THE CHAIRMAN OF PERSONAL DATA PROTECTION

Warsaw, 22

April

2021

DECISION

DKN.5130.3114.2020

Based on Article. 104 § 1 and 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 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) in connection with Art. 24 sec. 1, art. 31, art. 32 sec. 1 and 2, art. 34 sec. 1, as well as art. 83 sec. 1 and 2 and article. 83 sec. 4 lit. a) Regulation of the European Parliament and the EU Council 2016/679 of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46 / EC (general regulation on data protection) (Journal of Laws UE L 119 of May 4, 2016, p. 1, Journal of Laws UE L 127 of May 23, 2018, p. 2 and Journal of Laws UE L 74 of March 4, 2021, p. 35) , after conducting the administrative procedure initiated ex officio regarding the processing of personal data by Cyfrowy Polsat Spółka Akcyjna with its registered office in Warsaw at ul. Łubinowa 4a, President of the Office for Personal Data Protection,

1) finding a breach by Cyfrowy Polsat Spółka Akcyjna with its registered office in Warsaw at ul. Łubinowa 4a Art. 24 sec. 1 and art. 32 sec. 1 and 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 the protection of data) (Journal of Laws UE L 119 of May 4, 2016, p. 1, Journal of Laws UE L 127 of May 23, 2018, p. 2 and Journal of Laws UE L 74 of March 4, 2021, p. 35)), hereinafter: "Regulation 2016/679", consisting in failure to implement appropriate technical and organizational measures ensuring the security of personal data processed in cooperation with the courier service provider by quickly identifying violations of personal data protection, is imposed on Cyfrowy Polsat Spółka Akcyjna with its registered office in Warsaw at ul. Łubinowa 4a, for violation of Art. 32 sec. 1 and 2 of Regulation 2016/679, an administrative fine in the amount of PLN 1,136,975 (in words: one million one hundred and thirty-six thousand nine hundred and seventy-five zlotys),

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

JUSTIFICATION

Cyfrowy Polsat Spółka Akcyjna with its seat in Warsaw at ul. Łubinowa 4a (hereinafter also referred to as: the "Company") regularly submitted reports to the President of the Personal Data Protection Office (hereinafter also referred to as: "the President of the Personal Data Protection Office") of violations of the protection of personal data of the Company's clients, which included, inter alia, on the loss of documents by couriers containing personal data of customers or on the issuance by couriers of documents containing personal data to the wrong person in the form of: name and surname, address of residence or stay, PESEL number, e-mail address, series and number of an ID card or other identity document, telephone number and data relating to the contracts between the parties. This proceeding covered [...] notifications submitted by the Company in the period from [..] June to [...] July 2020 (the list of these notifications is provided in the case file). A detailed analysis of the notifications made by the Company in the above-mentioned period, as well as in the period from [...] August to [...] September 2020, is the basis for the resolution made by this decision and justifies the finding by the Company of the breach described in the decision conclusion.

Accepting the Company's explanations regarding infringements of this type, reported to the Personal Data Protection Office in the period from December 2019 to May 26, 2020, the President of the Personal Data Protection Office in letters of [...] April and [...] May 2020 also indicated that the violations in question would be subject to further and continuous benchmarking with possible future breaches to determine the effectiveness of the measures taken to minimize the negative effects of the breach and the risk of its recurrence. In addition, it was emphasized that in order to control compliance with the law by data controllers, in particular to check whether they fulfill their obligations in the processing of personal data, the President of the Personal Data Protection Office has the power to carry out inspections also in relation to those entities with whom he corresponded regarding breaches of protection. data. The above-mentioned the letters (as well as previous letters concerning the breaches reported by the Company) indicated that a lot of information on the rules of personal data processing, the content of the legal acts in force in the aforementioned matter, as well as guidance on their application in practice, can be found on the website of the Office of Personal Data Protection Personal Data (www.uodo.gov.pl), on which are published, inter alia, The controllers' obligations related to personal data breaches and the Guidelines for reporting personal data breaches in accordance with Regulation 2016/679 of the Art. 29 (hereinafter also referred to as the "Guidelines"). This means that the

Company had the opportunity to become acquainted with these documents.

By making subsequent analyzes of reports of violations of personal data protection related to the Company's cooperation with an entity providing courier services, in which the Company indicated that there was a high risk of violating the rights or freedoms of natural persons, attention was drawn to the increase in the number of notifications of such violations in June 2020, in compared with the period from [...] January to [...] May 2020. In addition, attention was drawn to the significant lapse of time from the date of the event causing the breach of personal data protection to the date of its discovery by the Company and, consequently, notification of data subjects and the President of the Personal Data Protection Office on the infringement, because the reports submitted by the Company in the analyzed period of June 2020 concerned, inter alia, events causing a breach of personal data protection from February and January 2020, and even events from 2019. Analyzing [...] notifications of a personal data breach that were received by the President of the Personal Data Protection Office in June 2020, no cases were found by the Company of a breach within the deadline up to 7 days from the date of the incident that caused the violation. It was found that […] infringements were found more than 7 to 14 days after the event giving rise to the infringement, […] infringements were found more than 14 to 30 days, […] infringements were found in more than 30 to 60 days. […] The breaches were identified by the Company within more than 60 days from the date of the breach event, which represents 60% of the total number of personal data breaches reported in the analyzed period.

In connection with the above, on [...] July 2020, the President of the Personal Data Protection Office, pursuant to Art. 58 sec. 1 lit. a) and e) of Regulation 2016/679, requested the Company to provide information and indicate:

1. actions aimed at minimizing the risk of a recurrence of the infringement undertaken by the Company in the 2nd quarter of 2020 in cases of infringements related to the delivery of parcels by courier companies; 2.if, and how, what technical and organizational protection measures have been implemented by the Company to immediately identify a breach of personal data protection and notify the supervisory authority and the data subject without undue delay; 3. has the Company analyzed the impact of timely identification of personal data breaches on the rights and freedoms of data subjects, how, what were the results of the above-mentioned analysis.

At the same time, in a letter of [...] July 2020, the Company was presented with the general results of the analysis of personal data breach notifications made by it in June 2020. The President of the Personal Data Protection Office emphasized that together with the explanations, evidence should be submitted to confirm them. The company was also informed that the failure

to submit explanations and evidence to confirm them in the above-mentioned scope may result in the imposition of an administrative fine in accordance with Art. 83 sec. 5 lit. e) of Regulation 2016/679.

In a letter of [...] July 2020, the Company provided explanations, which show, inter alia, that it was assured by the carrier about the ongoing monitoring of the scale of violations and taking actions aimed at eliminating or at least minimizing such violations. The company indicated that in the second quarter of this year, it was primarily important for the Company to ensure the safety and health of customers and couriers during the pandemic, which was reflected in the instructions developed between the parties during the delivery of parcels, while maintaining the highest possible standards of data security.

The company also informed that it is currently conducting talks with the carrier in this regard, presenting as evidence the correspondence constituting Annex 3 to the above-mentioned Company letters. As evidence, an e-mail of [...] June 2020 was attached regarding the cases of loss of parcels, without providing other evidence of the explanations provided. In addition, the analysis of the above-mentioned of the document showed that the e-mail was not addressed to the Company, but to another entity ([P. Sp. z o.o.]). The company did not refer to this fact in its explanations. In addition, in Annex 3, the Company presented the correspondence of May 2020 (two e-mails) regarding the untimely notification of violations by the entity providing courier services.

The company also indicated that it is explaining infringement cases with the carrier on an ongoing basis in order to eliminate the problem of delays in providing information on data loss. The company also explained that the period of the pandemic had a significant impact on the timeliness of notifications of personal data breaches related to the proceedings in question in the scope of verifying the correct handling of the return documents process. As explained by the Company, due to the limitations of courier entities related to the pandemic period, the process of verification and handling of return documents was extended, hence the information about the events was reported by the carrier with a delay. The company emphasized that in its opinion, the actions it undertook bring effects in the long term, as the percentage of personal data breaches in relation to the volume of all shipments is small and presented calculations for the month of June in this regard.

