THE CHAIRMAN OF PERSONAL DATA PROTECTION

Warsaw, on 03

of December

2020

DECISION

DKN.5112.1.2020

Based on Article. 104 § 1 of the Act of 14 June 1960 Code of Administrative Procedure (Journal of Laws of 2020, item 256), art. 7 sec. 1, art. 60 and art. 101 of the Act of 10 May 2018 on the protection of personal data (Journal of Laws of 2019, item 1781) and art. 57 sec. 1 lit. a, art. 58 sec. 2 lit. i, with art. 83 sec. 3, art. 83 sec. 4 lit. a, art. 83 sec. 5 lit. and in connection with art. 5 sec. 1 lit. f, art. 5 sec. 2, art. 24 sec. 1, art. 25 sec. 1 and art. 32 sec. 1 lit. b and lit. d and art. 32 sec. 2 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46 / EC (general regulation on the protection of data) (Journal of Laws UE L 119 of 4 May 2016, p. 1, as amended), after administrative proceedings regarding the processing of personal data by Virgin Mobile Polska Sp. z o.o. based in Warsaw, President of the Personal Data Protection Office

finding an infringement by Virgin Mobile Polska Sp. z o.o. based in Warsaw, the provisions of art. 5 sec. 1 lit. f, art. 5 sec. 2, art. 25 sec. 1, art. 32 sec. 1 lit. b and lit. d and art. 32 sec. 2 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46 / EC (general regulation on the protection of data) (Journal of Laws UE L 119 of 4 May 2016, p. 1 as amended), consisting in failure to implement by Virgin Mobile Polska Sp. z o.o. with its registered office in Warsaw, appropriate technical and organizational measures ensuring a level of security corresponding to the risk of data processing using IT systems used to register personal data of subscribers of pre-paid services, which led to an unauthorized person obtaining access to this data, imposes on Virgin Mobile Polska Sp. z o.o. with its registered office in Warsaw, an administrative fine in the amount of PLN 1,968,524.00 (in words: one million nine hundred sixty eight thousand five hundred and twenty four zlotys).

JUSTIFICATION

The Office for Personal Data Protection [...] on December 2019 received a notification of a personal data breach submitted by Virgin Mobile Polska Sp. z o.o. (hereinafter: the Company), registered under the number DKN.405.499.2019, informing about a breach of personal data protection of subscribers of prepaid services, consisting in obtaining by an unauthorized person access to this data and obtaining 142 222 records of pre-paid service registration confirmations containing data personal details of 114 963 clients in terms of name and surname, PESEL registration number, series and number of ID card, telephone number, tax identification number and the name of the entity. The incident which was the subject of the report took place in the period from [...] to [...] December 2019. Due to the scope of personal data disclosed, the indicated breach resulted in a high risk of violating the rights and freedoms of natural persons.

In connection with the reported breach, the President of the Office for Personal Data Protection (hereinafter also the President of the Office) decided to conduct an audit of the compliance of personal data processing with the provisions on the protection of personal data, i.e. with the Regulation of the European Parliament and of the Council (EU) 2016/679 of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46 / EC (General Data Protection Regulation) (Journal of Laws UE L 119 of 4 May 2016, p. 1, as amended), hereinafter referred to as Regulation 2016/679 or GDPR, and the Act of May 10, 2018 on the protection of personal data (Journal of Laws of 2019, item 1781). The scope of the inspection covered the method of processing, including the method of securing data, as part of the provision of telecommunications services to subscribers of prepaid services. In the course of the inspection (reference number [...]), oral explanations were received from the Company's employees and system A, used to register personal data of subscribers of prepaid services, was inspected. The facts are described in detail in the inspection report signed by the Management Board of Virgin Mobile Polska Sp. z o.o.

Based on the information and evidence collected in the control proceedings, it was found that in the process of processing the data of pre-paid subscribers, the Company, as the controller, breached the provisions on the protection of personal data. These shortcomings consisted in a breach of the principle of data confidentiality expressed in Art. 5 sec. 1 lit. f of Regulation 2016/679 and the obligations that reflect this principle, set out in art. 24 sec. 1, art. 25 sec. 1, art. 32 sec. 1 lit. b and lit. d and art. 32 sec. 2 of Regulation 2016/679 by failure to implement appropriate technical and organizational measures ensuring a level of security corresponding to the risk of data processing using IT systems used to register personal data of subscribers of prepaid services.

During the inspection it was found that:

1) The subject of the Company's activity is the provision of wireless telecommunications services.

2) The legal basis and the purpose of the processing of personal data in the Company in the process of registration of prepaid services is the performance of a telecommunications service contract concluded by performing a factual action, i.e. sending an SMS, MMS, downloading data or initiating a telephone connection, based on the Act of July 16 2014. Telecommunications law (Journal of Laws of 2019, item 2460).

3) The obligation to obtain personal data for a pre-paid service (registration of prepaid cards) was introduced in Art. 60b paragraph. 2 in connection with from paragraph 1 of the Telecommunications Law of July 16, 2004 (Journal of Laws of 2019, item 2460, as amended), which entered into force on July 25, 2016. For pre-paid subscribers who concluded an agreement before the date of entry into force the implementation of the Act of June 10, 2016 on anti-terrorist activities (Journal of Laws of 2016, item 904), i.e. before July 2, 2016, the obligation of the subscriber to provide the service provider with his personal data was introduced by Art. 60 of the same act.

4) The scope of personal data processed in connection with the registration of the pre-paid service in the case of a subscriber who is not a natural person, includes data in the form of the entity's name, tax identification number, telephone number, and if the proxy is registered, the proxy's personal data are also obtained in terms of name and surname and number PESEL number or series and number of the identity document. When registering a prepaid card by a natural person, the first and last name, PESEL number, ID card number or other identity document number and telephone number are obtained. In addition, personal data in the form of e-mail addresses and telephone numbers are collected for contact purposes.

5) Collecting the above-mentioned data takes place at the stage of card registration using the point of sale (points of sale, hereinafter referred to as "POS") - carried out by external entities with which the Company has signed cooperation agreements, also specifying the rules for entrusting the processing of personal data. Application A has been developed by the Company for entities that do not have their own software solutions to provide the service of registering prepaid cards. It is used to register these cards.

6) The process of data registration via POS takes place through the A application available from the public network via a web browser. Personal data for this application are entered by POS on the basis of the presented identity document.

7) Application A allows you to generate a printout of the registration confirmation. The solutions adopted for entities using their

own IT systems for the registration of prepaid cards, e.g. cash register systems or terminals, do not allow for printing the confirmation of the card registration.

8) The central system used in the Company is the IT system called B, which is connected with application A for the registration of prepaid cards.

