Warsaw, on 03

November

2022

Decision

DKN.5131.18.2022

Based on Article. 104 § 1 of the Act of June 14, 1960 Code of Administrative Procedure (Journal of Laws of 2022, item 2000) and art. 210a sec. 1 points 2 and 3 in connection with joke. 174a sec. 1 and 3 of the Act of July 16, 2004 Telecommunications Law (Journal of Laws of 2022, item 1648, hereinafter referred to as: "Telecommunications Law") in connection with joke. 2 sec. 1 and 2 and art. 3 section 1, 3 and 4 of Commission Regulation (EU) No. 611/2013 of June 24, 2013 on the 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 connectivity electronic (Journal of Laws UE.L.2013.173.2, hereinafter referred to as: "Regulation 611/2013"), as well as art. 209 sec. 1a and art. 210 sec. 2 in relation to joke. 210a sec. 2 of the Telecommunications Law, after carrying out administrative proceedings initiated ex officio regarding the infringement by P4 Sp. z o.o. with headquarters in Warsaw at ul. Invention 1 of the provisions of the Telecommunications Law, President of the Office for Personal Data Protection,

stating that P4 Sp. z o.o. with its seat in Warsaw, the provisions of art. 174a sec. 1 and 3 of the Telecommunications Law in connection with joke. 2 sec. 1 and 2 and art. 3 section 1, 3 and 4 of Regulation 611/2013, consisting in not notifying the President of the Office for Personal Data Protection about a personal data breach within 24 hours of detecting a personal data breach and not immediately notifying the subscriber affected by the breach of personal data, imposes on P4 Sp. z o.o. with its seat in Warsaw, a fine of PLN 250,000 (say: two hundred and fifty thousand zlotys).

Justification

The President of the Personal Data Protection Office, hereinafter referred to as the "President of the UODO", on February [...] 2022 received information from Mr. J. G., hereinafter referred to as the "third party", sent by e-mail from the e-mail address: [...], who stated that: "Today I received an e-mail with the Play contract. I am not a Play customer, the contract concerns another person with the same name. The contract contains all the data of this person, including PESEL and ID number." To the above information, a third party attached an e-mail received from P4 Sp. z o.o., ul. Invention 1, 02-677 Warszawa

(hereinafter referred to as the "Company" or "Administrator"), from which it follows that: "As requested, we are sending you a set of documents for order No. [...]".

In connection with the above information, in a letter of [...] February 2022, the President of the UODO requested the Company to provide information on the personal data breach of February 2022, consisting in allowing an unauthorized third party to view the "(...) set [u] documents for order No. [...]" and to present an assessment in terms of the obligation to report a breach to the supervisory authority and notify the data subject.

The response, which the Company provided in the letter of [...] March 2022 [...], shows in particular that:

Order number [...] concerns Mr. J. G. (hereinafter: "Client"). On [...] February 2022, at the Sales Service Point (hereinafter: "POS"), the Customer concluded with the Company an agreement for the provision of telecommunications services number [...] for telephone number +48 [...] (hereinafter: "Agreement").

In addition to the data necessary to conclude the contract, the Customer also indicated the contact number and e-mail address for contact: […].

During the process of concluding the Agreement, an e-mail was generated containing a copy of the Agreement with attachments (Regulations and Price Lists). The message was sent to the address indicated by the Customer in the Agreement.

On [...] February 2022, the Customer returned to the POS with information that the address indicated in the Agreement was incorrect and asked for its removal. The customer did not indicate a different e-mail address for contact. The company noted this fact in the application number […].

The company, after receiving a summons from the President of the UODO, contacted the POS employee where the contract with the Customer was concluded, asking for an explanation of the course of the event.

The company has determined that when the person concluding the contract provides an e-mail address for contact during the process of signing the contract with printing of documents (to be signed), the sending of copies of documents to the indicated e-mail address is automatically generated. You can choose not to ship by marking a special field in the sales system. The POS employee did not uncheck this box and therefore an e-mail with copies of documents was sent to the Customer.

A copy of the Agreement was sent to the address specified in the Agreement, previously signed by the Customer. Signing the document is a signal for the Administrator that the Company, by sending an e-mail to the address indicated in the Agreement (even if it is incorrect), contacts the data subject (based on the signed document and data confirmation), and not with another

person.

The company shares the position of the President of the UODO expressed in the decision regarding the case ZSPR.440.1090.2019 "[...] Each person may freely indicate their e-mail address, because they bear the consequences of failure to collect correspondence sent to this address. The company is not able to verify the authenticity of the data regarding the e-mail address provided by the client, and by directing correspondence to an e-mail address other than the one indicated by the interested person, it would fail to exercise due diligence in contacts with this person, which would make it impossible to effectively deliver correspondence to it via this channel contact.[…]".

Until [...] March 2022, the Company did not record information from the Customer about an incorrect shipment and thus disclosure of his personal data to an unauthorized person. The company also did not record a signal from a third party about possible unauthorized access to the Customer's personal data as a result of incorrect sending. "Due to the above, the Company has no grounds to treat the event in question as a violation of (...) personal data."

