THE CHAIRMAN OF PERSONAL DATA PROTECTION

Warsaw, 08

June

2021

DECISION

DKN.5131.10.2020

Based on Article. 104 § 1 of the Act of June 14, 1960, Code of Administrative Procedure (Journal of Laws of 2021, item 735) and art. 210 paragraph 1 and 2 in connection with Art. 210a paragraph. 1 point 2 and sec. 2 and art. 174a paragraph. 1 of the Act of July 16, 2004, Telecommunications Law (Journal of Laws of 2021, item 576), after conducting administrative proceedings initiated ex officio on reports of personal data breaches made by P4 Sp. z o.o. with headquarters in Warsaw at ul. Wynalazek 1, President of the Office for Personal Data Protection,

finding a breach by P4 Sp. z o. o. with headquarters in Warsaw at ul. Invention 1 of Art. 174a paragraph. 1 of the Act of July 16, 2004 Telecommunications Law (Journal of Laws of 2021, item 576) in connection with joke. 2 clause 2 of the 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 (Journal U.UE.L.2013.173.2), consisting in not notifying the President of the Personal Data Protection Office about personal data breaches within 24 hours from the detection of the personal data breach, imposes on P4 Sp. z o. o. with headquarters in Warsaw at ul. Invention - 1 fine in the amount of PLN 100,000 (say: one hundred thousand zlotys).

Justification

P4 Spółka z oo, hereinafter referred to as the "Company" or "administrator" as one of the telecommunications operators operating in the territory of the Republic of Poland, processes the personal data of subscribers professionally and on a mass scale in connection with the provision of mobile telecommunications services, sale of mobile telecommunications devices and the provision of network management services distribution of telecommunications products.

The company notified the President of the Personal Data Protection Office (hereinafter also referred to as the "President of the Personal Data Protection Office") about the personal data breaches of the Company's clients on the following days:

- [...] October 2020 (issued [...] October 2020), administrator's reference number: [...], date of finding the infringement: [...]

October 2020, which was registered under the reference number [...];

- [...] December 2020 (issued [...] December 2020), administrator reference number: [...], date of finding the infringement: [...] November 2020, which was registered under reference number [...];

- [...] December 2020 (issued [...] December 2020), administrator reference number: [...], date of finding the infringement: [...] November 2020, which was registered under reference number [...];

- […] December 2020 (assigned […] December 2020), reference number: […], date of finding the infringement: […] November 2020, which was registered under reference number […];

- [...] December 2020 (issued [...] December 2020), administrator's reference number: [...], date of finding the infringement: [...] November 2020, which was registered under the reference number [...].

By submitting the above-mentioned notification of personal data breach, the Company did not inform the supervisory body about the reasons for the delay in notifying the President of the Personal Data Protection Office about the breach.

In connection with the above, by letters of [...] October 2020 (in the case reference number [...]) and of [...] December 2020 (in the case reference number [...], [...], [...] and [...]), the President of the Personal Data Protection Office asked the Company to provide explanations within 7 days from the date of delivery of the letter, including: what were the reasons for the delay in submitting the notification of a personal data breach to the supervisory body, i.e. in its submission after 24 hours from the finding of the violation, which period results from Art. 2 clause 2 of the 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 (Journal U.UE.L.2013.173.2), hereinafter referred to as Regulation 611/2013.

In response to the above, the Company, in a letter dated [...] October 2020 ([...]), presented that the quotation: "(...) 1. a personal data breach was found on […] October 2020; 2. the notification to the data subject was sent by letter of [...] October 2020; 3. a notification of a personal data breach to the President of the Personal Data Protection Office regarding the above event was sent by letter of [...] October 2020 (case reference [...]), in accordance with Art. 174a paragraph. 1 of the Act of July 16, 2004, Telecommunications Law (consolidated text, Journal of Laws of 2019, item 2460, as amended), i.e. within the time limit specified in Art. 2 clause 2 of the Commission Regulation (EU) No 611/2013 of 24 June 2013 on measures applicable to the notification of personal data breaches, pursuant to Directive 2002/58 / EC of the European Parliament and of the Council

on privacy and electronic communications (...) ".