9) The creator of the B system is T. Sp. z o.o. s.k.a. based in W. Ww. the company also dealt with the maintenance of the B system from [...] April 2014 to [...] June 2017. The operation and maintenance of the B system from [...] July 2017 until now the employees of A. S.A. on the basis of a framework agreement.

10) Basic personal data are stored in one central table of the database of system B based on a database engine [...], which receives registration data entered by POS using A and data from the systems of wholesale customers, i.e. without access to A and using their IT systems.

11) The producer of A is W. J. M. P. S. s.c. based in W. She developed the above-mentioned the application, which started operating from [...] September 2014. Until now, W. J. M. P. S. s.c. is also responsible for the service, development and supervision of the A application. A is an application for entering data into system B through the use of a web interface [...]. Originally, T. was responsible for maintaining the web-service enabling the exchange of information between application A and the central system B (from [...] April 2014 to [...] June 2017). From [...] July 2017 until now, the maintenance of the web service enabling the exchange of information between the application and the central system B and the maintenance of the system is provided by A. S.A. based in K.

12) During the inspection, it was found that from [...] to [...] December 2019, an incident of personal data leakage occurred in the Company as a result of obtaining unauthorized access to the data of pre-paid subscribers by exploiting the vulnerability of the IT system, ie a service that generates confirmation of registration of prepaid cards. The identified vulnerability of the service generating the registration confirmation consisted in the lack of verification [...]. Correct verification was to consist in generating a registration confirmation only when [...]. System B did not verify [...].

13) Technical and organizational measures applied in the Company from [...] May 2018 (the date of application of Regulation 2016/679), i.e. before the infringement occurred, were reviewed and updated as necessary in the event of organizational or legal changes (a copy of the e-mail informing about the need to review the applied monitoring together with the questionnaire).

14) The Company has not carried out comprehensive, regular testing, measurement and evaluation of the effectiveness of

technical and organizational measures to ensure the security of processing. In situations where there was a suspicion of a vulnerability, work was carried out to protect against a given vulnerability (printouts from the C system confirming the remedial actions taken regarding confirmed suspicions about the vulnerability of the system). The above is also confirmed by, inter alia, in explanations submitted by an inspected entity in a letter of [...] March 2020 and in printouts of screen shots from system C sent for evidence purposes, indicating the performance of tests on [...] vulnerability and verification of the entered data.

15) The Company did not conduct tests aimed at verifying the security of application A and [...] system B concerning the IT system's vulnerability related to the personal data breach that has occurred. Such actions were taken only after the incident on [...] December 2019.

16) In the documentation kept by the Company describing the data processing process and the organizational and technical measures applied, obtained in the course of performing control activities, i.e. "Virgin Mobile Personal Data Processing Policy", "[...] Procedure [...]", "[...] Plan [...]", the issues related to regular testing, measuring and evaluating the effectiveness of measures have not been regulated technical and organizational to ensure the security of processing.

17) The company undertook corrective actions and eliminated the vulnerability of the IT system by modernizing it, consisting in correlation [...]. Currently [...]. It introduced a restriction [...]. When there is a need to regenerate the application, it is possible [...].

In connection with the above, in a letter of [...] June 2020 (letter reference [...]), the President of the Office for Personal Data Protection notified the Company about the initiation of ex officio administrative proceedings regarding violation of the provisions on the protection of personal data with respect to them implementation of appropriate technical and organizational measures ensuring the level of security corresponding to the risk. In the course of these proceedings, the President of the Office for Personal Data Protection established the facts of the case in accordance with the findings of the control No. [...] (points 1-17 above). The President of the Office also obtained additional explanations of the Company (submitted by the Company's attorney in letters of [...] July 2020 and [...] August 2020), in which it was indicated, inter alia, that:

1) From the beginning of its operation, the Company offered prepaid services in a model that did not require providing personal data. The requirement to provide data was introduced by the Act of June 10, 2016 on anti-terrorist activities (i.e. Journal of Laws of 2019, item 796). For the entry into force of the provision of Art. 43 above of the act specifying the scope of collected data, the legislator set a 30-day period. As the representative pointed out, a month to implement such large changes is

definitely too short a time to implement and test any IT system on such a scale. The deadline imposed by the legislator increased the risk of errors and shortcomings.

2) At this stage of the proceedings, it has not been established who the attacker was. The way the vulnerability was exploited indicated that the attacker had previously accessed the system and knew [...]. At present, the Company does not know if and with what rights the attacker could have had, and to what period this right could apply. In the opinion of the Company, it is up to the President of the Office to prove whether the data has been disclosed to an unauthorized person.

3) The investigation into unauthorized access conducted by the District Prosecutor's Office in W. was discontinued by the decision of [...] July 2020 due to the failure to identify the perpetrator. Therefore, the company does not know whether the vulnerability was used to disclose personal data to an unauthorized person. This circumstance requires clarification by the authority in the course of the proceedings.

4) The Company, referring to the allegation of violation of Art. 25 sec. 1 GDPR points out that the provisions of the GDPR apply from [...] May 2018, when the changes required by the anti-terrorist activity act were introduced, the Company was not obliged to comply with the data protection principle at the design stage. However, at further stages of processing, this principle is essentially the same as the obligation to secure personal data pursuant to Art. 32 GDPR, as contained in art. 25 sec. 1 GDPR, the principle of data minimization does not apply in the present case due to the fact that the scope of personal data is defined by law.

5) The company, deciding to implement and use the B system, carried out numerous tests, measurements and assessments of whether it is appropriate to properly perform its functions, including securing subscribers' personal data entered into it. The risk to the rights and freedoms of data subjects was constantly assessed by the Company. Each time in the event of organizational or legal changes in the Company, technical and organizational measures were reviewed and updated.

6) In the Company's opinion, the manner of using the vulnerability indicates that the personal data of persons affected by the violation in question was not collected as a result of external bypassing the system. Using knowledge to break into a system is a risk that is more difficult to avoid than an external attack by compromising security.

7) According to the Company's assessment, the use of the system's vulnerability to the attack in question, resulting in gaining access to data, was not dependent on the lack of proper testing, measurement or evaluation of the system, as the indicated activities were regularly and properly carried out by the Company. This is confirmed by the printouts from the C system

concerning the vulnerability [...] and the verification of the entered data, which prove that although V did not carry out tests specifically related to the vulnerability used during the attack of [...] - [...] December 2019. , however, other tests [...] aimed at detecting vulnerabilities and improving data quality were conducted.

8) The Company does not agree with the allegation that regular testing, measurement and evaluation of the effectiveness of technical and organizational measures to ensure the security of processing were not carried out in the Company. The company carried out a wide range of activities aimed at verifying the correct functioning of the IT system, application A and [...] system B used to register prepaid cards. The company has conducted comprehensive technical and organizational security reviews several times, such as the November 2019 audit, contract review, certification audit, security and risk reviews and assessments with the participation of the management board, carried out in December 2019. These activities were continued in 2020 rm in. in connection with the implementation of ISO.