Summarizing the above, it was found that despite:

- obtaining on February [...], 2022, information from the Client (J.G.) about the wrong indication by him in the Agreement concluded with the Company on February [...], 2022, of the e-mail address to which the Agreement containing personal data was sent, i.e.: name and surname, address of residence or stay, PESEL registration number, e-mail address (incorrect), series and number of ID card, telephone number (whereas the request to remove it was recorded by the Company in the application number xxxxxxxxx),
- receipt of a request for clarification of [...] February 2022, in which the President of the Personal Data Protection Office called on the Company to provide information on the data breach of February 2022, consisting in allowing an unauthorized third party to view a set of documents for order No. [xxxxxxxxxx] and to present the assessment of this event in terms of the obligation to report the breach to the supervisory authority and notify the data subject,

The company stated that there are no grounds for treating the event in question as a personal data breach, therefore it did not report the above-mentioned infringement to the President of the UODO and failed to notify the Client (subscriber) of it in accordance with Art. 174a sec. 1 and 3 of the Telecommunications Law in connection with: art. 2 sec. 1 and 2 and art. 3 section 1, 3 and 4 of Regulation 611/2013.

In the absence of notifying the President of the UODO of the personal data breach and failing to notify the Client (subscriber)

affected by the breach, on April […], 2022, the President of the UODO instituted administrative proceedings against the Company in this regard (letter reference: DKN.5131.18 .2022).

After the Company received a notification of the initiation of administrative proceedings, on [...] April 2022, the Company's representative appeared at the Office for Personal Data Protection to inspect the case files, and then on [...] April 2022 (as from the Submission Certificate indicated by the Official Administrator), the Company sent to the President of the UODO a notification of a personal data breach [...] together with the content of the subscriber's letter of April 2022 about the breach of his personal data.

In the submitted notification, the Company indicated, inter alia: that: "On [...] February 2022, P4 was informed by the President of the Personal Data Protection Office (hereinafter: PUODO or the Office) about an event related to the processing of the data subject's personal data (letter from DKN [...]). In connection with the incident, P4 took actions and explanatory actions, which show that: a) On February [...], 2022, at the Partner's Sales Service Point (hereinafter: POS), the data subject signed an agreement for the provision of telecommunications services (hereinafter: Agreement);b) the Agreement indicated an e-mail address for contact, which was not questioned by the data subject in any way before signing it, and by signing the Agreement, the data subject confirmed the correctness of the data contained in the Agreement (including the e-mail address for contact) ;c) a message containing the Agreement with attachments was sent to the indicated e-mail address, despite the fact that the data subject signed the agreement on paper at the POS;d) on [...] February 2022, the data subject reported to the POS that the address indicated on the Agreement is incorrect and requested its removal. The data subject did not indicate a different e-mail address for contact;e) on February [...], 2022, P4 received a request from PUODO to provide explanations on the information obtained by the Office about the violation of (…) personal data, consisting in enabling an unauthorized third party access to "[...] a set of documents for order number [xxxxxxxxxx]";f) P4 analyzed the case and sent a reply to PUODO on [...] March 2022, describing the result of the event analysis and the mechanism based on which the sending of e-mails mail to the data subject has been generated. P4 also indicated in the letter the reason for not qualifying the event as a breach of (...) personal data of the data subject;g) on April […], 2022. P4 received a notification from PUODO about the initiation of the proceedings (letter DKN.5131.18.2922);h) on [...] April 2022, the P4 Data Protection Officer (hereinafter: DPO) appeared at the Office to review the case files.

After obtaining additional information as a result of the review of the case files (in particular the content of the notification

submitted to PUODO by a third party whom the Company did not know before) and re-analyzing the material collected in the case, on [...] April 2022, the DPO found a violation (...) personal data of the data subject.

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

Article 174a sec. 2 and 4 of the Telecommunications Law indicate that a personal data breach is understood as accidental or unlawful destruction, loss, change, unauthorized disclosure or access to personal data processed by a telecommunications undertaking in connection with the provision of publicly available telecommunications services, and a breach of personal data that may have an adverse effect on the rights of a subscriber or end user who is a natural person, it is understood as such a breach which may result in particular in the unauthorized use of personal data, property damage, violation of personal rights, disclosure of a bank secret or other professional secret protected by law.

In accordance with art. 174a sec. 1 of the Telecommunications Law, the provider of publicly available telecommunications services shall notify the President of the UODO of a breach of personal data within the time limit and on the terms set out in Regulation 611/2013. Pursuant to Art. 2 sec. 1 and 2 of Regulation 611/2013, the supplier shall notify the competent national authority of all cases of personal data breach, and notification of such a case shall take place no later than 24 hours after detecting a personal data breach, if feasible. In the notification addressed to the competent national authority, the supplier includes the information specified in Annex I to Regulation 611/2013. It is considered that a personal data breach has been detected when the supplier has obtained sufficient knowledge of the occurrence of a breach of protection that led to a breach of personal data in order to provide a reasonable notification in accordance with the requirements of this notification.