Additionally, in response to the above-mentioned letter of the President of the Personal Data Protection Office of [...] July 2020. The company provided explanations regarding violations consisting in the delivery of documents to third parties, according to which in most cases, as it follows from the carrier's explanations, the persons to whom the documents are served are relatives (household members) data subjects. The company indicated that, in its opinion, the delivery of the document to a third person

who is a close person of the data subject causes a very low probability of materializing the possible risk of violating the rights and freedoms related to this event, and therefore requiring the Company to inform customers about the potential consequences in terms of breach of their personal data related to the transfer of their personal data to a third party - a close one, as a result of acting at the request or request of the client, is, in the opinion of the Company, at least pointless. However, the company did not explain which of the 3 questions from the letter of the President of the Personal Data Protection Office (UODO) it refers to, or what, in its understanding, it means the transfer of personal data to a third party - a close one, as a result of acting at the request or request of the client.

The analysis of the material collected in the case showed that in the scope specified in point 1) of the letter of the President of the Personal Data Protection Office of [...] July 2020, the Company did not provide sufficient evidence of its actions aimed at minimizing the risk of recurrence of the infringement. To the extent specified in point 2) of the letter of the President of the Personal Data Protection Office, in which a request was made to indicate the technical and organizational protection measures implemented by the Company in order to immediately find a breach of personal data protection and without undue delay notify the supervisory body and the data subject, the Company does not indicating whether technical or procedural measures have been implemented, it informed that it "explains the cases of violations on an ongoing basis with the carrier in order to eliminate the problem of delays in providing information about data loss." However, the e-mail correspondence attached by the Company in the subject "Late notification of violations" indicated that in May 2020 violations related to shipments sent in December 2019 and in January and February 2020 were explained, which questioned the above the quoted information of the Company in the scope of ongoing clarification of infringement cases with the carrier. The collected evidence could not confirm the additional explanations of the Company that "the timely reporting of personal data breaches related to the Office's proceedings regarding the verification of the correct handling of the return documents process was significantly influenced by the pandemic period", because 60% of the total number of personal data breaches reported in June 2020, events were identified by the Company over 60 days from the date of the violation event, and over 33% of the total number of reports were events identified by the Company over 90 days from the date of the event, i.e. pre-pandemic events. Over 17% of the total number of personal data breaches reported in June 2020 concerned events from January 2020 and 2019, which means that they were identified by the Company over 120 days from the date of the event causing the breach of personal data protection. Moreover, the Company did not refer to the request of the President of the Personal Data Protection Office to indicate whether

it analyzed the impact of the timely identification of personal data breaches on the rights and freedoms of data subjects, and if so, what were the results of the above-mentioned analysis.

The collected evidence indicated that the Company, as the data controller, may breach the provisions of Regulation 2016/679 in the scope of:

1. Failure to implement appropriate technical and organizational measures for the processing to be carried out in accordance with Regulation 2016/679 and to be able to demonstrate it, and failure to review and update these measures, which constitutes a violation of Art. 24 sec. 1 and art. 32 sec. 1 and 2 of Regulation 2016/679. / 2. Failure to notify, without undue delay, data subjects of a breach that may result in a high risk of violating the rights or freedoms of natural persons, which constitutes a breach of Art. 34 sec. 1 of Regulation 2016/679. 3. Failure to provide information in accordance with the request of the President of the Personal Data Protection Office, providing incomplete or unreliable information, failure to provide evidence confirming the submitted explanations, which constitutes a violation of Art. 31 of Regulation 2016/679.

In connection with the above, by a letter sent on [...] July 2020 (ref .: DKN.5130.3114.2020 [...]), the President of the Personal Data Protection Office initiated ex officio administrative proceedings in the scope covering the above-mentioned violations.

In a letter of [...] August 2020, being a response to the notice of initiation of administrative proceedings, the Company indicated, inter alia, that it operates in accordance with the Policy of assessing and notifying personal data breaches at Cyfrowy Polsat S.A. (hereinafter: "Policy"), attaching the content of the document as Appendix 1 to the explanations. The company indicated that in accordance with point 3.3. Polityka makes every effort to ensure that employees and associates have the necessary knowledge in the field of personal data protection, in particular violations, and that for this purpose, regular training in the field of personal data protection is carried out. As evidence, the Company presented the content of the announcement addressed to the employees of the Company informing about compulsory training in the field of personal data protection, which is attached as Appendix 2 to its explanations. One of the training modules are issues related to personal data breaches. At the same time, pursuant to point 3.4. Policies, entities processing data at the request of the Company, are obliged to cooperate with the Company in the field of identified violations of personal data protection.

The company indicated that the issues related to entrusting the processing of personal data, including the liability of the courier company towards the Company, are regulated by the cooperation agreement in the field of courier services, as well as an annex to this contract (hereinafter jointly: the "Agreement"), which imposes on the courier company in particular obligation to

secure the shipment during its transport and from the moment of its release to delivery to the recipient, the obligation to follow the instructions for the courier attached each time to the shipment, the content of which is attached as Appendix 4 to the indicated letter of the Company, the obligation to verify the identity of the person collecting the shipment with the data on the list shipping and documents contained in the package and securing the return documents through their safe deposit in the return envelope attached to the shipment, the obligation to immediately report the loss of the shipment and / or data contained therein to the Data Protection Officer of the Company and provides for the possibility of submitting a complaint as Provision of courier services, claiming damages provided for in the contract, including in particular the possibility of imposing penalties in the event of violation of the principles of protection of entrusted personal data.

The company indicated that it had taken steps to "eliminate future violations of events through, inter alia, preparation of instructions for the courier company on the recognition of personal data breaches and their immediate reporting. " The content of the instruction was attached by the Company as Annex 13 to the letter of [...] August 2020. The Company indicated that each courier receives educational material describing the basic issues of personal data protection, presenting the content of the "Guide for couriers" as Annex 20 to the above-mentioned writings. The company explained that in connection with the actions taken, it found a lower number of logistic violations in July 2020 than in the previous months, i.e. in May and June, presenting an appropriate statement in this regard. In addition, the Company provided explanations and documented that the correspondence (reference number [...] attached as a reply to the letter of the President of the Personal Data Protection Office of [...] July 2020, confirming the actions taken to eliminate or at least minimize the occurrence of violations of personal data protection related to with the delivery of parcels by courier companies, carried out between the carrier and [P. Sp. z oo], also applies to activities undertaken in this regard by the Company, because [P. Sp. zoo] on the basis of the contract between it and the Company of [...] January 2017 and Annex No. 1 of [...] May 2018, provides services for the logistic processes for the Company, and the activities related to [P. Sp. z oo] are the same in the context of servicing the Company's customers. above, the Company presented as Annex 16 to its explanations of [...] July 2020.

Additionally, referring to the number of notifications indicated in the notice of initiation of the procedure, the Company noted that due to the telecommunications activity conducted, each time it assesses the validity of notifying the breaches to the supervisory body and notifying the person, not based on the premises of Art. 33 and art. 34 of Regulation 2016/679, and on the basis of specific provisions, i.e. Commission Regulation (EU) No 611/2013 of 24 June 2013 on measures applicable to the

notification of personal data breaches, under Directive 2002/58 / EC of the European Parliament and of the Council on privacy and electronic communications (hereinafter "Regulation 611/2013"). According to Art. 2 clause 1 of Regulation 611/2013, the provider shall notify the competent national authority of all personal data breaches. Such a structure of the provision is definitely more rigorous than the disposition resulting from Art. 33 of the Regulation 2016/679, which in turn affects the number of notifications.

The company, in its explanations sent by letter of [...] August 2020, emphasized that Art. 33 of the Regulation 2016/679 states that "(...) he shall notify the supervisory authority competent pursuant to Art. 55, unless it is unlikely that the breach would result in a risk of violation of the rights or freedoms of natural persons ". At the same time, pursuant to Art. 3 sec. 2 lit. ac of Regulation 611/2013, the likelihood that a personal data breach may adversely affect the personal data or privacy of the subscriber or natural person shall be assessed taking into account, in particular, the following circumstances: a) the nature and content of the personal data concerned, especially if such data are related to financial information, specific categories of data referred to in art. 8 sec. 1 of Directive 95/46 / EC, e-mail data, location data, internet log files, registers of searched websites and lists of telecommunications services provided; b) the likely consequences of the personal data breach for the subscriber or individual concerned, especially if the breach could result in identity theft or falsification, bodily harm, mental suffering, humiliation or damage to reputation; and (c) the circumstances under which the personal data breach occurred, in particular where the data was stolen and when the provider became aware that the data is in the possession of an unauthorized third party. The company indicated that, taking into account the above, it made an individual risk assessment of each event having the characteristics of a breach of personal data protection, taking into account the dual nature of the provisions referred to above. The company assessed the seriousness of personal data breaches according to the methodology for assessing the degree of breach of data protection developed by the European Union Agency for Network and Information Security (ENISA), which proposed three main criteria: 1 (NREAP) Context of data processing, 2 (ŁI) Ease of identification of the data subject, 3 (ON) Circumstances of the breach, having an additional impact on the seriousness (severity) of the breach. As indicated by the Company, the final result of the infringement severity assessment (DN), after taking into account the adopted point values for individual criteria, can be obtained using the following formula: DN = NREAP x ŁI + ON.