9) Before the breach, the Company adopted data protection measures in the form of: procedures specifying the risk analysis methodology, information security level classification procedure, information security policy, IT system management procedure with appendices: [...] Procedure [...], [...] Procedure [...], [...] Policy [...], [...] Procedure [...], [...] Procedure [...], [. ..] Procedure [...] and [...], as well as elements [...]: [...] Plan [...], [...] Plan [...], [...] Plan [...].

10) The company, in a letter of [...] August 2020, explained that the letter of [...] the scope of the data concerned by the breach in question was much narrower than that indicated in the content of the personal data breach notification of [...] December 2019, point 5. A breach of the full scope of personal data occurred only in 4,522 cases, i.e. it referred to names and surnames, PESEL number and the subscriber's document number. In the remaining scope, the infringement related to: names, surnames and PESEL number (108702 cases) or the subscriber's document number (10167 cases).

11) The Company submitted to the case file a copy of the ISO / IEC 27001: 2013 certificates obtained on [...]. 07.2020 certifying the implementation and maintenance of the information security management system by the Company in the field of services provided by the telecommunications operator and ISO / IEC 27701: 2019 certifying the implementation and maintenance by the Company of a personal data management system as an extension of ISO / IEC 27001: 2013 and ISO / IEC 27002: 2013 for privacy management in the field of services provided by a telecommunications operator.

12) In the explanations of [...] October 2020 (supplemented by a letter of [...] October 2020), the Company indicated that the requirements for maintaining the certificates of compliance of the management system in the Company with the implemented

standards mean in particular: verification of the (before receiving the certificate of a series of comprehensive security reviews and the functioning of the management system (personal data and information security), commitment (in the agreement with the institution issuing the certificate) at least once a year (in the coming years) to a similar comprehensive management review and to perform at least after one internal audit in the area of each standard, as well as covering the functioning of the information security and data protection management system in the Company by an annual audit of an independent institution issuing the certificate.

13) In accordance with the requirements of maintaining certificates of compliance with the implemented standards, the Company makes and documents successively measuring the effectiveness of technical and organizational measures to ensure the security of processing by: measuring the number of personal data processing processes (activities) with a full description in relation to all processing processes (activities) personal data (evidence: "[...]"), measurement of the number of IT systems processing personal data with a full description for all systems (evidence "[...]"), measurement of the number of processes for which risk analysis was carried out for the purposes of assessing the effects of processing on the protection of personal data (element of the assessment of the effects of processing on the protection of personal data), measurement of the number of identified security incidents (including personal data breaches) and measurement of the number of complaints of persons about the lack of appropriate safeguards applied), formal definition of the objectives set for before the Company in the area of personal data protection and information security (proof: [...] in force from [...] December 2019), preparation and implementation of the procedure for measuring these goals, tests of IT system vulnerability tests performed internally, penetration tests carried out in July 2020, made by an external company I. sp. z oo

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

Article 5 of Regulation 2016/679 indicates the rules for the processing of personal data that must be respected by all administrators, i.e. entities that independently or jointly with others determine the purposes and methods of personal data processing. Pursuant to Art. 5 sec. 1 lit. f of Regulation 2016/679, personal data must be processed in a manner that ensures adequate security of personal data, including protection against unauthorized or unlawful processing and accidental loss, destruction or damage, by appropriate technical or organizational measures. The principle of integrity and confidentiality referred to in this provision stipulates that data are processed in a manner that ensures appropriate security of personal data,

including protection against unauthorized or unlawful processing and accidental loss, destruction or damage, by appropriate technical or organizational measures. Data confidentiality is a property that ensures that data is not disclosed to unauthorized entities.

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

The provision of art. 24 sec. 1 specifies the basic and main obligations of the administrator, who is burdened with the implementation of appropriate technical and organizational measures to ensure the compliance of processing with the requirements of Regulation 2016/679. This is, in particular, about the implementation of the principles set out in Art. 5 sec. 1 of Regulation 2016/679.

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

Pursuant to Art. 32 sec. 1 lit. b of the Regulation 2016/679, taking into account the state of technical knowledge, the cost of implementation and the nature, scope, context and purposes of processing as well as the risk of violating the rights or freedoms of natural persons with different probabilities and severity, the controller and the processor implement appropriate technical and organizational measures to ensure the level of security corresponding to this risk, including, inter alia, the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services, as appropriate, and pursuant to Art. 32 sec. 1 lit. d of the regulation, regular testing, measurement and evaluation of the effectiveness of technical and organizational measures to ensure the security of processing.

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

The provision of art. 32 of the Regulation 2016/679 is therefore a specification of the provisions referred to in Art. 5 sec. 1 lit. f

of the Regulation 2016/679, the principles of integrity and confidentiality. On the other hand, Art. 5 sec. 2 of Regulation 2016/679 imposes an obligation on the data controller to demonstrate, in this case, that he has ensured adequate security of personal data, including protection against unauthorized or unlawful processing and accidental loss, destruction or damage, by appropriate technical or organizational measures.

The principle of confidentiality, the correct implementation of which ensures that the data is not made available to unauthorized persons, as it results from the established facts - was breached as a result of using the vulnerability of the IT system, which resulted in the acquisition of data of subscribers of prepaid services from the Company's database system and the implementation of the risk of violating rights and freedoms natural persons whose data is processed by the Company.

The President of the Personal Data Protection Office in the notification of the initiation of administrative proceedings indicated that the Company had not fulfilled the obligation under Art. 32 sec. 1 lit. b and lit. d of Regulation 2016/679, consisting in the selection of effective technical and organizational measures to ensure the security of the processed data, including the ability to continuously ensure confidentiality, integrity, availability and resilience of processing systems and services, as well as solutions ensuring regular testing, measurement and evaluation of the effectiveness of the measures adopted technical and organizational, which also breached the administrator's obligations to ensure and demonstrate compliance of the processing with the requirements of the regulation referred to in art. 24 sec. 1 and the obligation to effectively implement the data protection principles referred to in art. 25 sec. 1 of Regulation 2016/679, and consequently breached the principle of confidentiality set out in Art. 5 sec. 1 lit. f of the Regulation 2016/679 and the principle of accountability resulting from art. 5 sec. 2 of Regulation 2016/679.

It should be emphasized that the security measure adopted by the Company to ensure the resilience of IT systems, consisting in only [...] verification, which resulted in a breach of data confidentiality, cannot be considered a security measure referred to in the above-mentioned provisions of Regulation 2016 / 679. The breach of the protection of personal data of subscribers of prepaid services took place as a result of exploiting the vulnerability of the IT system [...] enabling unauthorized access to data. The identified vulnerability of the service [...] consisted in the lack of verification of all required parameters, ie [...]. Correct verification was to be based on [...] only if [...]. System B did not verify [...] or whether the claim was derived from this [...].