In turn, Art. 174a sec. 3 of the Telecommunications Law, states that in the event that a personal data breach may have an adverse effect on the rights of a subscriber or end user who is a natural person, the provider of publicly available telecommunications services shall immediately notify the subscriber or end user of such a breach on the terms set out in Regulation 611/2013 , subject to sec. 5. Art. 3 s. 1, 3 and 4 of Regulation 611/2013, in turn, provides that if there is a likelihood that a personal data breach will adversely affect the personal data or privacy of the subscriber or individual, the provider, in addition to the notification referred to in art. 2, shall also notify this subscriber or natural person of the breach, and the notification of the subscriber or natural person shall take place without undue delay after detecting a personal data breach, as specified in Art. 2 sec. 2 third paragraph. The above is not dependent on the notification of a personal data breach addressed

to the competent national authority referred to in art. 2. In the notification addressed to the subscriber or natural person, the provider includes the information specified in Annex II to Regulation 611/2013. The notification addressed to the subscriber or individual is formulated in a clear and easily understandable manner, and the provider does not use the notification as an opportunity to promote or advertise new or additional services. Recital 12 of the preamble to Regulation 611/2013 explains that when assessing whether a personal data breach may have adverse effects on the personal data or privacy of a subscriber or individual, the nature and content of the personal data in question should be taken into account in particular, especially when the data concerns financial information, such as credit card and bank account information; special categories of data referred to in art. 8 sec. 1 of Directive 95/46/EC; and some data specifically related to the provision of telephone or Internet services, e.g. e-mail data, location data, Internet registry files, registers of searched websites and lists of telecommunications services performed. These issues are regulated more precisely in Art. 3 s. 2 of Regulation 611/2013, which will be quoted later in the justification for this decision.

In the case in question, there was a breach of personal data consisting in the Company's disclosure to a third party via e-mail of the subscriber's data contained in the Agreement. In such a situation, the provisions of art. 174a sec. 1 of the Telecommunications Law in connection with Art. 2 sec. 1 and 2 of Regulation 611/2013, according to which the Company should have notified the President of the Personal Data Protection Office of a personal data breach no later than 24 hours after its detection (it should be emphasized that in accordance with Article 2(1) of the above-mentioned regulation, the obligation to notify of the supervisory authority applies to each detected personal data breach).

Moreover, this breach (leading to accidental, unauthorized disclosure to a third party of personal data processed by the telecommunications undertaking in connection with the provision of publicly available telecommunications services) may have an adverse effect on the subscriber's rights, in particular it may result in unauthorized use of personal data, property damage , violation of personal rights - therefore, after detecting a violation, the Company should also notify the Client about it without undue delay, to enable him to take the necessary preventive measures to protect rights or freedoms against the negative effects of the violation (Article 174a section 3 of the Law telecommunications in connection with Article 3(1), (3) and (4) of Regulation 611/2013).

The above-mentioned provisions precisely indicate the date by which providers of publicly available telecommunications services (which is also the Company) are required to notify the competent national authority (President of the Personal Data

Protection Office) of a personal data breach (no later than 24 hours after its detection), and also indicate that the subscriber should be notified of the infringement without undue delay after its detection. The basic issue requiring clarification in the case in question is therefore when - in accordance with the principles of logic and the law - the Company should have detected the infringement.

As already indicated above, it is considered that a personal data breach has been detected when the supplier has obtained sufficient knowledge of the occurrence of a breach of protection that led to a breach of personal data in order to submit a notification in accordance with the requirements of the relevant regulations. In the case in question, the Company obtained information that, after analyzing it, would allow detecting a personal data breach twice:

1) for the first time, on [...] February 2022, when the Customer (J.G.) returned to the POS with information that the e-mail address provided by him during the process of signing the Agreement was incorrect and asked for its removal, which was by the Company noted in the application number xxxxxxxxx; analysis of the information obtained from the Customer about the wrong e-mail address in combination with the knowledge that providing the contact e-mail address by the person concluding the contract with the Company during the process of signing the contract with the printing of documents (to be signed) automatically generates copies of documents for shipment to the address provided, allowed the Company to detect the infringement;

2) for the second time, on [...] February 2022, when the Company received a request for clarification of [...] February 2022, in which the President of the UODO called on the Company to provide information on the data breach of February 2022 r., consisting in enabling an unauthorized third party to view a set of documents for order No. [xxxxxxxxxx] and present an assessment in terms of the obligation to report a breach to the supervisory authority and notify the data subject, which - especially in conjunction with the above-mentioned information previously obtained on this subject by the Company - should have resulted in the detection of the infringement.

In the opinion of the President of the UODO, obtaining on [...] February 2022 the information indicated in point 1 (i.e. about the e-mail address incorrectly indicated by the Customer together with the knowledge about the applicable procedure for sending documents in electronic form) was sufficient to detect a personal data breach (however, even if this moment is associated with the moment of obtaining the information indicated in the above-mentioned point 2, this does not have any effect on the need to impose a penalty in this case, as the duration of the infringement is long in each of these cases). Meanwhile, the Company

