THE CHAIRMAN OF PERSONAL DATA PROTECTION

Warsaw, on 06

July

2022

DECISION

DKN.5131.34.2021

Based on Article. 104 § 1 of the Act of 14 June 1960 Code of Administrative Procedure (Journal of Laws of 2021, item 735, as amended), art. 7 sec. 1, art. 60 and art. 102 paragraph. 1 point 1 and sec. 3 of the Act of May 10, 2018 on the Protection of Personal Data (Journal of Laws of 2019, item 1781), as well as Art. 57 sec. 1 it. a) and h), art. 58 sec. 2 it. e) i i), Art. 83 sec. 1-3 and art. 83 sec. 4 it. a) in connection with Art. 33 sec. 1 and art. 34 sec. 1, 2 and 4 of Regulation 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 data protection) (Journal of Laws UE 119 of 04/05/2016, p. 1, as amended), hereinafter also referred to as "Regulation 2016/679", after conducting administrative proceedings initiated ex officio regarding violation of provisions on the protection of personal data by the University Clinical Center of the Medical University of Warsaw with headquarters in Warsaw at ul. Banacha 1a, President of the Personal Data Protection Office,

finding a violation by the University Clinical Center of the Medical University of Warsaw with its seat in Warsaw at ul. Banacha 1a regulations:

a) Art. 33 sec. 1 of Regulation 2016/679, consisting in not reporting the breach of personal data protection to the President of the Personal Data Protection Office without undue delay, no later than 72 hours after the breach has been found,

b) art. 34 sec. 1 of Regulation 2016/679, consisting in not notifying about a breach of personal data protection, without undue delay of the data subject,

1) imposes on the University Clinical Center of the Medical University of Warsaw with its seat in Warsaw at ul. Banacha 1a, an administrative fine of PLN 10,000 (say: ten thousand zlotys),

2) orders to notify the data subject about the breach of personal data protection in order to provide him with the information required in accordance with art. 34 sec. 2 of the Regulation 2016/679, i.e .:

a) description of the nature of the personal data breach;

(b) the name and contact details of the data protection officer or designation of another contact point from which more information can be obtained;

c) a description of the possible consequences of a breach of personal data protection;

d) a description of the measures taken or proposed by the administrator to remedy the breach - including measures to minimize its possible negative effects,

within 3 days from the date on which this decision becomes final.

Justification

The University Clinical Center of the Medical University of Warsaw, hereinafter also referred to as the Administrator, pursuant to the statute constituting Annex 2 to the resolution [...] of the Senate of the Medical University of Warsaw of [...] October 2021, is a medical entity that is not an entrepreneur and is run in the form of an independent public a healthcare facility on the basis of the order of the Minister of Health and Social Welfare No. 2/98 of December 4, 1998 on the transformation of a public healthcare facility into an independent public healthcare facility, resolution No. [...] of the Senate of the Medical University of Warsaw of [...] May 2018 [...] and ordinance No. [...] of the Rector of the Medical University of Warsaw of [...] May 2018 [...]. The main goal of the University Clinical Center of the Medical University of Warsaw is, inter alia, providing health services and promoting health. The University Clinical Center of the Medical University of Warsaw has been entered into the National Court Register under number KRS 0000073036 and to the Register of Entities Performing Medical Activities, kept by the Mazowieckie Voivode, under number 000000018598.

On [...] March 2021, the President of the Office for Personal Data Protection, hereinafter also referred to as the "President of the Personal Data Protection Office", received information from the Patient Ombudsman about a possible breach of personal data protection at the University Clinical Center of the Medical University of Warsaw with its seat in Warsaw. The attached materials showed that the Administrator's patient had received a referral from one of the doctors to a specialist clinic containing personal data of another person in the scope of: name, surname, address, PESEL identification number and information on health (information about the diagnosis and purpose of the advice).

In connection with the above, in a letter of [...] April 2021, the President of UODO asked the Administrator to provide information whether, in connection with the above-mentioned the incident, an analysis of the risk of violation of the rights or

freedoms of natural persons was carried out, necessary to assess whether there was a breach of data protection resulting in the need to notify the supervisory authority and the data subject.

In response, in a letter of [...] April 2021, the Administrator informed, inter alia, the supervisory authority that: "(...) The Controller's department [...], after performing a preliminary, simplified analysis of the risk level of an incident, due to its scope subjective (potentially the victim was one natural person whose data was disclosed to one identifiable person in a narrow and incorrect scope), qualified them as a security incident. Thus, the employees of the above-mentioned of the Administrator's department, decided not to report the incident to the President of the Data Protection Office "and" (...) due to the fact that the incident does not have significant effects on the rights and obligations of the data subject, the Administrator maintained its decision not to notify the President Office for Personal Data Protection, as well as data subjects ".