In response to the notification of the initiation of administrative proceedings, the Company indicated that before the infringement took place, it had adopted data protection measures in the form of procedures specifying the risk analysis

methodology, information security level classification procedures, information security policy, IT system management procedures with appendices: [...] Procedure [...], [...] Procedure [...], [...] Policy [...], [...] Procedure [...], [...] Procedure [...], [...] Procedure [...] and procedure [...], as well as elements [...]: [...] Plan [...], [...] Plan [...], [...] Plan [...].

In the opinion of the President of the Personal Data Protection Office, the measures adopted by the Company could be effective if, as part of the procedures implemented, they also contained regulations on regular testing, measuring and assessing the effectiveness of technical and organizational measures to ensure the security of processing and which would be complied with by the Company. Meanwhile, in the above-mentioned documentation describing the data processing process and the organizational and technical measures applied, obtained in the course of performing control activities, these issues have not been regulated.

As indicated by the Provincial Administrative Court in Warsaw in the judgment No. II SA / Wa 2826/19 of August 26, 2020 "This provision [Art. 32 GDPR] does not require the data controller to implement any technical and organizational measures that are to constitute personal data protection measures, but requires the implementation of adequate measures. Such adequacy should be assessed in terms of the manner and purpose for which personal data are processed, but also the risk related to the processing of such personal data, which may vary in size, should be taken into account. (...) The adopted measures are to be effective, in specific cases some measures will have to be low risk mitigating measures, others - high risk mitigating measures, but it is important that all measures (and each individually) are adequate and proportionate to the degree of risk ", which is shared by this authority.

In the opinion of the President of the Personal Data Protection Office, the lack of regulations in the procedures adopted by the Company ensuring regular testing, measurement and evaluation of the effectiveness of the technical and organizational measures used to ensure the security of data processing contributed to the occurrence of a personal data breach.

At the same time, the evidence collected in the course of the inspection shows that regular testing, measurement and evaluation of the effectiveness of technical and organizational measures to ensure the security of processing were not carried out in the Company. In situations where there was a suspicion of a vulnerability, only work was carried out to protect against a given vulnerability (printouts from the C system confirming the remedial actions taken regarding confirmed suspicions about the vulnerability of the system). The above is also confirmed by, inter alia, in explanations submitted by the inspected entity in a letter of [...] March 2020 and in printouts of screen shots from system C sent for evidence purposes, indicating the

performance of tests on [...] vulnerability and verification of the entered data. On the other hand, no tests were carried out to verify the security of application A and [...] system B regarding the IT system's vulnerability related to the personal data breach. Such actions were taken only after the incident of [...] December 2019. Technical and organizational measures applied in the Company from [...] May 2018 [...] until the violation occurred were reviewed and updated only in the event of organizational or legal changes (copy of the e-mail informing about the need to review monitoring used together with the questionnaire).

It should be noted that, as it results from the material collected in the course of the inspection, the creator of the B system was T. Sp. z o.o. ska, which also dealt with the maintenance of system B, as well as the maintenance [...] enabling the exchange of information between application A (developed by WJMPS sc and operating since [...] September 2014) and the central system B in the period from [...] ...] April 2014 to [...] June 2017 These functions were then taken over by ASA and has been doing them until now.

In the opinion of the President of the Office, the change of operator should entail a comprehensive assessment of the effectiveness of the implemented technical and organizational solutions to ensure the security of the processed data in the Company's IT systems. The evidence gathered in the course of the proceedings did not provide any evidence that such an assessment would be carried out in this situation. It should be emphasized that this change took place already during the period of application of Regulation 2016/679, in which the EU legislator gave data controllers a two-year period to adapt data processing to the requirements of the regulation.

In the explanations of [...] January 2020, the Company indicated that the last comprehensive review of technical and organizational measures was carried out in May 2018. As follows from the subsequent explanations of [...] July 2020, "The Company decides to for the implementation and use of the B system, it has carried out numerous tests, measurements and assessments of whether it is appropriate to properly fulfill its functions, including securing subscribers' personal data entered into it ". The Company further points out that “The risk to the rights and freedoms of data subjects was constantly assessed by the Company. Each time in the event of organizational or legal changes in the Company, technical and organizational measures were reviewed and updated. This proves that these activities were carried out in accordance with the individual needs of the Company. The company, while using the above-mentioned system, made every effort to ensure that the system fulfills its functions and properly protects the data entered into it. As indicated above, taking into account the state of technical knowledge that the Company had at the time of this event, the technical solutions adopted and used by it were of the highest

possible level ”.

The President of the Personal Data Protection Office cannot agree with this position, because to detect the vulnerability used, it would be enough to verify the basic principle of operation of system B, i.e. to check whether [...], while failure to take this action proves that the indicated by The company of reviews. Checking the correctness of [...] validation of the above-mentioned data does not require any specialist knowledge or large financial outlays, but only access to the system. In addition, it should be emphasized that the vulnerability identified as a result of a breach of personal data protection is related to the technical measures used to identify users, and thus their rights in the system. As indicated by the Company in the notification of a personal data breach of [...] December 2019, "the breach consisted in the use of [...] due to its purpose [...], due to a design error it allowed [...]. The identifying argument [...] that should be validated so that only knowing [...] is not actually taken into account. Therefore, the induction of [...] was possible with the administration of [...]. The attacker used [...] ”. Checking the correctness of the assumed validation [...] is so obvious and basic that the only correct conclusion that can be drawn is the statement that the implementation of a system for the processing of personal data for use without properly functioning of the above-mentioned validation proves a gross neglect of the basic obligations of the personal data controller, in the context of art. 32 GDPR.

According to the Company, "the use of the system's vulnerability to the attack in question, resulting in gaining access to data, was not dependent on the lack of proper testing, measurement or evaluation of the system, as the indicated activities were regularly and properly carried out by the Company. This is confirmed by the printouts from the C system concerning the vulnerability [...] and the verification of the entered data, which prove that although V did not carry out tests specifically related to the vulnerability used during the attack of [...] - [...] December 2019. , however, these are other tests [...] aimed at detecting vulnerabilities and improving the quality of data being conducted ”.

In the opinion of the President of the Office, performing tests only in the event of an emerging threat, without introducing a procedure that would define a schedule of activities ensuring regular testing, measurement and evaluation of the effectiveness of the implemented measures, is insufficient. According to the collected material, the company, despite the adopted solutions, was not able to detect the vulnerability due to the lack of regular tests of the B system implemented by the Company, which, according to the Company's explanations obtained during the inspection, was supposed to verify [...] and compliance of the id of the application for registration with the [...] registrant of the application.