notified the President of the UODO of the personal data breach only on [...] April 2022 - after the initiation of administrative proceedings in the case in question (of which it was informed in the letter of [...] April 2022) and after inspecting the case files - its explanations contained in section 4A of the personal data breach notification form show that the violation was found on [...] April 2022: "[p]on obtaining additional information as a result of the review of the case files (in particular the content of the notification submitted to PUODO by a third party whom the Company did not know before) and re-analysis of the material collected in the case (...)". However, the analysis of the content of the letter sent by a third party to the President of the UODO allows us to conclude that it does not contain any additional information relevant to the possibility of detecting a personal data breach by the Company, which at that time already had the information referred to in points 1 and 2 above. In this letter (which was received in the form of an e-mail), the third party indicated that »Today I received an e-mail with the Play contract. I am not a Play customer, the contract concerns another person with the same name. The contract contains all the data of this person, including PESEL number and ID number. Worst of all, Play does not provide any simple way to report this fact - it sends a message from a no-reply address to which it is impossible to reply. And yet, in the footer, he places a "request" that "The accidental and/or mistaken recipient of this message immediately notify the sender" - even though it is physically impossible to reply to this email. In turn, the "warning" that the message may contain company secrets, without hesitation about the fact that it may also contain customer secrets, is simply embarrassing in the context of this situation.

An e-mail sent to this person from the Company is also attached to the above.

After obtaining the information referred to in point 1 above, the company did not conduct an analysis that would result in the correct result, i.e. detection of a personal data breach. It also failed to do so after obtaining the information referred to in the above-mentioned point 2. As a result of these omissions, the Administrator not only failed to notify the President of the UODO of the personal data breach within the time limit resulting from Art. 2 sec. 2 of Regulation 611/2013, but also failed to meet the obligation to notify the Customer of the breach without undue delay to enable him to take the necessary preventive measures to protect rights or freedoms against the negative effects of the breach (Article 174a(3) of the Telecommunications Law in conjunction with Art. 3 sections 1, 3 and 4 of Regulation 611/2013), despite the fact that in the case in question there is a likelihood that a personal data breach will have adverse effects on the subscriber's personal data or privacy. This probability (pursuant to Article 3(2) of Regulation 611/2013) is assessed taking into account, in particular, the following circumstances:

a) the nature and content of the relevant personal data, in particular if these 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, records of searched websites and lists of telecommunications services performed; b) the likely consequences of a personal data breach for a given subscriber or individual, in particular if the breach could result in identity theft or fraud, bodily harm, mental distress, humiliation or reputational damage; andc) the circumstances in which the personal data breach occurred, in particular, where the data was stolen and when the provider learned that the data is in the possession of an unauthorized third party.

In the case in question, the breach concerned the Customer's personal data contained in the Agreement, i.e. his: name and surname, address of residence or stay, PESEL registration number, series and number of the ID card, as well as telephone number. It should be emphasized that, in particular, unauthorized disclosure of such a category of data as the PESEL number (in combination with the name and surname) may have a real and negative impact on the protection of the rights or freedoms of natural persons (vide: https://www.bik.pl/poradnik- bik/wyluwiedz-loan-tak-dzialaja-szusci - where a case was described in which: "Only the name, surname and PESEL number were enough for fraudsters to extort several loans in total for tens of thousands of zlotys. Nothing else matched: neither the ID number personal or residential address"). The PESEL number, i.e. an eleven-digit numerical symbol that uniquely identifies a natural person, containing the date of birth, serial number, gender designation (and control number), and thus closely related to the private sphere of a natural person, is data of a special nature and requires special protection. Not without significance for assessing the likelihood that a personal data breach will have adverse effects on the subscriber's personal data or privacy is also the possibility of easy (based on the disclosed data) identification of the person whose data was affected by the breach. Disclosure of the Customer's data in the above-mentioned scope may, in the opinion of the President of the UODO, result in some of the consequences indicated in point b) above (e.g. identity theft or reputational damage). However, when assessing the circumstances indicated in point c) above, it should only be additionally noted that a personal data breach may also take place when the Administrator is not at fault for its causes (e.g. in a situation of an error made by the data subject).

Pursuant to Art. 3 section 6, first sentence of Regulation 611/2013, the provider shall notify the subscriber or natural person of a personal data breach, using means of communication that ensure quick access to information and are properly secured. The administrator should fulfill this obligation without undue delay (Article 3(3) of the above-mentioned regulation) - meanwhile, the Company informed the subscriber only on [...] April 2022. The purpose of this provision is to enable the data subject to take adequate steps to in order to protect its interests (which the Company as the administrator should enable its Client, even if it is

not at fault for the personal data breach).