To the above The administrator enclosed the "Form for assessing the effects of a personal data breach" and explanations of the doctor responsible for the occurrence of the personal data breach. With the above explanations showed that "Patient P.Ż. he was [...] .03.2021 in the Clinic [...] in the hospital. After examination and evaluation of the research, he was referred to the local clinic [...]. (…) After some time, patient Ż. he returned to the office with the claim that the Clinic […] was closed until further notice. (...) In order for the patient not to waste time, I sent a referral to another clinic [...] with a request for treatment. (...) Due to my nervousness, I took the wrong disease card and entered the wrong patient data by mistake. The data was written on the patient A. W. But these are not the data of this patient. The data belongs to patient A. W. Patient A. W. does not exist with such data ”.

The President of the Personal Data Protection Office did not agree to the above-mentioned position and therefore, pursuant to Art. 61 § 1 and 4 of the Act of 14 June 1960 Code of Administrative Procedure (Journal of Laws of 2021, item 735, as amended), hereinafter also referred to as "the Code of Administrative Procedure", in connection with Art. 58 sec. 2 it. e) of Regulation 2016/679, in a letter of [...] July 2021, he initiated ex officio administrative proceedings against the University Clinical Center of the Medical University of Warsaw with its seat in Warsaw regarding the failure to notify the personal data breach to the President of the Personal Data Protection Office and the failure to notify the data breach personal data of the affected person.

In response to the letter informing about the initiation of administrative proceedings, the Administrator, in a letter of [...] August 2021, informed the President of the Personal Data Protection Office that he had learned about the incident on [...] March 2021,

as a result of receiving a request for explanations from Office of the Patient Ombudsman (file reference [...]). Moreover, in the above-mentioned the letter explained that "On the date of receipt of the information, the Administrator's [...] Department, after making a preliminary, simplified analysis of the risk level of an incident, due to its subject-subject scope (potentially one, non-existent natural person [on the referral, who was supposed to be issued to Mrs. A. W., a non-existent A. W. was indicated, whose data was disclosed to one identifiable person), qualified them as a security incident ". As a consequence of the finding that the incident in question concerned a non-existent person, the Administrator concluded, as a result of the risk assessment carried out, that it did not have "significant effects on the rights and obligations of the data subject, ie Ms A. W.". Due to the assumption that this breach is unlikely to result in a risk of violation of the rights or freedoms of natural persons, the Controller decided not to report it to the supervisory authority, as well as to notify the data subject about it.

To the above The administrator has re-attached the "Personal data breach impact assessment form" and the explanations of the doctor responsible for the breach of personal data protection.

Having read all the evidence collected in the case, the President of the Office for Personal Data Protection considered the following:

Pursuant to Art. 4 point 12 of Regulation 2016/679, "breach of personal data protection" means a breach of security leading to accidental or unlawful destruction, loss, modification, unauthorized disclosure or unauthorized access to personal data transmitted, stored or otherwise processed.

Art. 33 sec. 1 and 3 of Regulation 2016/679 provides that in the event of a breach of personal data protection, the data controller shall, without undue delay - if possible, no later than 72 hours after finding the breach - report it to the competent supervisory authority pursuant to Art. 55, unless it is unlikely that the violation would result in a risk of violating the rights or freedoms of natural persons. The notification submitted to the supervisory authority after 72 hours shall be accompanied by an explanation of the reasons for the delay. The notification referred to in para. 1 must at least:

a) describe the nature of the personal data breach, including, if possible, the categories and approximate number of data subjects, as well as the categories and approximate number of personal data entries affected by the breach; b) include the name and contact details of the data protection officer or the designation of another contact point from which more information can be obtained;

c) describe the possible consequences of the breach of personal data protection; (d) describe the measures taken or proposed

by the controller to address the personal data breach, including, where appropriate, measures to minimize its possible negative effects.

In turn, Art. 34 sec. 1 of Regulation 2016/679 indicates that in a situation where a breach of personal data protection may result in a high risk of violation of the rights or freedoms of natural persons, the controller is obliged to notify the data subject about such a breach without undue delay. Pursuant to Art. 34 sec. 2 of Regulation 2016/679, the correct notification should: 1) describe the nature of the personal data breach in clear and simple language; 2) contain at least the information and measures referred to in art. 33 sec. 3 it. b), c) and d) of Regulation 2016/679, i.e. a) name and surname and contact details of the data protection officer or designation of another contact point from which more information can be obtained; b) description of the possible consequences of a breach of personal data protection; (c) a description of the measures taken or proposed by the controller to address the personal data breach, including, where appropriate, measures to minimize its possible negative effects.