However, in a letter of [...] December 2020 ([...]), the Company explained that the quotation: "(...) 1. all breaches of personal data protection were found on [...] November 2020; 2. notifications to data subjects were sent on […] and […] November 2020; 3. notifications about a breach of personal data protection to the President of the Office for Personal Data Protection) regarding the above events were submitted to the Company's office on [...] November 2020 in the morning for dispatch in accordance with the deadline resulting from Art. 174a paragraph. 1 of the Act of July 16, 2004, Telecommunications Law (consolidated text, Journal of Laws of 2019, item 2460, as amended) and Art. 2 clause 2 of the 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; 4. the delay in sending the notices was caused by an inadvertent error of an employee of the Company's office (action without malicious intentions); 5. On [...] December 2020, the data protection officer of the Company provided the supervisor of employees of the Company's law office with a notice reminding him to exercise due diligence in timely shipment of parcels to the President of the Personal Data Protection Office (...) ".

Responding to the explanations of the Company contained in the letter of [...] October 2020 (reference number: [...]), quotation: "(...) a notification of a personal data breach to the President of the Personal Data Protection Office regarding the above event was sent by letter of [...] October 2020 (case reference [...]) (...) ", it should be noted that the indicated parcel was posted by the Company by registered mail on [...] October 2020 via the postal operator PSA as clearly evidenced by the date of the postmark (with the date [...] October 2020). Consequently, this means that the Company notified the personal data breach in question (found on [...] October 2020) within the deadline resulting from Art. 2 clause 2 of Regulation 611/2013, i.e. 24 hours after its detection.

Due to the lack of notification of the personal data breach (administrator reference [...]) within the period specified in Art. 2 clause 2 of Regulation 611/2013, on [...] November 2020, the President of the Personal Data Protection Office initiated administrative proceedings against the Company in this regard (case reference number: [...]).

In response to the notification on the initiation of administrative proceedings, the Company, in a letter of [...] November 2020 (reference number [...]), informed that the quotation: "(...) 1. after detailed arrangements regarding the dispatch of the Company's report [...], the delay was caused by an inadvertent error of an employee of the Company, without malicious

intentions, dealing with the dispatch of correspondence, for which I apologize on behalf of the Company; 2. the employee was instructed on the need to timely send reports of violations of personal data protection to the President of the Office for Personal Data Protection (...) ”.

On [...] February 2021, the President of the Personal Data Protection Office, pursuant to Art. 61 § 1 and 4 of the Act of June 14, 1960, Code of Administrative Procedure (Journal of Laws of 2020, item 256, as amended), notified the Company that the proceedings against P4 Sp. z o.o. with its seat in Warsaw, administrative proceedings with reference number [...] was extended to include the following personal data breaches:

1) Company name: [...], registered in the Personal Data Protection Office under the reference number [...]; 2) Company name: [...], registered in the Personal Data Protection Office under the reference number [...]; 3) Company name: [...] , registered in the Personal Data Protection Office under the reference number [...] 4) Company name: [...], registered in the Personal Data Protection Office under the reference number [...], which were also notified to the supervisory body after the deadline resulting from Art. 2 clause 2 of Regulation 611/2013.

In response to the above-mentioned letter, the Company in a letter of [...] March 2021 ([...]) explained the facts of the situation, pointing in particular to the following: "(...) Company letter of [...] November 2020 ([...]), the appendices of which (Appendices No. 2-5) were notifications of a breach of personal data protection with reference numbers: [...], [...], [...] and [...] (hereinafter the "letter"), was submitted to the Company's office in on [...] November 2020 in the morning and transferred on the same day by an employee of the Company's office to an employee of PSA The package containing the personal data breach notices was dispatched that day and left the Company. The person handling the shipment at the Company's office, however, did not enter the letter in the mailing book provided to the employee of P. S.A. along with all your shipments. The parcel containing the letter was returned to the Company by P. S.A. on [...] November 2020 - attached (Appendix 2) a copy of the non-compliance report, confirming the Company's explanations, in particular with regard to the lack of an entry in the sending book. The person accepting the return (the same who handled the shipment) did not notice that there were 2 returned parcels under the outgoing book and attached everything that was brought by an employee of P. S.A. to a binder with mailing books. On [...] December 2020, another employee of the Company's office, browsing a binder with mailing books, noticed the returned 2 letters and gave them immediately with priority. In accordance with the information provided by the Company in a letter of [...] December 2020 ([...]), the Data Protection Officer of the Company provided the person supervising the work of the Company's office on [...]