It should be emphasized that regular testing, measuring and evaluating the effectiveness of technical and organizational measures to ensure the security of processing is a fundamental duty of every controller and processor under Art. 32 sec. 1 lit. d of Regulation 2016/679. The administrator is therefore obliged to verify both the selection and the level of effectiveness of the technical measures used at each stage of processing. The comprehensiveness of this verification should be assessed through the prism of adequacy to risks and proportionality in relation to the state of technical knowledge, implementation costs and the nature, scope, context and purposes of processing. On the other hand, in the present state of facts, the Company partially fulfilled this obligation, verifying and modifying the level of effectiveness of the implemented security measures in situations where there was a suspicion of the existence of a vulnerability - then works were undertaken to protect against a given vulnerability. As mentioned above, no tests were carried out to verify the security of application A and [...] system B related to the breach of personal data protection.

Nor can it be considered that the activities, as indicated by the Company, consisting in subjecting technical and organizational measures to reviews and updates in the event of organizational or legal changes occurring, constitute the fulfillment of the administrator's obligation to ensure regular, measurement and testing. Such activities do not satisfy the requirement of regularity. The tests should be performed regardless of whether such changes in the Company's operations take place or not. The changes referred to by the Company should, however, be a factor causing the need to re-analyze the risk and their impact on the security of the processed data, the result of which should be taken into account when applying a security measure, which is regular testing.

Therefore, it should be emphasized that carrying out reviews in the event of an organizational or legal change, as well as taking actions only in the event of suspicion of a vulnerability, cannot be considered as regular testing, measuring and assessing the effectiveness of technical and organizational measures to ensure the security of data processing. They are undertaken in connection with the occurrence of a specific event, e.g. an organizational change at the data controller. Therefore, they have more features of a risk analysis, which should be performed in the event of this type of changes in the organization and the course of personal data processing processes. Meanwhile, it is advisable to test, measure and evaluate to fulfill the requirement under Art. 32 sec. 1 lit. d of Regulation 2016/679, must be performed on a regular basis, which means conscious planning and organization, as well as documenting (in connection with the accountability principle referred to in Article 5 (2) of Regulation 2016/679) of this type of activities in specific time intervals, regardless of changes in the organization

and the course of data processing processes caused, for example, by an organizational change at the data controller. However, the Company did not take such actions, which proves that this provision of Regulation 2016/679 was breached.

The President of the Office for Personal Data Protection shares the view expressed by the Provincial Administrative Court in Warsaw in the judgment of 3 September 2020, file number II SA / Wa 2559/19, according to which: "Regulation 2016/679 introduced an approach in which risk management is the foundation activities related to the protection of personal data and is a continuous process. Entities processing personal data are obliged not only to ensure compliance with the guidelines of the above-mentioned of the regulation through one-off implementation of organizational and technical security measures, but also to ensure the continuity of monitoring the level of threats and ensuring accountability in terms of the level and adequacy of the introduced security. This means that it becomes necessary to prove to the supervisory authority that the implemented solutions aimed at ensuring the security of personal data are adequate to the level of risk, as well as taking into account the nature of the organization and the personal data processing mechanisms used. The administrator is to independently carry out a detailed analysis of the data processing processes carried out and assess the risk, and then apply such measures and procedures that will be adequate to the assessed risk.

The consequence of such an orientation is the resignation from the lists of security requirements imposed by the legislator, in favor of the independent selection of security measures based on the analysis of threats. Administrators are not informed about specific security measures and procedures. The administrator is to independently carry out a detailed analysis of the data processing processes carried out and assess the risk, and then apply such measures and procedures that will be adequate to the assessed risk. "

In the context of the judgment cited, it should be noted that the risk analysis carried out by the personal data administrator should be documented and justified on the basis of, first of all, the determination of the actual state of affairs at the time of its performance. The characteristics of the ongoing processes, assets, vulnerabilities, threats and existing safeguards as part of the ongoing processes of personal data processing should be taken into account in particular.

The term assets is used to indicate everything that is of value to the organization, company - the personal data administrator. Some assets will be worth more than others and should also be assessed and secured from this perspective. The interrelationships of existing assets are also very important, e.g. the confidentiality of assets (personal data) will depend on the type and method of processing these data. Establishing the value of assets is necessary to estimate the effects of a possible

incident (breach of personal data protection).

It is necessary, inter alia, to define the existing security features so as not to duplicate them. It is also essential to check the effectiveness of these security measures, because the existence of an unchecked security may, firstly, eliminate its value, and secondly, it may give a false sense of security and may result in omitting (not detecting) a critical vulnerability, which, if used, will have very negative consequences, including in particular it may lead to a breach of personal data protection.

Vulnerability is commonly defined as a weakness or a security gap which, when exploited by a given threat, may interfere with functioning, and may also lead to incidents or violations of personal data protection. Identifying threats consists in determining what threats and from what direction (reason) may appear.

The method of conducting a risk analysis is, for example, defining the risk level as the product of the probability and the effects of the occurrence of a given incident. Typically, a risk matrix is used to visualize the levels of risk, representing the levels of risk for which the organization defines the relevant activities.

The risk analysis presented during the inspection, carried out in May 2018, does not fully reflect the actual state of the [...] process being the subject of the inspection, in connection with the occurrence of a personal data breach reported by the Company on [...] December 2019 r. According to the material collected during the inspection, the review of technical and organizational measures was carried out by the Company only before the application of the general regulation. However, it cannot be considered real and factual, as it did not reveal a vulnerability in the functioning of the system.

It should be emphasized that the examination of the probability of the occurrence of a given event should not be based solely on the frequency of occurrence of events in a given organization, because the fact that a given event did not occur in the past does not mean that it cannot occur in the future.

The risk indicated in the risk analysis presented in the form of "unauthorized access by third parties or unauthorized disclosure of data to third parties" should not be defined by the Company at the level "Not applicable", because this event may occur in any organization due to many different reasons, while the answer "Not applicable" would be justified if the Company did not process personal data in this process. On the other hand, as evidenced by the evidence found in the course of the inspection and administrative proceedings, this is the threat that materialized through the use of an unidentified vulnerability in the processing of personal data [...] in connection with the breach of personal data protection of pre-paid subscribers.

The assumption of the value "Medium / rare" and the rating at the level of "2" for the risk of "lack of testing the vulnerability of

IT systems" also proves the superficial approach to the risk of violating the rights and freedoms of natural persons by the Company. The adopted assessment should reflect the real situation prevailing in a given organization and be based primarily on the facts found during the examination of this situation, carried out in the form of an audit, verification or on the basis of the stated facts. However, as it results from the evidence collected during the audit, in 2019 the Company did not conduct a review of the technical and organizational measures applied, which in itself disqualifies the assessment made at this level, and as indicated above, incidental actions do not meet the hallmarks of regularity.