In its explanations, the Company distinguished three types of violations, ie: 1) events related to the delivery of the shipment to a third party, where, according to the Company's explanations, in most cases the third party is the closest family member who

lives at the same address with the customer; 2) loss of documents by the courier company; 3) theft of a parcel with equipment. With regard to shipments delivered to third parties, the Company indicated that, according to the information provided by the courier company, such events, as a rule, occur at the express request of the Company's customer, and the courier acts against the instructions provided by the Company, thus breaking the rules of proper delivery shipment. Additionally, couriers often act at the express request of customers who ask them to hand over parcels to the people they designate, usually their closest family members. As regards the parcels delivered to third parties, the Company emphasized again that the analysis of these notifications shows that these persons are most often relatives (family members) of the people to whom the parcels are actually addressed. Therefore, issuing such documents to a person who knows this data and lives with the client in the same household, has greater consequences in terms of civil law [no authorization to sign the contract, and therefore no possibility to start the service by the Company] than it gives the risk of possible negative consequences in the sphere of the rights and freedoms of the data subject. At the same time, as explained by the Company, this method of delivering correspondence is a generally accepted principle in the delivery procedure in civil and administrative proceedings. As indicated by the Company, "the above allows the conclusion that there are no premises to claim that there may be negative consequences for the customer as a result of the described event, in the form of identity theft or the use of his data for, for example, extorting loans or medical services."]

The company indicated that it had performed a detailed infringement risk assessment for each of the three above-mentioned categories of events. As explained by the Company, the result obtained according to the ENISA methodology allowed to define the level of severity of a data protection breach for data subjects as low. The results of the "detailed risk analysis" of violations that are the subject of these proceedings, specified by the Company in its explanations, are presented respectively in Annexes 12, 14 and 15 to the Company's letter of [...] August 2020.

The company indicated that despite the analysis of violations, the result of which allowed to determine the level of severity of the data protection violation for data subjects as "low", it nevertheless notified these violations due to the guidelines of the President of the Personal Data Protection Office provided to the Company in the statement of [...] September 2018 (reference number [...]), indicating the need to notify events that included the PESEL number, considering the risk as "high".

Moreover, the Company indicated the compliance of its activities with Art. 33 of Regulation 2016/679 and recital 85 of Regulation 2016/679 and informed that on [...] February 2020 it imposed contractual penalties on the entity providing courier

services, in connection with the loss of personal data of the Company's customers, for the total amount of PLN [...] , presenting the debit note as Appendix 9 to his explanations. The company also indicated that it decided to impose further penalties for breach of the provisions of the contract by presenting debit notes of [...] June 2020 and [...] July 2020 for the total amount of PLN [...] (Annexes 10 and 11).

Due to the fact that the notice of initiation of the administrative procedure indicated, inter alia, on the possibility of the Company violating Art. 34 (1) of Regulation 2016/679 and the content of recital 87 was quoted, while the Company, in its letter of [...] August 2020, explained its compliance with the requirements set out in Art. 33 and recital 85 of Regulation 2016/679, and due to the fact that in the letters of [...] July and [...] August 2020, the Company did not reply whether it had analyzed the impact of the timely identification of personal data breaches on the rights or freedom of data subjects, and if so, what were the results of the above-mentioned analysis, the President of the Personal Data Protection Office (UODO), in a letter of [...] October 2020, again asked the Company to provide explanations in this regard. At the same time, the President of the Personal Data Protection Office asked for an indication whether, in addition to the contract with the courier company, the Company has internal procedures to ensure compliance with the requirements set out in Art. 34 sec. 1 of Regulation 2016/679, while asking for specific provisions from internal regulations. In the above-mentioned In the letter, the President of the Personal Data Protection Office also mentioned that in the notice of initiation of administrative proceedings, he referred to recital 87 of Regulation 2016/679, and not, as the Company indicated in its explanations, recital 85 of Regulation 2016/679. In addition, the President of the Personal Data Protection Office (UODO) asked for a detailed risk assessment methodology used by the Company to assess the risk referred to in point 2 of its explanations of [...] August 2020.

By letter of [...] October 2020, the Company provided additional explanations on the matter. With regard to the request of the President of the Personal Data Protection Office for a reply, whether an analysis of the impact of the timely identification of personal data breaches on the rights or freedoms of persons has been analyzed, the Company indicated, inter alia, that it undertakes activities aimed at analyzing the impact of personal data breaches on the rights and freedoms of natural persons . The company informed that it assesses the risk of the occurrence of consequences for the data subject individually in each case, through the prism of possible negative consequences for the data subject. The company indicated that as at the date of preparation of the said reply, it had not recorded any correspondence from persons whose data had been violated as to the incurring of any consequences by these persons, referred to in particular in Regulation 611/2013. The company explained that

"by carrying out a risk analysis, it assesses the potential negative effects for the data subject, using a list of threats prepared for internal purposes, including the rights and freedoms of a natural person that may constitute a breach, taking into account the risks, effects and preventive measures that are Annex 1 to this letter. ". Referring to the application regarding the identification of internal regulations aimed at ensuring compliance with the requirements set out in Art. 34 sec. 1 of Regulation 2016/679, the Company emphasized that as a telecommunications undertaking, it applies the provisions of Regulation 611/2013 first to the personal data of subscribers, and secondly the provisions of Regulation 2016/679. In addition, the Company indicated point 5.5 of the Policy of Assessment and Notification of Violations of Personal Data Protection in Cyfrowy Polsat SA, according to which "if it is established that there is a probability that the violation of personal data will have adverse effects on the personal data or privacy of the subscriber or natural person, the Administrator makes the notification referred to in point 5.5. Of the Policy, and also immediately informs the Data Subjects affected by the Breach of the Breach (...). If it is not possible to exhaustively define the Data Subjects affected by the Breach, the Administrator places information on its website or provides it in another way that maximizes the chance of reaching the relevant Data Subjects. " In response to the request for the submission of the detailed risk assessment methodology used for the risk assessment, the Company emphasized that in its previous letter sent to the Personal Data Protection Office on [...] August 2020, it indicated that when assessing the risk severity it uses the methodology for assessing the severity of the infringement prepared by the European Union Agency for Network and Information Security (ENISA). Moreover, in its explanations, the company sent the formulas used to assess the risk of infringements. The company also confirmed that individually conducted analyzes of the risk of violating the rights and freedoms of the data subject for each violation covered by this proceeding, in accordance with the ENISA methodology, were submitted to the Personal Data Protection Office (UODO) with its letter of [...] August 2020.

In addition, the Company informed that at the beginning of September 2020, there was a change in the parameters of services assigned to parcels sent to the carrier, in order to further oblige the courier to deliver the parcel only to the subscriber's own hands, whose details appear on the parcel's address label. In the opinion of the Company, the change allowed for the elimination of cases of delivering the parcel to an unauthorized person, including household members living at the same delivery address. The company also announced the implementation of additional measures aimed at improving the process of tracking parcels on the way, so as to determine its final status shortly after sending the parcel. All parcels sent via the Company's remote channels are periodically verified. According to the explanations of the Company, the information obtained

as part of explanations and interventions with the carrier allows the Company to take further actions regarding the shipment, including confirmation, in particular, of the loss of shipments, and thus faster identification and reporting of possible loss of personal data. The company indicated that, in its opinion, the introduced changes brought positive results, based on the scale of infringements, which significantly decreased in September 2020. the number of infringements related to the delivery of courier items in the period from April to September 2020

In the letter of [...] February 2021, the Company again indicated the period of the pandemic, which caused additional difficulties in the proper performance of services by the courier service provider, and indirectly contributed to the number of violations and delays in notifying the Company about these events.

The company emphasized that by making the said notifications (both to the President of the Personal Data Protection Office and to the data subjects), the Company was not delayed - it implemented them immediately after finding the breach (i.e. immediately after informing it about the event constituting a breach of data protection by the courier company).). The company also indicated that the lapse of a longer time between the events leading to a breach of personal data protection and the notifications made by the Company to the President of the Personal Data Protection Office and to the data subjects was not the result of the delay of the Company as the data controller, but the courier's failure to comply with the contractual and statutory obligation to immediately notify the personal data breach to the data controller.