December 2020, reminding him of the need to exercise due diligence in timely shipment of parcels to the President of the Office for Personal Data Protection (hereinafter: "PUODO"), who reprimanded the law office employee who handled the shipment and return of the letter. Currently, this person is no longer an employee of the Company. "The company also explained that" (...) The reports were sent on time and left the Company, unfortunately they were returned by PSA due to an error by an employee of our law firm (this is confirmed by the PSA's non-compliance report). data subjects, etc.) (…) ". Notification of [...] March 2021, in which the President of the Personal Data Protection Office informed the Company, inter alia, on the collection of evidence sufficient to issue a decision and on the right to comment on the evidence and materials collected in the course of the proceedings and on the requests submitted (within 7 days from the date of receipt of this letter by the Company), was delivered to the Company on [...] April 2021 In response to the above-mentioned notification, on [...] May 2021, the representatives of the Company submitted to the President of the Personal Data Protection Office a letter entitled "Request of a party to impose an administrative fine together with a statement on the evidence and materials collected in the proceedings". In this letter (submitted without observing the above-mentioned seven-day deadline), the persons applying for the proceedings as the Company's attorneys at the same time submitted explanations, requested that the evidence indicated in the letter be admitted and carried out, and filed:

1) for the cancellation of the entire administrative procedure conducted by the President of the Personal Data Protection Office,

2) or: for the President of the Personal Data Protection Office to refrain from imposing an administrative fine and be content with an instruction due to the fact that the gravity of the violation of the law is negligible and the party to the proceedings has ceased to violate the law (Article 189f § 1 point 1 of the Code of Administrative Procedure),

3) relatively (in the event that the President of the Personal Data Protection Office did not agree to the arguments of the Company and decided that there were no grounds for redemption and did not refrain from imposing an administrative fine): o the maximum possible reduction in the amount of the administrative fine by the President of the Personal Data Protection Office, due to the existence of premises lowering the penalty (Art. 189d CAP).

Justifying the above-mentioned conclusions, the Company's representatives indicated, inter alia, that the violation of (quoted) "(...) Art. 2 clause 2 of Regulation 611/2013, consisting in the delay in sending the notification of a personal data breach by the Company to the supervisory body is a minor breach "and that: (quoted)" In this case, the statutory conditions for waiving the penalty were met, because:

1) the company has ceased to violate the law (restored legal status),

2) the gravity of the violation of the law in the sanctioned norm is negligible for the following reasons:

a) the breach of the legal order was incidental (one-off),

b) the subject of the breach of the sanctioned standard were only delays in the fulfillment of the notification obligation towards the supervisory authority (notification), which, however, did not affect the effectiveness of the subsequent notification activity,

c) breach of the sanctioned standard did not result from the party's disregard of the legal order, but was caused only by simple errors of the entrepreneur's employees,

d) the scale of breaches of the sanctioned standard was negligible from the point of view of the comprehensive and timely performance of the obligation included in the sanctioned standard,

e) breach of the sanctioned standard did not cause any negative consequences in the area of goods protected by the said standard ”.

In a letter of [...] May 2021, the Company's representatives emphasized that (quoted) "(...) the Company, despite failing to meet the 24-hour deadline set out in Art. 2 clause 2 of Regulation 611/2013, it provided the supervisory authority with the notification of a breach of personal data protection as soon as possible, which means that it restored the legal status. The essence of the obligation specified in Art. 2 clause 1 and 2 of Regulation 611/2013 is to provide the President of the Personal Data Protection Office with information on the occurrence of a breach of personal data protection, so that he can verify the actions taken by the provider of publicly available telecommunications services and possibly indicate other necessary steps to be performed ”. Moreover, in the same letter it was indicated that (quoted):

“The breaches of the norm sanctioned by the Company consisted in incidental notification of the breach after the expiry of the 24-hour period specified in Art. 2 clause 2 of Regulation 611/2013: - once in relation to the notification of a data protection breach marked by the Company as [...], and - the second time in relation to four notifications of data protection violations ([...], [...], [...] and [...], which were sent as one parcel to the President of the Personal Data Protection Office ([...]) ",

“(…) The scale of breaches of the norm sanctioned by the Company was negligible from the point of view of the comprehensive and timely fulfillment of the obligation included in the sanctioned norm. The five notifications of personal data breaches that are the subject of this proceeding account for only 1.5% of all breaches reported to the supervisory authority in 2020, which confirms that the breach of the breach notification deadline is incidental, as the Company carefully manages the

personal data breaches that occur. It should also be noted that in 2020, the Company's office handled approx. 15,000 outgoing registered parcels. Two parcels containing notifications of data breaches that are the subject of this proceeding account for only 0.013% of all outgoing parcels registered from the Company's headquarters. ”Concluding extensive arguments, the representatives of the Company stated, inter alia, that (quoted):