The above findings allow for an unequivocal statement that the risk analysis was aimed only at showing that there is no high risk of violating the rights and freedoms of natural persons, and thus that it is not necessary to implement additional technical and organizational measures. However, such an approach resulted in the lack of a proper assessment of threats to the processing of personal data of pre-paid subscribers (a process called [...]) and, as a consequence, their inadequate protection, which resulted in a breach of personal data protection.

It should also be noted that the presented risk analysis was carried out in May 2018, and therefore for over a year and a half (from May 2018 to December 2019), the Company did not take any steps to verify its assumptions and ratings. Meanwhile, like other organizational measures, the risk analysis should also be subject to periodic reviews and updates, and as it results from the collected material, another risk analysis for the process [...] was carried out only [...] in December 2019, so already after a breach of personal data protection. It should be emphasized that each check, audit or review must be based on complete and reliable information. The functioning of any organization, especially in the area of personal data protection, cannot be based on unreliable or unrealistic grounds, and disregarding the value of basic information may result, as indicated above, in a false sense of security and failure by the personal data controller to undertake actions to which it is obliged, which in turn may result, as in the present case, in a breach of personal data protection, causing, due to the scope of the personal data subject to breach, a high risk of violating the rights and freedoms of natural persons.

As indicated by the Provincial Administrative Court in Warsaw in the judgment with reference number II SA / Wa 2826/19 of August 26, 2020, "(...) technical and organizational activities are the responsibility of the personal data administrator, but cannot be selected entirely free and voluntary, without taking into account the degree of risk and the nature of the personal data protected. ”which this authority takes for its own view.

Therefore, the lack of a reliable risk analysis, combined with the lack of regular testing, measurement and evaluation of the

effectiveness of the implemented technical and organizational measures to ensure the security of processing, led, which should be emphasized again, to a breach of data protection, but also determines the breach by the Company of the obligations incumbent on it. data administrator, resulting from art. 24 sec. 1, art. 25 sec. 1, art. 32 sec. 1 lit. b and lit. d and art. 32 sec. 2 of Regulation 2016/679.

Referring to the submitted copies of the certificates obtained [...] July 2020: ISO / IEC 27001: 2013 certifying the implementation and maintenance of the information security management system by the Company in the field of services provided by the telecommunications operator and ISO / IEC 27701: 2019 certifying the implementation and the maintenance of the personal data management system by the Company as an extension of ISO / IEC 27001: 2013 and ISO / IEC 27002: 2013 with privacy management in the field of services provided by a telecommunications operator and the explanations provided in this regard, it should be considered that the Company has rectified the defect in the course of the proceedings in the form of the lack of procedures ensuring regular testing, measurement and evaluation of the effectiveness of the measures adopted in the documentation kept by the Company, describing the data processing process and the organizational and technical measures applied.

As indicated by the Company in the submitted explanations, the requirements of maintaining the certificates of compliance of the management system in the Company with the implemented standards mean, inter alia, covering the functioning of the information security and data protection management system with an annual internal audit conducted by the Company and an external independent institution issuing the certificate. The above means that the Company has implemented solutions that ensure regular testing, measurement and evaluation of the effectiveness of the measures adopted to ensure the security of data processing. However, the implementation of these solutions took place only [...] July 2020, i.e. after a significant time since the violation of the protection of personal data of subscribers of prepaid services.

Referring to the explanations of the Company and the circumstances indicated therein, that at the time of introducing changes to its activities required by the Act on anti-terrorist activities, it was not obliged to comply with the principle of data protection at the design stage referred to in Art. 25 sec. 1 of Regulation 2016/679, the President of the Office points out that the Act on anti-terrorist activities entered into force on July 2, 2016, i.e. after the entry into force of Regulation 2016/679, which was published in the EU Official Journal on May 4, 2016. According to Art. 99 sec. 1 of Regulation 2016/679, the said regulation shall enter into force on the twentieth day following its publication in the Official Journal of the European Union and shall apply

from 25 May 2018 (Article 99 (2)). Therefore, on May 24, 2016, Regulation 2016/679 entered into force with the obligation to apply directly from May 25, 2018. As emphasized in recital 171 of Regulation 2016/679 (the recitals contain the justification of the provisions of the enacting part of the act, i.e. the regulation), processing already in progress at the date of application of this Regulation should comply with its provisions within two years from the entry into force of this Regulation. Bearing in mind that systems B and A have been in operation since 2014, the Company has been adapting the systems used to the requirements imposed by the provisions of the Act on anti-terrorist activities, amending the Act of July 16, 2014, Telecommunications Law (Journal of Laws of 2019, item 2460), should take into account already at this stage the obligations imposed by the provision of Art. 25 of the Regulation 2016/679. The implementation of the obligations imposed by the Act on anti-terrorist activities coincided with the obligation to adjust data processing to the requirements of Regulation 2016/679.

It should also be emphasized that the referred to Art. 25 sec. 1 of Regulation 2016/679, despite the fact that the controller's obligation indicated therein is called "data protection at the design stage", it applies not only to the design stage, but also to the data processing stage itself. The implementation of security measures is a continuous process, not just a one-time action by an administrator. The measures mentioned therein, such as "data minimization" or "pseudonymization", are only an example of measures that should be applied in order to meet the requirement to implement data protection principles and provide processing with the necessary safeguards to meet the requirements of the regulation and protect the rights of data subjects. concern.

In the explanations, the company claims that at this stage of the proceedings it has not been shown who the attacker was. The way the vulnerability was exploited indicated that the attacker had earlier access to the system and knew how to construct an appropriate query. At present, the Company does not know if and with what rights the attacker could have had, and to what period this power could apply. In the opinion of the Company, it is up to the President of the Office to prove whether the data has been disclosed to an unauthorized person.

Referring to the above statement of the Company that it is on the part of the President of the Office to prove whether the data has been disclosed to an unauthorized person, it should be emphasized that the President of the Office does not have the authority to conduct proceedings aimed at detecting the perpetrator of a crime and assessing whether it has occurred. commissions, these are due to law enforcement authorities, because they are entitled to conduct such proceedings and assess whether a crime has been committed and to qualify a criminal act. There is no doubt, however, that the data was

disclosed, which was confirmed by the decision of the District Prosecutor in W. of [...] July 2020, file ref. [...] to discontinue the investigation into the failure to identify the perpetrator of the crime. The competences of the President of the Office include the assessment of whether the data controller processes data in accordance with the requirements resulting from the provisions on the protection of personal data and the responsibility of the data controller for data processing in a manner that violates these provisions.