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

Pursuant to the wording of Art. 24 sec. 1 of Regulation 2016/679, taking into account the nature, scope, context and purposes of processing as well as the risk of violating the rights and freedoms of natural persons of varying probability and seriousness, the controller implements appropriate technical and organizational measures to ensure that the processing is carried out in accordance with this Regulation and to be able to demonstrate it . These measures are reviewed and updated as necessary. This means that the controller, when assessing the proportionality of the safeguards, should take into account the factors and circumstances relating to the processing (e.g. type, method of data processing) and the related risks. At the same time, the implementation of appropriate safeguards is an obligation which is a manifestation of the implementation of the general principle of data processing - the principle of integrity and confidentiality, as defined in Art. 5 sec. 1 lit. f) Regulation 2016/679. The implementation of technical and organizational measures should rely on the administrator implementing relevant

provisions, rules for the processing of personal data in a given organization, but also regular reviews of these measures, and, if necessary, updating previously adopted safeguards.

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 likelihood 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, and regular testing, measurement and evaluation of the effectiveness of technical and organizational measures to ensure the security of processing.

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

Recital 87 of Regulation 2016/679 states, inter alia, that it is necessary to ensure that all appropriate technical protection measures and all appropriate organizational measures are implemented in order to identify a personal data breach immediately and inform the supervisory authority and the data subject swiftly. Whether the notification was made without undue delay should be determined taking into account, in particular, the nature and gravity of the personal data breach, its consequences and any adverse effects on the data subject.

In the opinion of the President of the Personal Data Protection Office, the Company insufficiently assessed the effectiveness of technical and organizational measures to ensure the security of the processing of personal data contained in documents provided to the Company's clients through the entity providing courier services, which constitutes a violation of Art. 24 sec. 1

and art. 32 sec. 1 and 2 of Regulation 2016/679.

First of all, it is necessary to refer to the explanations of the Company regarding the assessment of the risk of violation of the rights or freedoms of natural persons who were affected by the violation of the protection of personal data covered by this proceeding. In response to the initiation of administrative proceedings, the Company emphasized that pursuant to Art. 33 of Regulation 2016/679 "(...) notifies them to the supervisory authority competent pursuant to Art. 55, unless it is unlikely that the breach would result in a risk of violation of the rights or freedoms of natural persons ", while citing Art. 3 sec. 2 of Regulation 611/2013, according to which the probability that the breach of personal data may have adverse effects on the personal data or privacy of the subscriber or natural person, shall be assessed taking into account, in particular, the circumstances set out in points a-c of the said provision. Subsequently, the Company indicated that it had performed an individual risk assessment of each of the events having the characteristics of a breach of personal data protection. The company indicated that it assessed the seriousness of personal data breaches according to the data protection breach assessment methodology developed by the European Union Agency for Network and Information Security (ENISA).

In addition, the Company has distinguished three types of violations, ie 1) events related to the release of the parcel to a third party, 2) loss of documents by the courier company, 3) theft of the parcel with equipment. The company indicated that it had performed a detailed infringement risk assessment for each of the three above-mentioned types of infringements, presenting its results, respectively, in Annexes 12, 14 and 15 to the Company's letter of [...] August 2020.

In its letters of [...] August and [...] October 2020, the Company indicated that in all 3 types of breaches described above, based on an individual risk assessment according to the ENISA methodology, the result of the breach analysis made it possible to determine the severity of the breach of data protection for data subjects as "low". In the opinion of the Company, this also applies to violations consisting in theft of documentation, because, as the Company submitted, the thief was interested in the equipment sent to the customer, and not in his personal data. However, apart from the results of the analysis of such violations, the Company did not provide any other evidence justifying such an assessment.

The company explained that "despite the fact that the obtained result of the infringement analysis allowed to determine the level of severity of the data protection breach for the data subjects as" low ", the Company has nevertheless notified the violation, due to the guidelines of the President of the Personal Data Protection Office provided to the Company in the speech of [...] September 2018 (reference number [...]), indicating the need to notify events that included the PESEL number,

considering the risk as "high". " However, it is not clear from the above explanations whether the Company questions the assessment made by the President of the Personal Data Protection Office at the time, why it did not question it at the time and why it made reports, where in the application forms it indicated a high risk of violating the rights or freedoms of natural persons in connection with these violations despite the fact that different assessment of this risk.

At this point, it should be emphasized that the application (ref. data concern, about the breach of her personal data and provided the content of this notification. In the said request, the President of the Personal Data Protection Office indicated that the notification sent by the Company did not meet the conditions specified in Art. 34 sec. 2 of the Regulation 2016/679, i.e. it does not contain the information referred to in Art. 34 sec. 2 in connection with joke. 33 paragraph 3 lit. c) of Regulation 2016/679, as it does not describe the possible consequences of a breach of personal data protection. In response to the request, the Company informed by letter of [...] October 2018 that it had notified the data subject in accordance with the guidelines presented in the request of the President of the Personal Data Protection Office. The company did not question the indicated occurrence in any way, made reports of violations of personal data protection resulting from cooperation with the entity providing courier services and notified data subjects in cases concerning violations of personal data protection, in which there was a high risk of violating the rights or freedoms of natural persons . It should be emphasized that the Company raises the above only at the stage of these proceedings, thus questioning the legitimacy of its assessment of the high risk of violating the rights or freedoms of natural persons in the reports of personal data protection violations, since it could have already questioned it in response to the request of the President of the Personal Data Protection Office, ref. No. [...] of [...] September 2018.

Referring to the Company's assessment of the risk of violating the rights or freedoms of natural persons, presented for the types of violations identified by the Company, the following circumstances should be indicated. For violations related to the release of documentation to third parties, the Company argued that this documentation is most often issued to relatives and therefore issuing such documents to a person who knows these data and lives with the customer in the same household has greater consequences in terms of civil law [no authorization to sign the contract, and thus the inability to start the service by the Company], than it poses a risk of possible negative consequences in the sphere of the rights and freedoms of the data subject. In view of the above, it should be noted that, according to the Guidelines, depending on a specific situation, the administrator may consider a random recipient or a third party as "trusted", and the fact that the recipient is trusted may result

in the effects of the breach not being serious, but this does not mean that that there was no violation. This in turn may, however, eliminate the likelihood of a risk to individuals, with the result that there is no longer any need to notify the supervisory authority or the affected individuals. This means that the controller should make an assessment on a case-by-case basis. In its explanations, the company based its assessment on general information provided by the courier service provider, without presenting evidence of its individual analysis in this respect for individual cases of personal data breaches of this type. Although the Company informed that it had made a detailed assessment of the risk of violations consisting in delivering the parcel to a third party, the content of which is attached as Annex 12 (1-20) to the Company's explanations of [...] August 2020, however, the indicated documentation presented by the Company does not take into account the situation the delivery by the courier company of documents containing personal data of the Company's client to a person who could be considered a trusted recipient. It should be noted that recognizing the person who actually received the documentation containing the personal data of the Company's client as a trusted recipient would require that in each case the Company should examine the relationship between such a recipient and the client, e.g. whether they are in conflict and whether they already had all of them. customer's personal data. It should also be emphasized that the consequences raised by the Company in the field of civil law also translate into violation of the rights or freedoms of natural persons, referred to in Regulation 2016/679. This issue, as is clear from the documentation submitted by the Company, was also not taken into account by the Company when assessing the risk related to the breach of personal data protection.

The company in a letter of [...] July 2020 stated that in its opinion "it seems that the service of the document to a third party who is the data subject's relatives causes a very low probability of materializing the possible risk of violation of rights and freedoms related to this event", however, as indicated above, it has not sufficiently documented that it made an individual assessment of individual infringements of this type, basing its assessment mainly on explanations provided by the courier service provider. It should be emphasized that for the assessment of the high risk of violating the rights or freedoms of natural persons related to the violation of personal data protection, it is irrelevant whether this risk materializes, but the fact that the risk exists. Therefore, the arguments of the Company justifying the lack of a high risk of violating the rights or freedoms of natural persons in this regard cannot be accepted. Again, it should be emphasized at this point that the Company should explain each case individually, which it has not done according to the documentation presented. It should be emphasized that due to the scope of the disclosed personal data, violations of this type, in the absence of individual confirmation that the person

who received the documentation containing the client's personal data may be considered a trusted recipient, should be assessed as involving a high risk of violating the rights or freedoms natural persons and notify clients about them, which the Company did. Similarly, for the other two categories of violations identified by the Company, i.e. loss or theft of documentation containing personal data of customers, in the absence of an individual assessment sufficiently justifying the lack of high risk, due to the scope of the disclosed personal data, this risk should be assessed at a high level and notified about breach of the customer.