"As professional attorneys, we take into account that in terms of evidence it is easiest for a public administration body to demonstrate failure to meet the deadline as a basis for imposing a penalty, but in our opinion, taking into account the circumstances of this case, it is not sufficient to punish the obligated entrepreneur, precisely due to the entirety of the function of this punishment. In the present case, the penalty will not fulfill its basic function - a protective function ",

"(...) there is no need to additionally motivate the entrepreneur with a penalty to comply with the law, and the application of sanctions will be disproportionate to the infringement, the more so as this infringement - as shown above - did not have a negative impact on the values protected by the sanctioned standard. Therefore, the proceedings concerning the imposition of a penalty may also be discontinued as redundant, as the non-existence of the protective function may result in the lack of a material element of the relationship, and at most the authority in this case may substantially waive the imposition of the penalty. On the other hand, the possible imposition of a penalty in this case will not correspond to the principle of a just sanction, and will even be an expression of punishment for the sake of the punishment itself ”.

Having read the entirety of the evidence, the President of UODO considered the following.

Pursuant to Art. 174a paragraph. 1 of the Act of 16 July 2004 Telecommunications Law (Journal of Laws of 2021, item 576), the provider of publicly available telecommunications services notifies the President of the Personal Data Protection Office about the personal data breach within the time limit and on the terms specified in the 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 (OJ EU L 173, 26/06/2013, p. 2). Pursuant to Art. 2 clause 2 of the 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 (Journal U.UE.L.2013.173.2), the provider shall notify the competent national authority of the personal data breach no later than 24 hours after the personal data breach is detected, if practicable.

The above-mentioned provisions precisely indicate the date by which providers of publicly available telecommunications

services are required to notify the competent national authority (the President of the Personal Data Protection Office) about the breach of personal data. The company, as a provider of publicly available telecommunications services, was obliged to apply these provisions, and was obliged to organize the process of notifying about violations of personal data protection to the President of the Personal Data Protection Office in such a way as to make them within the time limit specified in the aforementioned provisions of law. Notifications of personal data breaches that were received by the supervisory authority exceeding this deadline (administrator's designations: [...] - date of finding the breach: [...] October 2020, date of posting: [...] October 2020, date of receipt: […] October 2020 and […], […], […] and […] - date of finding the infringement: […] November 2020, date of posting: […] December 2020, date of receipt: [...] December 2020), while confirming the lack of proper organization of this process.

The company, justifying the above-mentioned notifications of personal data breaches after the deadline resulting from art. 2 clause 2 of Regulation 611/2013 indicated inadvertent errors of the office employees responsible for sending correspondence, including correspondence regarding personal data breaches addressed to the President of the Personal Data Protection Office, consisting in e.g. failure to enter the correspondence in the mailing book, which resulted in its return by the postal operator. The errors of the Company's employees in this respect cannot, however, be considered a circumstance justifying the delay in notifying the supervisory body about the personal data breach. This is because they only show that the Company has improperly organized the process of notifying the President of the Personal Data Protection Office about personal data breaches, the more so as the Company has not demonstrated at any stage of the proceedings that it exercises adequate supervision over this process, and in particular over the law office employees responsible for sending such correspondence. It should also be noted that neither the provisions of the Telecommunications Law Act nor Regulation 611/2013 provide for the possibility of exceeding the 24-hour deadline in the notification of personal data breach for such reasons.

At this point, it is worth emphasizing that the Company decided to send all correspondence regarding personal data breaches to the President of the Personal Data Protection Office via the postal operator P. S.A. In view of the above, it should be noted that the President of the Personal Data Protection Office repeatedly sent letters to the Company, e.g. on [...] March 2020 in the case of [...] (administrator's name: [...]), on [...] April 2020 in the case of [...] (administrator's name: [...]), on [...] May 2020 in the case of [...] (administrator's name: [...]), on [...] August 2020 in the case of [...] (name of the administrator: [...]) and on [...] October 2020 in the case of [...] (administrator's name: [...]), to provide explanations regarding the notification of the violation

after 24 hours from its detection, i.e. after the deadline resulting from art. 2 clause 2 of Regulation 611/2013. Additionally, in some cases, eg in the case of […], the President of the Personal Data Protection Office informed the Company that the notification of a personal data breach can be made in two ways: electronically and by traditional mail, and indicated that the fastest way was to send the notification via the business platform. gov.pl or the ePUAP platform, which ensures that the deadline specified in the above-mentioned provision of Regulation 611/2013.