Considering the importance of the fact that the personal data breach occurred as a result of the Customer's error (who provided an incorrect e-mail address at the POS point), for assessing whether, in this case, the Administrator should have fulfilled the obligation to notify the President of the UODO of this breach and also notify about it the Customer, it must not be forgotten that the effect of sending an e-mail to this incorrectly provided address is to make a wide range of the Customer's personal data available to a third party (breach of data confidentiality). It is pointless here that the Company refers in the letter of [...] March 2022 to a fragment of the decision issued by the President of the UODO (quote): »The Company shares the position of PUODO expressed in the decision regarding the case ZSPR.440.1090.2019 "[...] Each the person may freely indicate his e-mail address, because he bears the consequences of not collecting correspondence sent to this address. The company is unable to verify the authenticity of the data regarding the e-mail address provided by the customer and by directing correspondence to an e-mail address other than the one indicated by the interested person, it would fail to exercise due diligence in contacts with this person, which would make it impossible to effectively deliver correspondence to it via this channel contact.[…]”«. Firstly, the fact is that the Administrator, having not obtained knowledge that the e-mail address provided by the customer is incorrect, has no reason not to send correspondence to this address. However, if the Company finds out that the address provided by the client, to which the document containing personal data was sent, may be incorrect, it should perform an appropriate analysis to detect a personal data breach. It should also be emphasized that in this case, the fact that the Customer's data contained in the Agreement was made available to an unauthorized person is indisputable. The fact that the e-mail address was incorrectly provided by the Customer himself does not eliminate the effects of incorrect sending of the message, i.e. the occurrence of a personal data breach. Therefore, the company should have reported the breach to the President of the UODO no later than 24 hours after its discovery, and the Client should have been notified of it without undue delay, as there was a likelihood that it would have adverse effects on the personal data or privacy of the Client. In addition, it should only be noted that in the above context, the Company's argumentation contained in the above-mentioned in writing that: "[...] until [...] March 2022, it did not receive information from the Customer about the incorrect shipment and thus the disclosure of his personal data to an unauthorized person. The company also did not record a signal from a third party about possible unauthorized access to the Customer's personal data as a result of incorrect sending. In connection with the above, the Company has no grounds to treat the event in question as a violation of (...) personal data." Referring to the

argument regarding the lack of information from an unauthorized recipient, it should only be pointed out that the Administrator, by sending an electronic message to an unauthorized person, a contract for the provision of the Customer's telecommunications services, did not indicate to that person the appropriate procedures to inform the Company about the event. The third party indicated to the President of the UODO in the message of [...] February 2022 that: »Worst of all, Play does not provide any simple way to report this fact - it sends a message from a no-reply address to which it is impossible to reply. And yet, in the footer, he puts a "request" that "The accidental and/or mistaken recipient of this message should immediately notify the sender" - even though it is physically impossible to reply to this email". In addition, the Company posted information in an electronic message to an unauthorized person that: "The accidental and/or mistaken recipient of this message is asked to immediately notify the sender and remove it from the system". These circumstances indicate the need for the Company to introduce appropriate organizational or technical changes that would enable notifications by accidental recipients of messages sent by the Administrator. This would increase the chances of detecting personal data breaches and meeting the obligations related to them by the Company.

As it is not possible to eliminate the risk, in a situation where persons concluding contracts for the provision of telecommunications services with the Administrator provide an incorrect e-mail address (a risk of which the Company should be aware by allowing the possibility of using e-mail for communication with the client), it would be justified for the Company to introduce additional technical and organizational measures to reduce or eliminate the risk of personal data breach in the event of sending documents to such an address (e.g. securing the sent file with an access password provided to the client via another communication channel, or introducing double verification of the e-mail address). This necessity (and the fact that the measures used so far did not work properly) also seems to be noticed by the Company, which in box 9B of the personal data breach notification form indicated as security measures applied or proposed to minimize the risk of recurrence of the breach: "Verification and possible modification of the mechanism and rules for sending e-mails containing documents with customer data." The current method of processing personal data by the Company to the extent to which the breach occurred generates the risk of recurrence of such breaches.

The company has repeatedly informed the President of the Personal Data Protection Office that it attaches great importance to the diligent implementation of the regulatory obligation, which is the notification of personal data breaches. It introduced new technical and organizational measures, i.e. it started sending notifications of violations to the President of the UODO in

electronic form, via the ePUAP platform (a tool that enabled quick reporting of a violation to the supervisory authority). In this case, however, it failed to meet its obligations related to notifying the supervisory authority of a breach and notifying the Client of it within the deadlines resulting from the relevant provisions. Considering the scale of breaches reported by the Company, awareness of the importance of personal data protection should grow - a process that requires commitment, time, people's work and dedicated resources.

Summarizing the findings made in this case by the President of the UODO, it should be stated that the Company did not notify the President of the UODO of the personal data breach within the time limit specified in art. 174a sec. 1 of the Telecommunications Law in connection with Art. 2 sec. 1 and 2 of Regulation 611/2013, and also failed to notify the subscriber of the breach without undue delay after its detection, pursuant to Art. 174a sec. 3 of the Telecommunications Law in connection with Art. 3 section 1, 3 and 4 of Regulation 611/2013. The overriding purpose of each notification of the supervisory authority about a breach is to protect the rights or freedoms of natural persons - meanwhile, the Administrator, after obtaining information that the Customer provided an incorrect e-mail address and after receiving a request for explanations addressed to him on [...] February 2022. by the President of the UODO, did not notify the breach to the supervisory authority and did not inform the data subject about it (within the appropriate deadlines). Thus, in practice, he deprived this person, provided without undue delay, of reliable information about the infringement and the possibility of counteracting its potential effects.

By making the above summing up, it should also be noted that the violation also involves a violation of the protection of fundamental rights and freedoms, in particular the right to privacy and confidentiality, with regard to the processing of personal data in the electronic communications sector, which clearly increases the seriousness of the violation and justifies its more severe punishment.