The President of the Personal Data Protection Office points out that the "detailed risk analysis" presented by the Company, constituting attachments to its explanations, is in fact printouts from the calculator of the severity of personal data protection violations available on the website of one of the entities providing support services in the field of personal data protection. The President of the Personal Data Protection Office (UODO) does not assess the correctness of the indicated calculator operation here, but underlines that it is possible to obtain any result with the help of calculators, depending on the data entered for the calculations. In addition, the above-mentioned printouts contain a reservation that "each breach or suspected breach of personal data protection should be analyzed individually, in particular with regard to the obligations set out in Art. 33 and 34 of the GDPR, therefore this calculator can only be used as an additional resource and cannot be used as an independent basis for decision-making by any entity or person that uses the calculator on their own responsibility ". These documents are not provided with the date of production, nor do they contain a description of the detailed criteria which the Company followed when making the assessment with the use of the indicated calculator. As already indicated, the risk assessment for breaches consisting in the delivery of documentation to a third party does not contain an individual assessment or justification that in a given case personal data has been disclosed to a trusted entity, which could justify, in this case, the assessment of the absence of a high risk of violation of the rights or freedoms of natural persons. . Apart from the indicated printouts from the calculator, the Company did not present such an assessment in relation to the other categories of infringements identified by it. In its explanations, the company only emphasizes that it performed the assessment in accordance with the ENISA method, without indicating any additional justification for the risk assessment criteria it adopted.

It should also be noted that the ENISA method indicates that the final score for the processing context (NREAP) may be increased or decreased depending on the occurrence of various factors, e.g. a wide range of data for one person, the nature of the data or possible negative consequences for the data subject, and the scale of the data breached (for the same person).

According to the Guidelines, a key factor in assessing risk is, of course, the type and sensitivity of the personal data that has been disclosed as a result of the breach. Typically, the risk of harm to those affected by a breach increases with the sensitivity of the data, but other personal data about those individuals that may already be available should also be taken into account (…). Breaches related to health data, identity documents or financial data such as credit card data can cause damage if they occur individually, but if they occur together, they can be used for identity theft. Typically, a collection of different personal data is more sensitive than a single piece of personal data. Moreover, in Art. 3 (2) of Regulation 611/2013, referred to by the Company in its explanations, also provides guidance on the factors that should be taken into account when reporting breaches in the electronic communications services sector. Pursuant to the provision in question, the probability that the personal data breach may adversely affect the personal data or privacy of the subscriber or natural person is assessed taking into account in particular the following circumstances: (...) the likely consequences of the personal data breach for the subscriber or natural person concerned , especially if the breach could result in theft or fraudulent identity, bodily harm, mental suffering, humiliation or damage to reputation.

The President of the Personal Data Protection Office (UODO), analyzing the assessment of the risk of violating the rights or freedoms of natural persons presented by the Company in the reports on violations of personal data protection covered by this proceeding, took into account the information contained in the content of these reports in this respect. When assessing the breach of personal data protection covered by this proceeding, the President of the Personal Data Protection Office decided that the breach of data confidentiality, in particular data concerning the total name and surname, address of residence or stay, PESEL number, series and number of an identity card or other identity document, telephone number and other categories of data concerning the contracting parties (e.g. contract ID, contract number, document number, hardware number, VAT invoice number and amount, account number for payments), causes a high risk of violating the rights or freedoms of natural persons, therefore it is necessary to notify the person, the data subject about the breach of their personal data. This means that when reporting personal data breaches, the Company correctly indicated in the notification forms that they cause a high risk of violating the rights or freedoms of natural persons.

The different risk assessment for reported violations presented at the stage of the proceedings in question was not sufficiently justified by the Company, and the printouts presented by the Company, subject to the supplier's reservation contained therein, may only be of an auxiliary nature and may not constitute the basis for assessing the risk of infringement of rights or the

freedom of individuals. The fact that the documentation presented by the Company may only be of an auxiliary nature can be proved by the fact that according to the "detailed", as the Company has defined it, assessments, events involving the loss of documentation by couriers containing personal data in the form of: name and surname, address of residence or stay, PESEL number, e-mail address, series and number of ID card or other identity document, telephone number and the above-mentioned other categories of data relating to the parties to the contracts, in accordance with the documentation provided by the Company (e.g. breaches marked by the Company [...], [...], [...]) were assessed not only as having a low severity (i.e. persons will not be affected by the breach or it will cause minor inconvenience), but also as events that are not subject to the reporting obligation. In the opinion of the President of the Personal Data Protection Office, in its calculations presented in the course of this proceeding, the Company did not take into account additional criteria related to the scope of disclosed personal data affecting the context of data processing, which in turn resulted in an unjustified risk reduction.

To sum up, the breaches of personal data protection covered by this proceeding resulting from the Company's cooperation with an entity providing courier services resulted in a high risk of violating the rights or freedoms of natural persons, and the Company, as the controller, was obliged to notify the data subjects of these breaches without undue delay.

In the course of the proceedings, the Company demonstrated that it has a Policy for the assessment and notification of personal data breaches in Cyfrowy Polsat S.A. The company indicated that in accordance with point 3.3. The Policy makes every effort to ensure that employees and associates have the necessary knowledge in the field of personal data protection, in particular violations, and that for this purpose, periodic training is carried out in the field of personal data protection, presenting as evidence the content of the message addressed to the employees of the Company informing about mandatory training in the scope of personal data protection.

The Company indicated that the issues related to entrusting the processing of personal data of the Company's clients, including the liability of the courier company towards the Company, were regulated in the contract with the entity providing courier services and in the relevant instructions for couriers.

It should be noted, however, that the Company, despite the implementation of the Policy and procedures for the protection of personal data related to reporting violations, as well as the conclusion of an agreement to entrust the processing of personal data with a processor, has not developed appropriate mechanisms to control the implementation of its obligations by the processor. The company indicated that it was taking steps to ensure the proper performance of the contract by the processor

and, consequently, to reduce the number of violations, presenting as evidence the correspondence attached to the explanations of [...] July 2020, but real steps in this regard were taken only in connection with a letter from the President of the Personal Data Protection Office of [...] July 2020, which presents the results of analyzes of personal data breaches reported by the Company, conducted at the Personal Data Protection Office, and then in connection with the initiation of the administrative procedure in question. The above is evidenced by the correspondence of the Company constituting Appendices No. 8 and 17 to the Company's letter of [...] August 2020.

In the course of the proceedings, the Company implemented a change in the parameters of services assigned to parcels delivered to the carrier, in order to further oblige the courier to deliver the parcel only to the Subscriber's own hands, which, in the opinion of the Company, allowed for the elimination of cases of delivering the parcel to an unauthorized person, including household members living at the same delivery address. As part of the shipment of parcels containing only a copy of the contract for the customer, additional elements of verification of the completeness of the parcels sent were added in the process. The company also announced the implementation of additional measures to improve the process of tracking parcels on the way, so as to establish its status shortly after sending the parcel. As indicated by the Company, the information obtained as part of explanations and interventions with the carrier allows the Company to take further actions with regard to the shipment, including confirmation, in particular, the loss of shipments, and thus faster identification and reporting of possible loss of personal data.

In the course of the administrative procedure, the Company provided explanations as to its compliance with the requirements set out in Art. 33 and recital 85 of Regulation 2016/679. In its explanations of [...] October 2020, the company emphasized that it applies the provisions of Regulation 611/2013 in the first place, and the provisions of Regulation 2016/679 second.