In the cases ([...], [...], [...]), the Company explained in particular that the team members worked remotely, and due to the state of epidemic threat announced in Poland, the closest possible date to send notifications of infringement to the President of UODO It was Monday, or that the employee preparing the personal data breach notification made an obvious typographical error on the date the breach was found ([...], [...]). In view of the above, it should be concluded that repeated reports of a personal data breach exceeding the deadline resulting from art. 2 clause 2 of Regulation 611/2013 constitute an aggravating circumstance for the telecommunications operator due to the failure to apply appropriate measures to eliminate similar events in the future.

Therefore, it should be considered that the Administrator has calculated the risk of not reporting personal data breaches to the President of the Personal Data Protection Office on time, which is also an aggravating circumstance.

The Company did not draw any conclusions from this correspondence, and in particular, it did not change the way of organizing the sending of correspondence regarding notifications about personal data breaches addressed to the President of the Personal Data Protection Office, still sending it via the postal operator P. S.A., which required involvement in this process, among others the chancellery employees responsible for its shipment. The consequence were, in particular, the errors of these employees, resulting in the Company not meeting the 24-hour deadline for notifying the President of the Personal Data Protection Office of the personal data breach, resulting from Art. 2 clause 2 of Regulation 611/2013, in the case of infringements marked by the Company […], […], […], […] and […]. This practice was changed by the Company only on [...] February 2021 - from that date infringements submitted by the Company via the ePUAP platform began to be submitted to the President of the Personal Data Protection Office.

It should be noted that the President of the Personal Data Protection Office, pursuant to Art. 174a paragraph. 2a of the Telecommunications Law and Art. 2 clause 4 of Regulation 611/2013, it provided secure electronic means of notification of personal data breaches (via the biznes.gov.pl platform and the ePUAP platform), as well as information on the mode of access

to these measures and their use (information in this regard is available in particular on the website of the Office for Personal Data Protection). Therefore, there were no contraindications for the Company to use these means to notify the President of the Personal Data Protection Office before […] February 2021. Thus, it should be stated that reporting the personal data violations covered by this proceeding to the President of the Personal Data Protection Office within the period specified in Art. 2 clause 2 of Regulation 611/2013 was workable.

It should be emphasized that providers of publicly available telecommunications services, and thus also the Company, are not only obliged to protect the personal data of people using their services, but also in the event of a breach of personal data protection, they are obliged to notify the national supervisory authorities of this fact, in Poland - The President of the Personal Data Protection Office. The overriding purpose of any notification of a breach to a supervisory authority is to protect the rights and freedoms of natural persons. An extremely important issue in this case is the controller's reaction time, i.e. notifying the supervisory authority about a breach as soon as possible. A personal data breach should be reported no later than 24 hours after the breach is detected. The company should make every effort to send the information required by law within 24 hours.

In the case in question, which clearly follows from the findings made, it should be stated that the Company did not report any personal data breaches (administrator's designations: [...], [...], [...], [...] and [...]), to the President of the Personal Data Protection Office the deadline specified in Art. 174a paragraph. 1 of the Telecommunications Law in connection with Art. 2 clause 2 of Regulation 611/2013.

When deciding to impose a fine on the Company, the President of the Personal Data Protection Office also familiarized himself with the arguments of the Company contained in the application of [...] May 2021 and considered them in the context of the findings made so far. It stated, inter alia, that the fact that the Company finally made notifications of violations of personal data protection (without meeting the deadline provided for by law) does not mean, however, that the Company "ceased to violate the law". In the present case, there was undoubtedly a breach of the norm resulting from Art. 2 clause 2 of Regulation 611/2013 and late notification does not cure the violation of this provision. As already indicated, the meaning of the provision of Art. 2 clause 2 of Regulation 611/2013 is to ensure the fastest possible reaction of the administrator - and then the supervisory authority when justified. It is difficult to assume that the Company, by notifying the supervisory authority of the violations without meeting the deadline (in the case of four violations being the subject of this proceeding, the notification took place 12 days after their discovery), "restored the legal status" - such a statement is not allowed by the purpose of the regulations,

which this term follows.

In its application of [...] May 2021, the company also pointed to the negligible gravity of the violation of the law in the sanctioned standard, inter alia, referring to the fact that "the breach of the legal order was incidental (one-off)". Meanwhile, as shown above, other violations reported by the Company were also violated by the legal deadline. It is also impossible to ignore the fact that this procedure covered five notifications of personal data breaches - hence, the breach of the provisions could not be of a one-off nature.

