings made by the President of the Personal Data Protection Office allow the conclusion that the Company has not implemented appropriate technical and organizational measures to ensure the security of processing of personal data of customers in situations where it receives the first signal about irregularities in the processing of personal data of which it is the administrator.

The other, specified in Art. 83 sec. 2 of Regulation 2016/679, the circumstances:

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

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

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

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

There is no evidence that the Company obtained financial benefits and would avoid losses in connection with the breach.

Good cooperation on the part of the Company, which sent explanations within the set deadline and provided comprehensive answers.

Taking into account all the above-mentioned circumstances, the President of the Personal Data Protection Office decided that the imposition of an administrative fine on the Company is necessary and justified by the weight, nature and scope of the infringements made by the Company.

Referring to the amount of the administrative fine imposed on the Company, the President of the Personal Data Protection Office concluded that in the established circumstances of the case - i.e. in the event of a breach of several provisions of Regulation 2016/679 (the principle of data confidentiality, expressed in Article 5 (1) (a)), f, and reflected in the obligations set out in Article 24 (1), Article 25 (1), Article 32 (1) (b) and (d) and Article 32 (2), both Article 83 sec. 4 lit. a regulation 2016/679, providing, inter alia, for breach of the administrator's obligations referred to in art. 25 and art. 32 of Regulation 2016/679, the possibility of imposing an administrative fine of up to EUR 10,000,000 (in the case of a company - up to 2% of its total annual worldwide turnover from the previous financial year), as well as Art. 83 sec. 5 lit. a regulation 2016/679, according to which violations of, inter alia, the basic principles of processing, including in art. 5 of this regulation are subject to an administrative fine of up to EUR 20,000,000 (in the case of an enterprise - up to 4% of its total annual worldwide turnover from the previous financial year, whichever is higher).

In view of the above, pursuant to Art. 83 sec. 3 of Regulation 2016/679, the President of the Personal Data Protection Office determined the total amount of the administrative fine in an amount not exceeding the amount of the fine for the most serious breach. In the presented facts, the most serious breach by the Company of the confidentiality principle specified in Art. 5 sec. 1 lit. f of the Regulation 2016/679. This is due to the serious nature of the breach and the group of people affected by it (140,699

- one hundred and forty thousand six hundred and ninety-nine customers of the Company, ie persons whose data is administered by the Company).

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

Bearing in mind the above, the President of the Personal Data Protection Office, pursuant to art. 83 sec. 4 lit. a and art. 83 sec. 5 lit. and in connection with art. 83 sec. 3 of the Regulation 2016/679 and in connection with Art. 103 of the Act of May 10, 2018 on the Protection of Personal Data, for the violations described in the operative part of this decision, imposed on the Company - using the average EUR exchange rate of January 28, 2020 (EUR 1 = PLN 4.2794) - an administrative fine in the amount of PLN 1,069,850.00 (equivalent to EUR 250,000).

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

In the opinion of the President of the Personal Data Protection Office, the penalty imposed on the Company will be effective, because it will lead to a state in which the Company will apply such technical and organizational measures that will ensure the level of security for the data processed, corresponding to the risk of violating the rights and freedoms of data subjects and the importance of the accompanying threats. the processing of this personal data. The effectiveness of the penalty is therefore equivalent to the guarantee that the Company, from the moment of the conclusion of these proceedings, will follow the requirements of the provisions on the protection of personal data with the utmost care.

The applied financial penalty is also proportional to the infringement found, in particular its seriousness, the number of individuals affected by it and the risk they incur in connection with the infringement. In the opinion of the President of the Personal Data Protection Office, the fine imposed on the Company is appropriate taking into account the net revenues of the Company determined for 2019 at the level of PLN 17.7 million and for 2018 at the level of PLN 33.4 million and will not constitute an excessive burden for it. As can be seen from the above amounts, the Company shows ever lower revenues. It

should also be emphasized that the Company took steps to terminate its operations by adopting on [...] June 2020 a unanimous resolution of the Extraordinary General Meeting of ID Finance Sp. z o.o. with its registered office in Warsaw, on the dissolution of the Company and appointment of its liquidator. At the same time, however, it should be noted that, according to the information corresponding to the current excerpt from the register of entrepreneurs (KRS number: "[...]"), as of December 14, 2020, the only shareholder of the Company is IDFI, SL, legal person, company capital registered under Spanish law with its seat in B.

The amount of the fine was therefore set at such a level that, on the one hand, it would constitute an adequate response of the supervisory authority to the degree of breach of the administrator's obligations, on the other hand, it did not result in a situation in which the necessity to pay a financial penalty would entail negative consequences, such as a significant deterioration of the financial situation. Companies. In the opinion of the President of the Personal Data Protection Office, the Company should and is able to bear the consequences of its negligence in the field of data protection, hence the imposition of a penalty of PLN 1,069,850.00 is fully justified.

In these specific circumstances, the administrative fine will fulfill a repressive function, as it will be a response to the Company's breach of the provisions of Regulation 2016/679, but also preventive, i.e. it will prevent future violations of the provisions on the protection of personal data by both the Company and other data administrators.

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

2020-12-29