In the context of the above-mentioned explanations of the Company, it should be noted that the President of the Personal Data Protection Office at any stage of assessing the compliance of the Company with Regulation 2016/679 in the case of infringements covered by this procedure did not indicate the possibility of the Company violating the provision of Art. 33 of the Regulation 2016/679. The provisions of Regulation 611/2013, which the Company rightly pointed out in its letter of [...] August 2020, are more stringent than the provision of Art. 33 of Regulation 2016/679, imposing an obligation on telecommunications entities to notify the competent national authority of all personal data breaches, no later than 24 hours after the personal data breach is detected. The fact that the Company meets the requirements set out in Art. 33 of Regulation 2016/679 (and Article 2

of Regulation 611/2013), it does not also mean that it meets the requirements set out in other provisions of Regulation 2016/679. Notification of a breach of personal data protection to the supervisory body within the time limit specified in the above-mentioned provision of Regulation 2016/679 or within the time limit specified in art. 2 clause 2 of Regulation 611/2013 does not release the data controller from taking actions aimed at efficient and quick identification of violations of personal data protection. "The deadline for reporting a personal data breach is counted from the moment it is discovered. A finding of a breach should be understood as obtaining by the administrator knowledge of the facts that could be classified as meeting the conditions set out in Art. 4 point 12. However, the moment when the administrator performed such a subsumption is not decisive. It should be remembered that, according to recital 87, the controller should introduce such technical protection measures as to be able to immediately identify a breach of personal data protection. If this is not the case, the failure to find a violation will not violate Art. 33 paragraph 1 due to the fact that the deadline for reporting has not started, but the controller breaches the requirements for the implementation of appropriate technical measures to detect possible violations. It should be emphasized that any delay in notifying people about a breach of their personal data additionally increases the possibility of materializing the risk of violating their rights or freedoms. The earlier the person whose data has been disclosed is properly informed about the breach, the earlier it will be able to take steps to minimize the risk of negative consequences of the breach. As indicated in the Guidelines on the reporting of personal data breaches in accordance with Regulation 2016/679 of the Art. 29, the provisions of Regulation 2016/679 oblige both administrators and processors to adopt appropriate technical and organizational measures to ensure a level of security corresponding to the risk related to the processing of personal data. Controllers and processors should take into account the state of technical knowledge, the cost of implementation and the nature, scope, context and purposes of processing as well as the risk of violating the rights and freedoms of natural persons with a different likelihood and severity. In addition, Regulation 2016/679 requires the adoption of all appropriate technical protection measures and all appropriate organizational measures to immediately identify a personal data breach, which in turn is decisive for determining whether the notification obligation applies in a given case. This means that the ability to prevent breaches where possible and the ability to react promptly to breaches where they nevertheless occur is a key element of any data security policy.

In the submitted explanations, the Company showed that, immediately after receiving information about the breach from the processor, it reported breaches and informed the data subjects. However, the lack of a quick response on the part of the

processor does not remove the responsibility of the controller for finding a breach of personal data protection, because the ability to, inter alia, Detection of breaches should be seen as a key element of technical and organizational measures, including any data security policy. 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. Pursuant to Art. 32 sec. 2 of Regulation 2016/679, the controller, 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. 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. The collected evidence confirms that the Company undertook actions aimed at explaining the reasons for delays in reporting breaches by the entity providing courier services, however, these actions were taken after the breaches were reported by this entity. Therefore, the company should not wait only for breaches to be reported by the processor, but to implement appropriate solutions enabling the verification of these obligations, e.g. through ongoing monitoring of the parcel delivery stage.

The company, referring to the delays in reporting information about violations by the carrier, thus confirms the lack of verification mechanisms on the part of the Company.

In the course of the proceedings, the Company indicated point 5.5 of the Policy, according to which "if it is established that there is a probability that the breach of personal data will have adverse effects on the personal data or privacy of the subscriber or natural person, the Administrator shall make the notification referred to in point 5.5. Of the Policy, and also immediately informs the Data Subjects affected by the Breach of the Breach ". The collected evidence indicates, however, that the above-mentioned policy provision was in fact dead, as the Company did not implement sufficient mechanisms to enable ongoing monitoring of courier services. The company indicated that it is explaining infringement cases with the carrier on an ongoing basis in order to eliminate the problem of delays in providing information on data loss, however, the correspondence presented by the Company, in which the reasons for delays in reporting personal data breaches by the processor are

explained, does not confirm the explanations of the Company in in this regard (e-mail correspondence constituting attachments No. 5, 6 and 7 to the Company's explanations of [...] August 2020)

In the course of the proceedings, the Company has demonstrated that it has concluded an agreement for entrusting the processing of personal data with an entity providing courier services. The company, in its explanations of [...] August 2020, quoted the wording of § 8 of the contract, and then explained that it had issued debit notes on this account. The President of the Personal Data Protection Office does not deny that the Company undertook actions aimed at the proper performance of the contract, however, the attached debit notes do not apply to § 8 indicated by the company, but to other contractual provisions. Even if the Company would incriminate the processor for the untimely reporting of breaches of personal data protection, the collected evidence clearly indicates the lack of sufficient supervision in this respect, which, in addition to the actual dates of identification of events causing personal data breaches, is evidenced by the abovementioned Company's correspondence explaining the reasons for reporting the events, including from July, October and December 2019, where inquiries from the Company were sent in January and May 2020.

According to the Guidelines, "GDPR states that individuals should be informed of a breach" without undue delay "- ie as soon as possible. Notifying individuals is primarily intended to provide them with detailed information on the preventive actions that should be taken. Depending on the nature of the breach and the risk arising, prompt notification will allow individuals to take action to protect themselves from any negative effects of the breach ". The importance of immediate response to violations is emphasized both in the Guidelines and in the document entitled Administrators' obligations related to personal data breaches, issued by the President of the Personal Data Protection Office. In view of the above, in the course of the proceedings, the President of the Personal Data Protection Office asked the Company to answer whether the Company had analyzed the impact of the timely identification of personal data breaches on the rights or freedoms of data subjects. In a letter of [...] October 2020, the Company explained that "by carrying out a risk analysis, it assesses the potential negative effects for the data subject, using a list of threats prepared for internal purposes, including the rights and freedoms of a natural person that may constitute a breach, taking into account threats, effects and preventive measures ", presenting the above-mentioned the list as Appendix 1 to the explanations. However, the presented documentation does not contain criteria for assessing breaches in terms of their quick identification and, consequently, quick notification of data subjects about breaches. The company has not analyzed the impact of the timely identification of personal data breaches on the rights or freedoms of data subjects.

In the light of the above-mentioned of the Company's explanations, it should be reiterated that Regulation 2016/679 sets out a requirement requiring the controller to implement all appropriate technical security measures and all appropriate organizational measures to immediately identify a breach of personal data protection and promptly inform the supervisory authority and data subjects. Regulation 2016/679 also states that whether the notification was made without undue delay should be determined taking into account, in particular, the nature and gravity of the personal data breach, its consequences and the adverse effects on the data subject. This implies an obligation on the controller to maintain the ability to "detect" any breach in a timely manner, in order to ensure that the data subject can also take appropriate action.

In the course of the proceedings, the Company indicated that it had implemented procedures aimed at immediately informing the data subjects and the supervisory body about breaches of personal data protection, but the collected material confirms that it did not conduct sufficient supervision in this area, which consequently led to notifying data subjects of a breach of their personal data in most cases after 60 days from the date of the event that caused the breach. In June 2020, the Company made [...] reports of personal data breaches. [...] breaches, which constitute 60% of the total number of personal data breaches reported in June 2020, were identified by the Company over 60 days from the date of the breach event, and over 33% of the total number of notifications were events identified by the Company over 90 days from the date of the event. Over 17% of the total number of personal data breaches reported in June 2020 concerned events from January 2020 and 2019, which means that they were identified by the Company over 120 days from the date of the event causing the breach of personal data protection. In July 2020, the Company made further [...] notifications. […] Of them, which accounts for over 44% of the total number of reports, were infringements identified above 60 days from the date of the infringement event, and 15% of the total number of reports were events identified by the Company above 90 days from the date of the infringement event. Before receiving the letter of the President of the Personal Data Protection Office, in which the analyzes of the timeliness of identification of violations were presented, the Company did ask the courier service provider to explain the reasons for the delay, but as evidenced by the evidence collected in the case, these were follow-up actions after the event was reported by the entity providing courier services and related to explaining the reasons for delays in reporting violations of events even several months ago from the date of reporting (e-mail correspondence constituting attachments No. 5, 6 and 7 to the Company's letter of [...] August 2020). The presented sample correspondence regarding the explanation of the reasons for late reporting by the courier company of irregularities in the delivery of parcels concerned, inter alia, events of July, October and December 2019,

where inquiries from the Company were sent in January and May 2020, which indicates the lack of sufficient supervision in this area also in relation to personal data breaches identified by the Company before June 2020 . and also before the pandemic period.

The company in the explanations of [...] October 2020 indicated that immediately after the occurrence of late reports of the loss or breach of personal data by the processing entity at the request of the Company, the process of distribution of parcels and settlement of return documents were reviewed again, which allowed to identify areas, which needed to be improved. Thanks to this verification, the Company introduced additional system changes, as well as changes on the carrier's side in the reporting of return documents sent to the Company as well as the verification and timeliness of reports regarding the suspected loss of personal data of the Company's customers.