Therefore, it should be pointed out again that the obligation of each controller is to process data in accordance with the principles set out in Art. 5 of Regulation 2016/679, in this case in accordance with Art. 5 sec. 1 lit. f. However, pursuant to Art. 5 sec. 2 of Regulation 2016/679, he is responsible for compliance with the provisions of para. 1 and must be able to demonstrate compliance with them (accountability). This obliges the administrator to exercise due diligence both when granting authorizations to process data and also when withdrawing authorizations for a former employee, contractor or contractor. The circumstances of making a decision to terminate the legal relationship with an employee, contractor or contractor may increase the risk of attempts of unauthorized access to the entity's resources. Therefore, constant monitoring of IT systems is the responsibility of the administrator ensuring that the requirements imposed by the provisions of Art. 32 sec. 1 lit. b and d of Regulation 2016/679. It is on the part of the Company to demonstrate to the supervisory authority that it has implemented appropriate data security measures and secured data against unauthorized access, e.g. by those whose authorization has expired, as well as to demonstrate that it has taken all possible steps to prevent a breach of data confidentiality and is not responsible for this breach.

The Company's statement that it does not know if and what rights the attacker could have, and what period could apply to this right, confirms that the technical and organizational measures implemented by the Company to ensure data security were insufficient. The lack of knowledge about this information also proves that the Company has no control over the data processing, which constitutes a breach of the principle of accountability.

The above proves that the findings of the President of the Office are correct that the Company has not correctly implemented the requirements of Regulation 2016/679 in the scope specified in Art. 24 sec. 1, art. 25 sec. 1, art. 32 sec. 1 lit. b and lit. d and art. 32 sec. 2 of Regulation 2016/679, which led to a breach of the protection of personal data of subscribers of prepaid services. The consequence of the violation of the above-mentioned provisions of Regulation 2016/679 is also the violation of the confidentiality principle expressed in Art. 5 sec. 1 lit. f of the Regulation 2016/679 and the accountability rules referred to in

art. 5 sec. 2 of Regulation 2016/679.

In summary, despite the removal by the Company of deficiencies in ensuring the security of the processed data, including the vulnerability of IT systems used to process the personal data of subscribers of pre-paid services, resulting in a breach of the confidentiality of personal data, there were premises justifying the application to the Company of the powers of the President of the Office to impose an administrative penalty for breach of the principle of confidentiality of data (Article 5 (1) (f) of Regulation 2016/679) and, consequently, of the principle of accountability (Article 5 (2) of Regulation 2016/679) in connection with the breach of the administrator's obligations when implementing technical and organizational measures in during data processing, in order to effectively implement data protection rules (Article 25 (1) of Regulation 2016/679); obligations to ensure the confidentiality, integrity, availability and resilience of data processing systems and services (Article 32 (1) (b) of Regulation 2016/679); the obligation to regularly test, measure and evaluate the effectiveness of the adopted technical and organizational measures to ensure the security of processing (Article 32 (1) (d) of Regulation 2016/679) and the obligation to take into account the risk related to processing resulting from unauthorized access to personal data being processed (Article 32 (2) of Regulation 2016/679).

The exercise by the President of the Office of exercising his / her rights results primarily from the fact that the controller breached the basic principles of data processing, i.e. the principle of confidentiality, as well as the principle of accountability, which is an absolute obligation to demonstrate to the President of the Office compliance with the provisions of the general regulation on data protection.

Based on Article. 58 sec. 2 lit. and Regulation 2016/679, each supervisory authority has the power to apply, in addition to or instead of other remedial measures provided for in Art. 58 sec. 2 lit. a - h and lit. j of this regulation, an administrative fine under Art. 83 of the Regulation 2016/679, depending on the circumstances of the specific case.

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

a) The nature and gravity of the infringement, the number of people injured (Article 83 (2) (a) of Regulation 2016/679). The violation found in the present case, which resulted in obtaining unauthorized access to the data processed by the Company by a person or unauthorized persons, and, consequently, the acquisition of personal data of subscribers of the Company's

prepaid services, is of considerable importance and serious nature, as it poses a high risk of negative legal consequences for a large the number of persons accessed by the person or unauthorized persons. The breach by the Company of the obligations to apply security measures to the processed data against their disclosure to unauthorized persons entails not only the potential, but also a real possibility of using this data by third parties without the knowledge and against the will of the data subjects, contrary to the provisions of Regulation 2016/679 e.g. to enter into legal relationships or to enter into commitments on behalf of the data subjects. The fact that the Company, which processes personal data in a professional manner, as part of its activities, has greater responsibility and greater requirements than the entity that processes personal data as part of a side activity, incidentally or on a small scale, also has a significant impact on the seriousness of the breach. When conducting commercial activities, the Company, as the data controller, should take all necessary actions and exercise due diligence in the selection of technical and organizational measures ensuring the security and confidentiality of data. The factual findings made by the President of the Personal Data Protection Office prove that the Company did not cope with this task at the time of the infringement;

b) Duration of the infringement (Article 83 (2) (a) of Regulation 2016/679). The President of the Office considers the long duration of the infringement to be an aggravating circumstance. It is true that the period during which the unauthorized person or persons had access to personal data processed by the Company was relatively short (although still sufficient to copy all available data), the breach was a long-term state. It was created before the date of application of Regulation 2016/679, i.e. before [...] May 2018, and was finally removed - during the procedure ended with the issuance of this decision - with the receipt by the Company on [...] July 2020 of ISO / IEC 27001: 2013, ISO / IEC 27701: 2019, ISO / IEC 27001: 2013 and ISO / IEC 27002: 2013 certificates, certifying the implementation of procedures ensuring regular testing, measurement and evaluation of the effectiveness of the measures adopted in the documentation kept by the Company describing the data processing process and the organizational and technical measures applied.

c) The extent of the damage suffered by the persons affected by the infringement (Article 83 (2) (a) of Regulation 2016/679). In the present case, there is no evidence that the persons accessed to the data obtained by the person or unauthorized persons suffered material damage. Nevertheless, the very breach of the confidentiality of their data is a non-pecuniary damage (harm) to them; natural persons whose data has been obtained in an unauthorized way may at least feel the fear of losing control over their personal data, identity theft or identity fraud, and finally of financial loss.

d) Intentional or unintentional nature of the infringement (Article 83 (2) (b) of Regulation 2016/679). Unauthorized access to the personal data of subscribers of the Company's prepaid services has become possible as a result of failure to exercise due diligence by the Company and undoubtedly constitutes an unintentional nature of the breach. Nevertheless, the Company, as the administrator, is responsible for any irregularities found in the data processing process. The fact that the Company, although it assumed that the system would verify [...], did not carry out a test for the correct operation of the system in accordance with the assumed requirements deserves a negative assessment. In this state of affairs, the negligence of the Company should be considered gross.