Pursuant to Art. 210a sec. 1 point 2 and 3 of the Telecommunications Law, who does not fulfill the information obligation: towards the President of the UODO, referred to in art. 174a sec. 1 or to the subscriber or end user referred to in Art. 174a sec. 3, is subject to a fine imposed by the President of the UODO in the amount of up to 3% of the revenue of the punished entity achieved in the previous calendar year. Pursuant to art. 210a sec. 2 of the Telecommunications Law, to penalties imposed on the basis of sec. 1 of this provision, the provisions of Art. 209 sec. 1a-3 and art. 210 of the Telecommunications Law. The powers of the President of UKE set out in these provisions are vested in the President of the UODO. However, pursuant to art. 209 sec. 1a of the Telecommunications Law, applied pursuant to art. 210a sec. 2 of this Act to fines imposed by the President

of the UODO, the penalty referred to in sec. 1 and 11 of this provision, may also be imposed in the event that the entity ceased infringing the law or repaired the damage caused, if the President of UKE (and in the case of personal data breaches - the President of the UODO) decides that the duration, scope or effects of the infringement speak for it. In this case, the Company, by notifying the President of the UODO on [...] April 2022 of a breach of the Customer's personal data and fulfilling the information obligation towards the Customer on the same day, undoubtedly ceased violating the law. It removed the state of infringement consisting in not notifying the President of the UODO - within 24 hours after detecting the infringement - and the Customer - immediately after detecting it - about the breach of the Customer's personal data. However, the scope of the infringement, its duration and its effects justify - in the opinion of the President of the UODO - the need to impose a fine on the Company, which is to fulfill a repressive, preventive and disciplining function for the Company to comply with the law on the protection of personal data, and in in relation to other entities, also a preventive function - consisting in discouraging them from committing such violations in the future.

Referring to the duration of the infringement, its scope and effects justifying the need to impose a fine on the Company in this case, which are referred to in Art. 209 sec. 1a of the Telecommunications Law, the President of the UODO states as follows: Duration of the infringement. In the opinion of the President of the UODO, the necessity to impose a fine on the Company in this case is justified by the duration of the infringement. According to the President of the UODO, already on [...] February 2022, i.e. on the date of obtaining information from the Customer about the incorrectly indicated e-mail address, the Company detected (or at least should have detected, assuming the appropriate level of diligence required for activities inextricably linked with the processing of personal data and in conjunction with the knowledge of the applicable procedure for sending documents confirming the conclusion of the contract to the e-mail address indicated by the customer) violation of the Customer's personal data. Between the date of detection of the breach ([...] February 2022) and the date of notification to both the President of the UODO and the client about the breach of personal data ([...] April 2022) almost two months passed, during which unlawful use of data was possible the Client's personal data for purposes violating his rights and interests. Even assuming that the Company detected a breach of its Client's personal data only on [...] February, that is on the date of receipt of the request of the President of the UODO to provide information on the breach of personal data being the subject of this case, this period is - in the opinion of the President of the UODO - also long - sufficient for the unlawful use of the Customer's personal data. During this period, the Customer was unable, without knowing about the breach of his personal data, to take any steps to protect his

rights and interests. Also, the President of the UODO could not take any action during this period and for the same purpose. In the opinion of the President of the UODO, it is also worth emphasizing that the notification of the President of the UODO and the Customer himself about the breach of the protection of his data took place not as a result of the proper operation of the procedures in force in the Company, but only as a result of the President of the UODO initiating proceedings in this case and after receiving request of the President of the UODO of February [...] 2022 to provide explanations in the case.

Scope of the infringement. The President of the UODO was not informed on time in accordance with the procedure provided for in art. 174a sec. 1 of the Telecommunications Law in connection with joke. 2 sec. 1 and 2 of Regulation 611/2013. The fact that the Administrator did not notify the President of the Personal Data Protection Office in a timely manner of a personal data breach despite the existence of such an obligation - in the event of obtaining information twice allowing to detect a personal data breach - should be considered an aggravating circumstance (especially since the Company already has as of […] February 2022 the information was sufficient to detect a personal data breach).

The administrator should always exercise due diligence when processing the personal data of its subscribers (especially due to the need to protect telecommunications secrecy). Their disclosure in such a wide scope as in the case in question is additionally associated with the probability that this breach will have adverse effects on the subscriber's personal data or privacy - as it carries a potential risk of using these data by unauthorized persons, as a result of which these persons may act to the material and non-material damage of the person to whom the data subject to the breach relate.

As a result of incorrectly conducted explanatory activities, as a result of which the Company did not classify the event as a personal data breach, initially not only was the President of the Personal Data Protection Office not notified of the personal data breach, but also the subscriber was not notified of it. This happened - as it should be repeated: despite the Administrator receiving information twice, which should have contributed to the analysis of the event in question (including the likelihood that it will cause adverse effects on the personal data or privacy of the Customer).

Personal data accessed by a third party and to which the personal data breach reported by the Administrator on [...] April 2022 concerned has a wide scope (name and surname, address of residence or residence, PESEL registration number, ID card series and number personal and phone number). In this situation, it is likely that a personal data breach may have adverse effects on the subscriber's personal data or privacy - their disclosure may result in, for example, theft or falsification of identity or damage to reputation (referred to in Article 3(2)(b) of the Regulation 611/2013). Therefore, the company should have

notified the client of a breach of confidentiality of his personal data without undue delay after detecting a breach of personal data (Article 3(1) and (3) of Regulation 611/2013).