The evidence collected in the course of the proceedings shows, however, that real actions aimed at quick identification of events causing a breach of personal data protection were taken only in connection with the letter of the President of the Personal Data Protection Office of [...] July 2020, and then in connection with the initiation of this the scope of administrative proceedings (correspondence constituting Annexes 8 and 17 to the Company's letter of [...] August 2020). It is also impossible to agree with the statements of the Company that its actions in this regard were taken immediately after the emergence of cases of late reporting of data breaches by the processor, because, as indicated by the e-mail correspondence presented by the Company, cases of late reporting of violations by the processor identified have been by the Company at least from January 2020. The lack of effective organizational measures in this regard allowing for quick identification of violations of personal data protection is decisive for the Company's breach of obligations under Art. 24 sec. 1 and 32 sec. 1 and 2 of Regulation 2016/679.

In a letter of [...] October 2020, the Company also indicated that at the beginning of September 2020 it had implemented new mechanisms that made it possible to eliminate the cases of delivering the shipment to an unauthorized person. The company also announced the implementation of additional measures to improve the process of tracking shipments, which in turn causes faster identification and reporting of possible loss of personal data. In connection with the explanations of the Company in the above-mentioned scope, the President of the Personal Data Protection Office analyzed the reports not listed in the list of infringements constituting the basis for the initiation of this proceeding. As a result of the analysis of the reports made in August and September 2020 listed by the Company in the statement sent by letter of [...] October 2020, there was not a single case of breach identified by the Company within more than 90 days from the date of the event causing the breach, and

notifications of breaches protection of personal data, in which the Company identified a breach within more than 60 days from the date of the event, constituted 16% of the total number of reports of personal data breaches made during this period by the Company. However, it should be emphasized again that the Company took these actions only after the initiation of the administrative procedure.

In the course of the proceedings, the Company emphasized that the period of the pandemic had a significant impact on the timeliness of notifications of personal data breaches related to these proceedings. The President of the Personal Data Protection Office (UODO), without denying the fact that various types of delays may occur during the pandemic, also indicates that the material collected in the case confirms the lack of supervision of the Company in this area, which consequently led to notifying data subjects about a breach of their data protection. even two or three months from the date of the infringement. In June 2020, violations identified by the Company within more than 60 days from the date of the event constituted 60% of the total number of personal data breaches reported to the Personal Data Protection Office. While in July 2020, i.e. immediately after sending to the Company the analyzes performed at the Personal Data Protection Office in this respect, violations identified by the Company within more than 60 days from the date of the event causing the infringement still accounted for 44% of the total number of reports, In the analyzed period of August and September 2020, violations identified within more than 60 days from the date of the event constituted only 16% of the total number of reports.

The above analysis confirms that it was possible for the Company to take effective actions aimed at minimizing the scale of violations, as well as faster identification of violations related to the delivery of courier items, even despite the pandemic period. However, these mechanisms were implemented after the initiation of the administrative procedure and prior presentation of own analyzes made by the President of the Personal Data Protection Office. This is also confirmed by the fact that the Company did not apply appropriate organizational and technical measures prior to the initiation of administrative proceedings to ensure the security of personal data processing and quick identification of violations of personal data protection, and, consequently, a breach in this respect of the above-mentioned provisions of Regulation 2016/679.

One should agree with the explanations of the Company that violations of this type arise mainly due to human errors and it is not possible to eliminate them in 100% by implementing any additional organizational or technical measures, nevertheless the evidence gathered in the course of the proceedings indicates, which should be emphasized once again that the Company did not exercise adequate supervision in the area of processing personal data contained in documents sent via courier service

providers, due to the lack of implementation of appropriate measures to quickly identify breaches of personal data protection, as well as to minimize their scale.

Referring to the additional explanations of the Company, according to which "the number of notifications of violations made by the Company is affected by its compliance with the provisions of Regulation 611/2013, which are more stringent than the provisions of Regulation 2016/679, because pursuant to Art. 2 clause 1 of the Regulation, the supplier notifies the competent national authority of all cases of personal data breaches, which in turn affects the number of notifications made ", the President of the Personal Data Protection Office indicates that the subject of these proceedings were only reports of personal data breaches resulting from the Company's cooperation with entities providing courier services, in which the Company indicated a high risk of violation of the rights or freedoms of natural persons, and the analysis of these cases carried out by the President of the Personal Data Protection Office confirmed the assessment made by the Company. Reports of other violations of personal data protection made by the Company, in the case of which the assessment by the President of the Personal Data Protection Office confirmed the lack of a high risk of violation of the rights or freedoms of natural persons, or reports of violations of personal data protection not resulting from the Company's cooperation with entities providing courier services, are included in separate internal statements of UODO, and did not constitute the basis for statistical calculations as part of the analysis of reports presented in the content of this decision and were not the subject of this proceeding.

By the way, the cases of reported personal data breaches related to irregularities on the part of postal operators are not exceptional in the practice of the Personal Data Protection Office, exceptions are, however, situations in which the administrator does not take immediate action related to the loss or incorrect delivery of parcels containing personal data. customers.

In view of the above, it should be considered that the Company insufficiently assessed the effectiveness of the implemented technical and organizational measures to ensure the security of processing of personal data contained in documents sent through the entity providing courier services and to ensure quick identification of violations of personal data protection, which breached the provisions of Art. 24 sec. 1, art. 32 sec. 1 and 2 of Regulation 2016/679.

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 sec. 4 lit. a) of 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, the President of the Personal Data Protection Office - pursuant to Art. 83 sec. 2 lit. a-k of the regulation 2016/679 - took into account the following circumstances of the case, aggravating and affecting the size of the imposed financial penalty:

1. The nature, gravity and duration of the breach (Article 83 (2) (a) of Regulation 2016/679). When imposing the penalty, it was important that the breach of Regulation 2016/679 resulted in delays in notifying the Company's clients about the breach of security. their personal data. Due to the lack of implementation of technical and organizational measures enabling quick identification of violations of personal data protection causing a high risk of violating the rights or freedoms of natural persons, the company notifies its clients about the violation with a significant delay (over 17% of the total number of violations of personal data protection reported in June 2020 concerned the events of January 2020 and 2019, which means that they were identified by the Company over 120 days from the date of the event causing a breach of personal data protection). The proceedings covered notifications of personal data breaches made by the Company in June and July 2020. The collected evidence indicates, however, the lack of supervision in this area already in the earlier period, because the reports of violations from this period included events identified by the Company even after 120 days from their occurrences. In addition, the sample correspondence presented in the course of the proceedings regarding the explanation of the reasons for late reporting by the courier company of irregularities in the delivery of parcels concerned, inter alia, events of July, October and December 2019, where inquiries from the Company were sent in January and May 2020, which indicates the lack of sufficient supervision in this area also in relation to personal data breaches identified by the Company before June 2020 The above-presented results of the analysis of notifications of personal data breaches made by the Company clearly indicate excessive - in relation to the deadlines recognized as appropriate by the provisions of Regulation 2016/679 - delays in identifying violations and, consequently, delays in notifying about violations to persons affected by these violations. Such delays, resulting - as shown above - from the failure by the Company to implement appropriate technical and organizational measures ensuring quick identification of violations of personal data protection, should be considered serious and requiring a negative assessment in the context of the risk borne by persons whose personal data were violated. As recital 85 of Regulation 2016/679 indicates: "In

the absence of an appropriate and quick response, a breach of personal data protection may result in physical damage, property or non-material damage to natural persons, such as loss of control over own personal data or limitation of rights, discrimination, theft or falsification of identity, financial loss, unauthorized reversal of pseudonymisation, breach of reputation, breach of confidentiality of personal data protected by professional secrecy or any other significant economic or social damage. '

2. The degree of liability of the Company (as an administrator), taking into account the implemented technical and organizational measures (Article 83 (2) (d) of Regulation 2016/679). The arrangements made by the President of the Personal Data Protection Office allow the conclusion that the Company, despite the concluded contract with the service provider courier service and relevant provisions in the Policy, did not exercise proper supervision in this area, thus not identifying on an ongoing basis violations of personal data protection related to the shipment of documentation containing personal data, which consequently led to notifying the data subjects after a significant time from the date an event causing a breach of the protection of their personal data. Therefore, it should be stated that the Company is liable for failure to implement mechanisms guaranteeing the effectiveness of measures (contractual provisions and provisions of the Company's internal documents), which are intended to ensure - in accordance with the provisions of Regulation 2016/679 - identification of violations of personal data protection and, consequently, reporting them to the President of the Personal Data Protection Office and about them to the people affected by the violation.