The Company's proxies, demonstrating the negligible importance of the violation of the law in the above-mentioned They also indicated in the letter that "the subject of the breach of the sanctioned standard were only delays in the fulfillment of the notification obligation towards the supervisory authority (notification), which, however, did not affect the effectiveness of the subsequent notification activity". As already shown above, the fact that there has been a notification of a breach of personal data protection does not, in the opinion of the President of the Personal Data Protection Office, mean that the legal status has been restored. Indication in the wording of art. 2 clause 2 of Regulation 611/2013, the specific deadline for making the notification is not accidental, and the acceptance of the Company's arguments in this respect would distort the meaning of this provision.

The insignificant seriousness of the violation of the law was demonstrated by the Company in the letter of [...] May 2021 also by indicating that (quoted): "the breach of the sanctioned standard was not due to the party's disregard for the legal order, but was caused only by simple errors of the entrepreneur's employees ". Avoiding repeating the arguments of the President of the Personal Data Protection Office (UODO) referred to earlier in this decision, it is worth emphasizing once again that in the present situation, the reason for not meeting the deadline resulting from Art. 2 clause 2 of Regulation 611/2013 on the side of the Company's employees. Supervision over employees (as well as notifying about breaches of personal data protection with keeping the deadline provided for by law) remains the responsibility of the administrator and he is responsible for its implementation.

In support of its thesis that the infringement of the law was negligible, in the above-mentioned in a letter of [...] May 2021, it appointed, inter alia, the argument that (quoted): "the scale of breaches of the sanctioned norm was negligible from the point of view of the comprehensive and timely performance of the obligation included in the sanctioned norm". In the opinion of the President of the Personal Data Protection Office, the statement that (quoted): "The five notifications of personal data breaches

that are the subject of this proceeding are only 1.5% of all violations reported to the supervisory authority in 2020 (...)" cannot justify the assumption that there was no for breach by the Company of the provision of Art. 2 clause 2 of Regulation 611/2013. The fact that the Company makes many reports of violations of personal data protection, and most of them are reported within the legal deadline, does not remedy the breach of law made by the Company. By the way, it is also worth noting that from the date of informing the administrator about the breach of personal data to the date the Company finds the breach, nineteen days should not pass, as was the case with the notification marked by the administrator with the reference number: [...] - registered by the local Office under the reference number [...] (in the notification, the anonymised content of which the Company provided to the President of the Personal Data Protection Office, the following excerpt was included: "I would like to inform you that on [...] September 2020, P4 Sp. z oo, with its registered office in Warsaw, ul. Taśmowa 7, (hereinafter referred to as "the Company") has been informed about an event related to the processing of your personal data "- the Company, by notifying about the breach, indicated, however, that it had not found the breach of personal data protection until [...] October 2020). Referring also to the arguments of the Company contained in the letter of [...] May 2021, it is worth pointing out that the argument cited by the Company remains completely irrelevant for the assessment of the Company's conduct that (quoted): "(...) in 2020 the Company's office handled approximately 15,000 outgoing registered mail. The two parcels containing reports of data breaches that are the subject of this proceeding account for only 0.013% of all outgoing parcels registered from the Company's headquarters ”.

In a letter of [...] May 2021, the company also argued that (quoted): "breach of the sanctioned standard did not cause any negative consequences in the area of goods protected by the said standard". The Company's representatives emphasized that the persons whose data concerned the infringement had been notified of this infringement. However, in the opinion of the President of the Personal Data Protection Office, the fulfillment by the controller of one of the obligations imposed on him by law (i.e. notification of a breach of personal data of persons affected by it) does not make his failure to fulfill another obligation negligible.

In order to complete the response to the Company's arguments contained in the letter of [...] May 2021 (as the legitimacy of imposing a fine on the Company will be shown further in the justification of this decision), the President of UODO emphasizes that the purpose of his action is not to "punish for the sake of punishment ", but the protection of the rights and freedoms of natural persons - and these values should also be guided by the administrators when carrying out their duties provided for in

the provisions on the protection of personal data.

Pursuant to Art. 210a paragraph. 1 point 2 of the Telecommunications Law, who does not fulfill the information obligation towards the President of the Personal Data Protection Office, referred to in art. 174a paragraph. 1 - is subject to a financial penalty imposed by the President of the Personal Data Protection Office in the amount of up to 3% of the income of the punished entity achieved in the previous calendar year. Pursuant to Art. 210a paragraph. 2 of the Telecommunications Law, to penalties imposed on the basis of par. 1 of this provision, the provisions of Art. 209 paragraph. 1a-3 and art. 210 of the Telecommunications Law. The powers of the President of UKE specified in these provisions are vested in the President of the Personal Data Protection Office. Pursuant to Art. 210 paragraph 2 of the Telecommunications Law, when determining the amount of the fine, the President of UKE takes into account the scope of the breach, the entity's activities to date and its financial capabilities.