When determining the amount of the administrative fine, the President of the Personal Data Protection Office took into account, as a mitigating circumstance, reducing the amount of the fine imposed, the good cooperation of the Company with the supervisory body undertaken and carried out in order to remove the violation and mitigate its possible negative effects (Article 83 (2)). letter f of Regulation 2016/679). It should be noted here that, apart from the correct fulfillment of the procedural obligations incumbent on the Company, both during the control proceedings and in the administrative proceedings concluded with the issuance of this decision, the Company fully implemented the recommendations of the President of the Office regarding supplementing the notification of data subjects about the breach that has occurred. The company also took specific and quick actions to eliminate the infringement. In particular, the Company removed from the IT system its susceptibility to violation of the protection of personal data processed in the system, used by a person or unauthorized persons. The company has also implemented ISO standards that guarantee a high level of procedures for the future regulating, inter alia, processing of personal data in the Company, including regular reviews and audits of security and functioning of personal data management and information security systems.

The sanctions applied by the President of the Office in the present case, in the form of an administrative fine, as well as its amount, had no influence on other sanctions indicated in Art. 83 sec. 2 of Regulation 2016/679, the circumstances:

a) actions taken by the Company to minimize the damage suffered by data subjects (Article 83 (2) (c) of Regulation 2016/679);

b) the degree of responsibility of the Company, taking into account the technical and organizational measures implemented by it pursuant to Art. 25 and 32 of Regulation 2016/679 (Article 83 (2) (d) of Regulation 2016/679);

c) relevant previous violations of the provisions of Regulation 2016/679 by the Company (Article 83 (2) (e) of Regulation 2016/679);

d) category of personal data affected by the breach (Article 83 (2) (g) of Regulation 2016/679);

e) how the supervisory authority learned about the breach (Article 83 (2) (h) of Regulation 2016/679);

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

(g) adherence to approved codes of conduct pursuant to Art. 40 of the Regulation 2016/679 or approved certification mechanisms pursuant to Art. 42 of Regulation 2016/679 (Article 83 (2) (j) of Regulation 2016/679);

(h) financial gains or losses avoided, directly or indirectly, from the infringement (Article 83 (2) (k)).

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

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

In view of the above, pursuant to Art. 83 sec. 3 of Regulation 2016/679, the President of the Personal Data Protection Office determined the total amount of the administrative fine in an amount not exceeding the amount of the fine for the most serious

breach. In the presented facts, the most serious breach by the Company of the confidentiality principle specified in Art. 5 paragraph 1 lit. f of Regulation 2016/679, and consequently the principle of accountability specified in Art. 5 sec. 2 of Regulation 2016/679. This is supported by the serious nature of the breach and the group of people affected by it (123,391 - one hundred twenty three thousand three hundred and ninety one subscribers of prepaid services administered by the Company). Importantly, in relation to the above-mentioned number of people, there is still a high risk of unlawful use of their personal data, because the purpose for which the person or unauthorized persons took steps to obtain these data through [...] containing personal data is unknown.

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

Bearing in mind the above, the President of the Personal Data Protection Office, pursuant to art. 83 sec. 4 lit. a and art. 83 sec. 5 lit. and in connection with art. 83 sec. 3 of the Regulation 2016/679 and in connection with Art. 103 of the Personal Data Protection Act of May 10, 2018, imposed on the Company - using the average EUR exchange rate of January 28, 2020 (EUR 1 = PLN 4.2794) - an administrative fine in the amount of PLN 1,968,524.00 (equivalent to EUR 460,000).

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

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

The applied financial penalty is also proportional to the infringement found, in particular its seriousness, the number of

individuals affected by it and the risk they incur in connection with the infringement. In the opinion of the President of the Personal Data Protection Office, the fine imposed on the Company is also proportional to the Company's net revenues for 2019 [...] and will not constitute an excessive burden for it. It should be emphasized that the Management Board of the Company took steps to ensure the possibility of going concern […].

The amount of the fine was therefore set at such a level that, on the one hand, it would constitute an adequate response of the supervisory authority to the degree of breach of the administrator's obligations, on the other hand, it did not result in a situation in which the necessity to pay a financial penalty would entail negative consequences, such as a significant deterioration of the financial situation. Companies. In the opinion of the President of the Personal Data Protection Office, the Company should and is able to bear the consequences of its negligence in the field of data protection, hence the imposition of a penalty of PLN 1,968,524.00 is fully justified.

In the opinion of the President of the Personal Data Protection Office, the administrative fine will fulfill a repressive function in these specific circumstances, as it will be a response to a breach by the Company of the provisions of Regulation 2016/679, but also a preventive one, as it will contribute to preventing future violations of the Company's obligations resulting from provisions on the protection of personal data, both when processing data by the Company itself and in relation to entities acting on its behalf.

In the opinion of the President of the Personal Data Protection Office, the applied fine meets the conditions referred to in Art. 83 sec. 1 of Regulation 2016/679 due to the seriousness of the breaches found in the context of the basic requirements and principles of Regulation 2016/679 - in particular the principle of confidentiality expressed in Art. 5 sec. 1 lit. f of the Regulation 2016/679.

The purpose of the penalty is to ensure that the Company complies with the provisions of Regulation 2016/679 in the future.

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

The decision is final. The party has the right to lodge a complaint against the decision with the Provincial Administrative Court in Warsaw, within 30 days from the date of its delivery, via the President of the Office for Personal Data Protection (address: ul. Stawki 2, 00-193 Warsaw). A proportional fee should be filed against the complaint, in accordance with Art. 231 in connection with Art. 233 of the Act of August 30, 2002, Law on proceedings before administrative courts (Journal of Laws of

2019, item 2325, as amended). Pursuant to Art. 74 of the Act of May 10, 2018 on the Protection of Personal Data (Journal of Laws of 2019, item 1781), the submission of a complaint by a party to the administrative court suspends the execution of the decision on the administrative fine.

In the proceedings before the Provincial Administrative Court, the party has the right to apply for the right of assistance, which includes exemption from court costs and the appointment of an attorney, legal advisor, tax advisor or patent attorney. The right to assistance may be granted at the request of a party submitted prior to the initiation of the proceedings or in the course of the proceedings. The application is free of court fees.

Pursuant to Art. 105 paragraph. 1 of the Act of 10 May 2018 on the Protection of Personal Data, the administrative fine must be paid within 14 days from the date of the expiry of the deadline for lodging a complaint to the Provincial Administrative Court, or from the date of the final decision of the administrative court, to the bank account of the Office for Personal Data Protection at the National Bank of Poland O / O Warszawa no. 28 1010 1010 0028 8622 3100 0000. Moreover, pursuant to Art. 105 paragraph. 2 of the above-mentioned Act, the President of the Personal Data Protection Office may, at a justified request of the punished entity, postpone the payment of the administrative fine or divide it into installments. In the event of postponing the payment of the administrative fine or dividing it into installments, the President of the Personal Data Protection Office shall charge interest on the unpaid amount on an annual basis, using a reduced rate of late payment interest, announced pursuant to Art. 56d of the Act of August 29, 1997 - Tax Ordinance (Journal of Laws of 2020, item 1325, as amended), from the day following the date of submitting the application.

2020-12-10