3. Categories of personal data concerned by the violation (Article 83 (2) (g) of Regulation 2016/679). Notifications of personal data violations covered by this proceeding concerned irregularities in the delivery of parcels containing personal data in the scope of: name, surname, address of residence or stay, PESEL identification number, often an e-mail address, series and number of an identity card or other identity document, telephone number and other categories of data concerning the parties to the contracts (e.g. contract ID, contract number, document number, hardware number, number and VAT invoice amount, account number for payments). Such a wide scope of personal data disclosed to unauthorized persons and held by these persons for a long time - as a consequence of the breach found in this decision - without the knowledge and without the possibility of any reaction from the data subject, must have a negative impact on the assessment of the breach found and the amount of the administrative fine . It should be emphasized that the breach by the Company involves a high risk of violating the rights or freedoms of the persons affected. The Guidelines already cited above clearly indicate the high risk associated with the

disclosure of, in particular, data relating to identity documents, they also emphasize that "a collection of various personal data is usually of a more sensitive nature than a single element of personal data".

When determining the amount of the administrative fine, the President of the Personal Data Protection Office took into account as a mitigating circumstance the premise specified in Art. 83 sec. 2 lit. f of the Regulation 2016/679, i.e. the degree of cooperation of the Company with the supervisory body in order to remove the breach and mitigate its possible negative effects. The President of the Personal Data Protection Office noticed and positively assessed the fact that the Company (after presenting its analyzes by the President of the Personal Data Protection Office and initiating this proceeding) took steps to faster identify breaches of personal data protection. Despite the fact that in the course of the proceedings the Company questioned the high risk of violating the rights or freedoms of natural persons related to the violations covered by the procedure, it implemented mechanisms, as a result of which both the number of violations of personal data protection related to such events, as well as those identified they are much faster. This is confirmed by the results of the analysis of personal data breach notifications made by the Company in August and September 2020 presented above in the justification to this decision (page 25).

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

1. Unintentional nature of the violation (Article 83 (2) (b) of Regulation 2016/679) - the President of the Personal Data Protection Office did not find in this case any deliberate actions of the Company leading to the violation of the provisions of Regulation 2016/679, but negligence in the control of the effectiveness of technical and organizational measures ensure the security of personal data processing in the process of delivering parcels to its clients, do not provide grounds for exempting it from liability for the violation found. 2. Actions taken by the Company to minimize the damage suffered by the data subjects (Article 83 (2) (c) of Regulation 2016/679) - in this case, no damage was found to the persons affected by the infringement, therefore there is no grounds for expecting the Company to take actions aimed at minimizing them. 3. Relevant previous violations of the provisions of Regulation 2016/679 by the Company (Article 83 (2) (e) of Regulation 2016/679) - no relevant prior violations of Regulation 2016/679 were found on the part of the Company. The way in which the supervisory body learned about the breach (Article 83 (2) (h) of Regulation 2016/679) - the President of the Personal Data Protection Office found the breach by analyzing reports of personal data breaches made by the Company itself, however, due to the fact that the

Company, when making of these reports, it only fulfilled its legal obligation, there are no grounds to believe that this circumstance constitutes an attenuating circumstance for the Company. 5. Compliance with previously applied measures in the same case, referred to in Art. 58 sec. 2 of Regulation 2016/679 (Article 83 (2) (i) of Regulation 2016/679) - in this case, the measures referred to in Art. 58 sec. 2 of Regulation 2016/679. 6. Application of approved codes of conduct pursuant to Art. 40 of the Regulation 2016/679 or approved certification mechanisms pursuant to Art. 42 of Regulation 2016/679 (Article 83 (2) (j) of Regulation 2016/679) - the Company does not apply approved codes of conduct or approved certification mechanisms referred to in the provisions of Regulation 2016/679. 7. Financial benefits achieved directly or indirectly in connection with the infringement or avoided losses (Article 83 (2) (k) of Regulation 2016/679) - the President of the Personal Data Protection Office did not state in the course of these proceedings that the Company obtained any financial benefits by committing the infringement subject to the penalty or she avoided any financial loss.

Taking into account all the above-mentioned circumstances, the President of the Personal Data Protection Office concluded that the imposition of an administrative fine on the Company is necessary and justified by the weight, nature and scope of the alleged infringements of the provisions of Regulation 2016/679. It should be stated that any other remedy provided for in Art. 58 sec. 2 of Regulation 2016/679, and in particular stopping at a reprimand (Article 58 (2) (b)), would not be proportionate to the identified irregularities in the processing of personal data and would not guarantee that the Company will not commit similar acts in the future as in this negligence case.

Pursuant to art. 103 of the Act of 10 May 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.

In the opinion of the President of UODO, an administrative fine of PLN 1,136,975 (in words: one million one hundred and thirty-six thousand nine hundred and seventy-five zlotys), which is the equivalent of EUR 250,000 (average EUR exchange rate from January 28, 2021 - PLN 4.5479)), performs the functions referred to in Art. 83 sec. 1 of Regulation 2016/679, i.e. it is effective, proportionate and dissuasive in this individual case. In the course of the proceedings, the Company presented the

financial statements for 2019, according to which its net sales revenues amounted to approximately PLN 2.38 billion, and the net profit amounted to PLN 586.8 million. It should also be noted that the Company is the parent entity of the Cyfrowy Polsat SA Capital Group, whose net sales revenues for 2019 amounted to approx. PLN 11.68 billion, and the net profit in 2019 was approx. PLN 1.1 billion (data presented by The Company in the "Consolidated annual report for the financial year ended December 31, 2019" posted on the website at the address https://grupapolsat.pl/sites/default/files/documents/cps_raport_Roczny_2019.pdf). Considering the above-presented financial results of both the Company and the capital group in which the Company is the parent company, it should be stated that the imposed administrative fine will not be excessively severe.

The administrative fine will fulfill a repressive function in these specific circumstances, as the Company has violated the provisions of Regulation 2016/679, but also preventive, i.e. preventing violations of the provisions on the protection of personal data in the future by both the Company and other data administrators. Moreover, the applied financial penalty meets the conditions referred to in Art. 83 sec. 1 of Regulation 2016/679, due to the importance of the infringements found in the context of the basic requirements and principles of Regulation 2016/679. II. At the same time, on the basis of the evidence gathered in the course of the proceedings, it should be stated that the company did not breach the remaining provisions of Regulation 2016/679 being the subject of this proceedings.

In a letter of [...] July 2020, the President of the Personal Data Protection Office, pursuant to Art. 58 sec. 1 lit. a) and e) of Regulation 2016/679, asked the Company to provide information and evidence to confirm it. By letter of [...] July 2020, the Company sent some of the clarifications requested by the President of the Personal Data Protection Office, providing only 3 e-mails as proof of this, one of which was sent by the carrier to another entity, which the Company did not explain in its reply. Therefore, when initiating administrative proceedings, the President of the Personal Data Protection Office also indicated the possibility of violating Art. 31 of the Regulation 2016/679, i.e. the lack of cooperation between the Company and the President of the Personal Data Protection Office, who demanded that the information necessary to consider the case be presented. Only after initiating the administrative procedure, the Company presented additional explanations and evidence to confirm the explanations submitted by it. The evidence obtained in this way was sufficient to issue an administrative decision, therefore the proceedings had to be discontinued as regards the possibility of violating Art. 31 of Regulation 2016/679.

In the course of the proceedings, the Company showed that it notifies data subjects about the breach of their personal data, immediately after finding the breach, while applying the provisions of Regulation 611/2013. As regards the possibility of the

Company violating Art. 34 sec. 1 of Regulation 2016/679, the proceedings became redundant due to the fact that the Company, without undue delay, fulfilled (even if it currently questions the existence of a high risk of violation of the rights or freedoms of natural persons related to violations) of the obligation to notify persons affected by the violation about this violation. Delays in fulfilling the obligation specified in Art. 34 sec. 1 of Regulation 2016/679 resulted from the lack of mechanisms enabling quick identification of violations of personal data protection, and not the delay between the finding of such violations and the notifications of the persons affected by them. In connection with the above, the proceedings had to be discontinued in the scope of the possibility of the Company violating the above-mentioned recipe.

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

2021-05-13