The obligation to notify the subscriber of a personal data breach is independent of the obligation to notify the President of the UODO, and joint failure to meet both of these obligations must be assessed more strictly.

According to the well-established position of the doctrine developed on the basis of 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 elements of harmfulness of an objective nature. They concern the type of infringed obligations, the type of infringed goods, the intensity of the infringement and social and economic values, the consequences of the act covered by the financial penalty, the amount of damage caused, the method of operation" (S. Piątek, Telecommunications Law. Commentary, Commentary on Art. 210 section 2, Warsaw 2019, 4th edition, Legalis). The basic objectives of the Act mentioned above include providing users with maximum benefits in terms of variety, price and quality of telecommunications services (Article 1(2)(4) of the Telecommunications Law). In the opinion of the President of the UODO, the phrase "maximum benefits in terms of [...] the quality of telecommunications services" includes 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 confirms the formulation of one of the objectives of the regulatory policy pursued by the authorities competent in telecommunications matters, which is to contribute to ensuring a high level of personal data protection (Article 189(2)(3)(c) of the Telecommunications Law).

In the present case, a violation of the provisions on the protection of personal data was found beyond any doubt - provisions protecting a good of high social value (constituting an element of the constitutional right to privacy) and economic (use of which may result in obtaining large financial benefits). The breach concerned the Company's obligation towards the President of the UODO, as well as towards the data subject. In the opinion of the President of the UODO, this breach reduces the high (optimal in certain circumstances) level of protection of personal data of the Administrator's clients. It delays the reaction of the President of the UODO to existing infringements, which may prevent, or at least limit, possible negative consequences for the data subject. Such a violation, which is not a one-time accident (as referred to below - in the point regarding the entity's activities to date), deserves a negative assessment, which is reflected in the imposition of a fine on the Company in this case.

Consequences of the breach. In this case, the President of the UODO did not find any material damage on the part of the

Client as a result of the breach of his personal data. However, it should be emphasized that the consequence of this breach was that the Client was deprived of the possibility to react to the breach of his personal data, and the President of the UODO - the possibility of taking action to remove this breach and its possible negative consequences. The almost two-month delay in the performance of the information obligations imposed on the Company created - regardless of whether this was the case in this case - the risk of unauthorized use of the Customer's personal data, the use of which the Customer could not prevent or adequately react to. Such a loss of control by the Customer over his personal data, which the Company could have prevented by fulfilling the obligations in the field of personal data protection specified in the Telecommunications Law in due time, is undoubtedly in contradiction with the above-mentioned purpose of this act, which is, among others, "providing users with maximum benefit in terms of [...] the quality of telecommunications services". For this reason, the effects of the breach speak for a negative assessment of the Company's actions taken in response to the breach of the Customer's personal data. This assessment is reflected in the sanction in the form of a fine imposed by this decision.

Summarizing the considerations regarding the application of the provision of art. 209 sec. 1a of the Telecommunications Law, it should be stated that in this case there were premises justifying the need to impose a fine on the Company for breach of information obligations towards the President of the UODO (Article 210a section 1 point 2 of the Telecommunications Law) and towards the Customer (Article 210a section 1 point 1 point 3 of the Telecommunications Law). Despite the Company's cessation of infringing the law, in the opinion of the President of the UODO, both the duration of the infringement and its scope and effects speak in favor of it. However, when determining the amount of the fine imposed in this case, the President of the UODO took into account - in accordance with the requirement set out in Art. 210 sec. 2 of the Telecommunications Law applied pursuant to Art. 210a sec. 2 of this Act to fines imposed by the President of the UODO - the scope of the infringement, the Company's current operations and its financial capabilities.

The scope of the infringement. Due to the fact that the scope of the infringement is both a premise justifying the need to impose a fine in the case, and a circumstance affecting its amount, reference should be made here to the above-presented assessment of this circumstance as a premise justifying the need to impose a fine on the Company . This assessment is also the basis for determining the amount of the fine imposed on the Company by the President of the Personal Data Protection Office - it is an aggravating circumstance affecting its amount. At this point, it should only be stated that the President of the UODO also notes the circumstances mitigating the amount of the fine imposed, namely:

a) unintentional infringement: the delay in the procedure of notifying the President of the UODO and the subscriber of a personal data breach is not due to the Company's intention not to comply with the deadline, but to the improper organization of the procedure in this respect, b) the fact that during these proceedings imposition of a fine on the Company, the Company notified the President of the Personal Data Protection Office of the breach of personal data and notified the subscriber of it (albeit with a delay), c) the breach of personal data concerned only one person who incorrectly provided his e-mail address, to which he was then sent data (of which the Company did not notify either this person or the supervisory authority on time).
The circumstances presented above have a mitigating effect on the fine imposed on the Company; however, they do not justify a departure from its ruling. The scope of the infringement, i.e. all the circumstances considered by the President of the UODO related to the breach by the Company of its disclosure obligations, speaks in favor of imposing a fine on the Company in this case and justifies its amount, which, in the opinion of the President of the UODO, is adequate to the infringement found.
The entity's activity to date. It should be emphasized here that the President of the UODO has already conducted administrative proceedings against the Company (described further in this point) regarding failure to notify the supervisory authority of personal data breaches within 24 hours of their detection (in connection with which the Company introduced changes in the method of sending notifications). The infringement in question, which is not a one-off incident as indicated, deserves a negative assessment, which is reflected in the imposition of a penalty on the Company in this case.
The premise of the "previous activity" of the entity subject to the penalty affecting the penalty is a directive aimed at individualizing the penalty due to the assessment of the activity of this entity in the past, which is in particular to indicate whether the violation is an incidental event and not resulting from the policy of this entity (which would not involve a large risk for a large number of the Company's customers - so it would not have to be an aggravating circumstance for the Company), or whether 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 calculated in its profit account and losses (which should be considered an aggravating circumstance). The assessment of the entity's activities to date covers a wide range of detailed circumstances, such as: the entity's performance of statutory obligations, violations of the law committed by it, previously imposed penalties or other administrative sanctions, or cooperation with the President of the UODO in the performance of its tasks.
The notification of a personal data breach considered under these administrative proceedings after 24 hours of its detection (i.e. without meeting the deadline specified in Article 2(2) of Regulation 611/2013) was not the first such case in the

Administrator's previous activity, which results from decision of the President of the UODO issued on June 8, 2021 in case DKN.5131.10.2020 (on the violation of Article 174a(1) of the Telecommunications Law in connection with Article 2(2) of Regulation 611/2013, consisting in not notifying the President UODO about personal data breaches within 24 hours of detecting a personal data breach). Despite the President of the UODO sending correspondence to the Company in this case on [...] February 2022, the Administrator notified the supervisory authority of the personal data breach and notified the Client about it only as a result of decisive (treated by the President of the UODO as last resort) action, then is to initiate proceedings to impose a fine on him for the infringement. The above-described operation of the Company (processing personal data in a professional manner and on a massive scale due to the subject of its business activity) is, in the opinion of the President of the UODO, reprehensible and evidence of disregarding the obligations in the field of personal data protection under the provisions of the Telecommunications Law.

The financial capabilities of the Company. The financial statements provided by the Company as at and for the year ended [...] December 2021 show that in 2021 the Company's operating revenues amounted to PLN 7,175,794,000, while its net profit: PLN 5,832,139,000 . The achievement by the Company in only one financial year of the net profit in the above-mentioned amount proves the Company's very high financial capabilities, for which the fine imposed by this decision in the amount of PLN 250,000 will be - in the opinion of the President of the UODO - small, although adequate to the seriousness of the violation found, financial burden (this amount is only 0.0035% of the above-mentioned operating revenues of the Company and 0.0043% of its net profit, while the maximum amount of a possible fine would be PLN 215,273,820 in this case).

Taking into account all the circumstances discussed above, the President of the UODO decided that imposing a fine on the Company is necessary and justified by the Company's violation of the provisions of art. 174a sec. 1 and 3 of the Telecommunications Law in connection with joke. 2 sec. 1 and 2 and art. 3 section 1, 3 and 4 of Regulation 611/2013.

The President of the UODO, after 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 sec. 1 of the Telecommunications Law, determined the amount of the fine imposed on the Company in the amount of PLN 250,000. It should be emphasized that the fixed amount of the fine, taking into account the Company's revenues, is within the limit of 3% of the revenue of the fined entity achieved in the previous calendar year, indicated in the above-mentioned the provisions of the Telecommunications Law. In the opinion of the President of the UODO, the amount of the fine imposed corresponds to the Company's financial capabilities and the scope of

the violation of the law. When imposing the above fine, the President of the Personal Data Protection Office took into account the Company's previous activity. 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 (it is to prevent similar violations in the future) and disciplinary for providers of publicly available telecommunications services (to discourage them from breaking the law. The penalty is, on the one hand, an affliction for the punished entity, and on the other hand, it is to refer to its financial capabilities. These conditions were met when imposing a penalty in the amount specified in this decision (see: judgment of the Court of Appeal in Warsaw of March 3, 2016, reference number: VI ACa 43/15, from which the thesis shows that penalties imposed on the basis of art. 209 and 210 of the Telecommunications Law should be both repressive and preventive in nature, as they should contribute to ensuring a permanent cessation in the future of violating the obligations imposed on the entrepreneur, and in order to effectively prevent attempts to appear in the future of behaviors contrary to the Act, they must be set at the level felt by the each of the entrepreneurs).

It should be emphasized that the penalty will be effective if its imposition leads to the fact that the Company, which processes personal data professionally and on a massive scale, will fulfill its obligations in the field of personal data protection in the future, in particular as regards timely notification of data breaches personal data of the President of the UODO and notifying subscribers about them.

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

Print article

Metadata

Provider:

Inspection and Infringement Department

Produced information:

Wioletta Golanska

2022-11-03

Entered the information:

Edith Magziar

2023-01-09 13:01:15

Recently modified:

Edith Magziar

2023-01-09 13:55:34