When deciding to impose an administrative fine on the Company, the President of the Personal Data Protection Office - pursuant to Art. 210 paragraph 2 of the Telecommunications Law - took into account the following circumstances of the case which necessitate the application of this type of sanction in this case and influencing the amount of the imposed fine:

1. Scope of the infringement. In accordance with the well-established doctrine position developed under the Telecommunications Law, “the scope of the infringement should be determined taking into account the basic objectives of the Act, taking into account mainly the objective harmful elements. They relate to the type of breached obligations, the type of breached goods, the intensity of the breach and social and economic values, the consequences of the act subject to financial penalty, the amount of the damage caused, the mode of action "(S. Piątek, Telecommunications Law. Commentary, Commentary to Article 210 (2), Warsaw 2019, 4th edition, Legalis). The basic objectives of the Act referred to above include "providing users with maximum benefits in terms of the variety, price and quality of telecommunications services" (Article 1 (2) (4) of the Telecommunications Act). In the opinion of the President of the Personal Data Protection Office, the phrase "maximum benefits in the field of [...] quality of telecommunications services" covers the highest possible level of protection of personal data of users (persons using a publicly available telecommunications service or requesting the provision of such a service). The above position is confirmed by the formulation of one of the objectives of the regulatory policy pursued by the authorities competent in telecommunications matters, that is "contributing to ensuring a high level of personal data protection" (Article 189 (2) (3) (c) of the Telecommunications Law Act). In the present case, it was found beyond doubt that the provisions

on the protection of personal data were violated - provisions protecting a good of high social value (constituting an element of the constitutional right to privacy) and economic value (the use of which may be associated with obtaining large material benefits). The violation concerned the Company's obligation towards the President of the Personal Data Protection Office, and not towards the data subjects, however, in the opinion of the President of the Personal Data Protection Office, this infringement reduces the high (optimal under certain circumstances) level of protection of personal data of the Company's customers. This is because it delays the reaction of the President of the Personal Data Protection Office to the occurring (in the case of the Company - numerous) violations, which may prevent or at least limit possible negative consequences for the data subjects. Such a breach affecting the personal data protection system, not being a one-off accident, but - as shown below in the section on "the entity's current operations" - the Company's constant practice (which can be defined as a high-intensity activity) deserves a negative assessment, which is expressed by is the imposition of a financial penalty on the Company in this case. At the same time, the President of the Personal Data Protection Office notices the circumstances which have a mitigating effect on the amount of the penalty imposed, namely: a) inadvertent breach (delays in the procedure of notifying the President of the Personal Data Protection Office about personal data breaches) not resulting from the Company's intention to do so, but from improper organization of this procedure, b) the fact that as a result of the breach, no damage was found on the part of persons who were affected by the breaches of personal data protection covered by this proceeding, reported by the Company with the failure to comply with the deadline specified in Art. 2 clause 2 of Regulation 611/2013, c) the fact that in the course of the present proceedings regarding the imposition of a fine on the Company, the Company made changes in the procedure of notifying the President of the Personal Data Protection Office on personal data violations in order to eliminate the possibility of future infringement subject to penalty in this case. 2. Previous activity of the entity. The premise of the "previous activity" of the subject of the penalty, which affects the penalty, is a directive aimed at individualising the penalty due to the evaluation of the activity of this subject in the past, which is to indicate in particular whether the violation is an incidental event and not resulting from from the business policy of this entity (which would not entail a high risk for a large number of the Company's customers; therefore, it would not have to be an incriminating circumstance for the Company), or the violation of applicable regulations (in this case, the provisions on the protection of personal data) is somehow included in the entity's policy and included in its profit and loss account (which should be considered an aggravating circumstance). The assessment of the entity's activities to date covers a wide range of specific circumstances, such as: the entity's performance of its statutory obligations, violations of the

law committed by it, previously imposed penalties or other administrative sanctions, previous cooperation with the President of the Personal Data Protection Office (the authority competent in matters of personal data protection) in in the performance of his tasks. Notifications of personal data breaches covered by this proceeding were not the first breaches reported by the Company to the President of the Personal Data Protection Office after 24 hours from their detection, i.e. in breach of the deadline specified in Art. 2 clause 2 of Regulation 611/2013. In the case of these violations, the President of the Personal Data Protection Office sent correspondence to the Company, e.g. on [...] March 2020 in the case of [...] (administrator's name: [...]), on [...] April 2020 in the case of [...] (administrator's name: [...]), on [...] May 2020 in the case of [...] (administrator's name: [...]), on [...] August 2020 in the case of [...] (administrator's name: […]) And on […] October 2020 in the case of […] (administrator's name: […]), to submit relevant explanations in this regard. Additionally, in some cases, eg in the case of […], the President of the Personal Data Protection Office informed the Company that the notification of a personal data breach can be made in two ways: electronically and by traditional mail, and indicated that the fastest way was to send the notification via the business platform. gov.pl or the ePUAP platform, which ensures compliance with the above-mentioned deadline. Despite these letters, the controller decided to make changes in the organization of the process of sending correspondence regarding personal data breaches to the President of the Personal Data Protection Office, only from [...] February 2021 - then they began to receive notifications of personal data breaches to the supervisory body via ePUAP platforms. Consequently, this means that the Company has not developed appropriate mechanisms for a long time to ensure timely notification of personal data breaches to the President of the Personal Data Protection Office. It did so only as a result of decisive action (treated by the President of the Personal Data Protection Office as a last resort) - initiating proceedings to impose a fine on it for the infringement. In the opinion of the President of the Personal Data Protection Office (UODO), the activity of the Company which processes personal data in a professional and mass-scale manner, described above, is reprehensible and demonstrates the disregard for the obligations arising from the provisions of the Telecommunications Law in the field of personal data protection. 3. The Company's financial capacity. From the "Annual report for the year ended December 31, 2020" published by the Company on the website [...] shows that in 2020 the Company's operating revenues amounted to PLN 7,054,988,000, while its net profit - PLN 887,901,000. The fact that the Company achieves a net profit of nearly PLN 888 million in only one financial year proves the very large financial capacity of the Company, for which the fine of PLN 0.1 million imposed by this decision will constitute - in the opinion of the President of the Personal Data Protection Office - small, but adequate to the seriousness of the

infringement found, the financial burden. At this point, referring to the request of the Company's representatives "for the maximum possible reduction" of the amount of the fine, contained in the letter of [...] May 2021, the President of the Personal Data Protection Office indicates that the amount of the fine is 0.011% of the net profit earned by the Company in 2020. This value is much lower than the ratio indicated by the Company (and which is to prove the "minor" nature of the deficiencies) the ratio of delayed notifications on personal data breaches constituting the subject of this proceeding to all violations reported to the President of the Personal Data Protection Office by the Company in 2020 (1.5 % - as calculated by the Company's representatives in a letter of [...] May 2021).

Taking into account all the above-mentioned circumstances, the President of the Personal Data Protection Office decided that imposing a fine on the Company is necessary and justified by the Company's breach of Art. 174a paragraph. 1 of the Telecommunications Law in connection with Art. 2 clause 2 of Regulation 611/2013.

The President of the Personal Data Protection Office, after conducting a comprehensive analysis of the evidence collected in the course of the proceedings, taking into account the permissible amount of the fine specified in Art. 210a paragraph. 1 point 2 of the Telecommunications Law, set the amount of the fine imposed on the Company at PLN 100,000 (in words: one hundred thousand zlotys). It should be emphasized that the determined amount of the fine, taking into account the Company's revenues, is within the limit of 3% of the income of the punished entity achieved in the previous calendar year, indicated in the above-mentioned provision of the Telecommunications Law (representing 0.0014% of the operating revenues achieved by the Company in 2020). In the opinion of the President of the Personal Data Protection Office, the amount of the imposed fine corresponds to the Company's financial capabilities and the scope of violation of the law. When imposing the above fine, the President of the Personal Data Protection Office took into account the activities of the Company to date, and in particular the fact that the Company has not been penalized by the President of the Personal Data Protection Office so far. A fine in this amount is adequate to the violation found in the course of these proceedings and fulfills the intended functions: repressive (the penalty is imposed for violation of obligations under the law), preventive (to seek similar violations in the future) and disciplining providers of publicly available telecommunications services (is intended to discourage them from breaking the law). The punishment is, on the one hand, an inconvenience for the punished entity, and on the other hand, it is to relate to its financial capabilities. These conditions were met when imposing the fine in the amount specified in this Decision.

It should be emphasized that the penalty will be effective if its imposition leads to the fact that the Company, professionally and

on a mass scale processing personal data, will in the future fulfill its obligations in the field of personal data protection, in particular with regard to timely notification of data breaches. personal data of the President of the Personal Data Protection Office.

In this factual and legal state, the President of the Personal Data Protection Office resolved as in the sentence.

2021-06-11