Reporting breaches of personal data protection by administrators is an effective tool contributing to a real improvement in the security of personal data processing. When reporting a breach to the supervisory authority, the administrators inform the President of the Personal Data Protection Office whether, in their opinion, there is a high risk of violating the rights or freedoms of data subjects, and - if such a risk occurred - whether they provided relevant information to natural persons affected by the breach. In justified cases, they can also provide information that, in their opinion, notification is not necessary due to the fulfillment of the conditions set out in Art. 34 sec. 3 it. a) - c) of Regulation 2016/679. The President of the Personal Data Protection Office (UODO) verifies the assessment made by the controller and may - if the controller has not notified the data subjects - request such notification from him. Notifications of a breach of personal data protection allow the supervisory authority to react appropriately, which may limit the effects of such breaches, because the controller is obliged to take effective measures to protect natural persons and their personal data, which on the one hand will allow for the control of the effectiveness of the existing solutions, and on the other for the assessment of modifications and improvements to prevent irregularities similar to those covered by the infringement.

In the case at hand, there was a breach of personal data protection consisting in the disclosure, as a result of an error of a doctor issuing a referral to a specialist clinic, of personal data to an unauthorized person (another patient of the Administrator) in the scope of: name, address, PESEL identification number and information on health. The document issued by the doctor

contained a mistake on the patient's behalf, ie instead of the name "A" (male name), the first name "A" (female name) was entered incorrectly. However, the presented materials show that the other data contained in the above-mentioned the referral, i.e. surname, address and PESEL number, related to Ms A. W. Therefore, it should be emphasized that there was only a spelling error (the so-called "typo") in the name of the person whose data was entered for referral to a specialist clinic who was released to another patient. Therefore, the circumstance indicated by the Administrator that "one natural person who does not actually exist has been potentially wronged" is not applicable. Despite the mistake on behalf of that person, he can be easily identified. For such identification, it is sufficient to have data in the form of surname, address and PESEL number. Moreover, the referral to a specialist clinic, issued by the Administrator's doctor to an unauthorized person (to another patient), also contained health data, including information on the diagnosis and purpose of the advice. Even assuming that the referral to the specialist clinic of the above-mentioned information about the state of health concerns in fact an unauthorized recipient (a patient who was referred to), the very fact that Ms A. W. is a patient of the Clinic [...] is also information about her health condition. Information in this regard also increases the possibility of identifying this person. It should also be emphasized that in the "Form for the assessment of the effects of a breach of personal data protection", the Administrator, specifying the scope of data covered by the violation in question, indicated that it also applies to health data, quoted: "The referral disclosed to an unauthorized person contained information about the identified disease entity and Further research".

The Article 29 Working Party in the guidelines on reporting personal data breaches pursuant to Regulation 2016/679, hereinafter also referred to as the "guidelines", indicated that "An important factor to be taken into account is the ease with which the party access to disclosed personal data, will be able to identify specific natural persons or match the data with other information used to identify natural persons. Depending on the circumstances, it may be possible to identify directly from the personal data concerned by the breach, without the need to collect additional information to identify the person concerned or to match the personal data to a specific person may be very difficult, but still feasible under certain conditions. Identification may be directly or indirectly possible based on disclosed data, but may also depend on the specific context of the breach and the public availability of the related personal data. This may be more relevant in the event of breaches of confidentiality and data availability. " Therefore, the above confirms the ease of identifying a specific natural person based on such data as name, address of residence or stay, PESEL number and data on health status. This is due in particular to the essence of the identification number of the Universal Electronic System for Registration of the Population. According to Art. 15 sec. 2 of the

Act of 24 September 2010 on population records (Journal of Laws of 2022, item 1191), this number uniquely identifies a natural person.

In the submitted explanations, the Administrator indicated that, after analyzing the facts of the case, a full analysis of the level of risks of threat to the rights and freedoms of data subjects (seriousness of violation) was carried out based on the risk impact assessment form adopted by the Administrator. As a result, the event was assigned a grade of 5 on a scale from 0 to 21, which classified the above-mentioned the event as "moderately severe". In accordance with the assessment methodology, the Administrator assumed that as a result of the event "Natural persons will be affected by the breach to an average extent, i.e. they may encounter certain inconveniences that are easy to overcome (time spent on re-entering information, irritation, irritation, etc.) . Nevertheless, the breach of data protection does not have significant effects on the rights and obligations of the data subject. It should be recorded in the incident register as a security incident, but is not subject to reporting to the Personal Data Protection Office ”.

In the case at hand, the Administrator found that the breach does not involve the risk of violating the rights or freedoms of the person affected. It is worth noting that the collected evidence shows that the controller, however, foresaw that the breach may involve such a risk, because, inter alia, "Conducted a visual audit, combined with collecting explanations from persons performing activities in the area of the incident, ie the doctor's office who issued a referral to a specialist clinic and [...] the Infant Jesus Clinical Hospital". Making the response to a breach dependent on the fulfillment of its potential consequences is contrary to the principle according to which the controller is to counteract the consequences of a breach or minimize its negative effects (in a situation where it is no longer justified to apply measures to prevent them). It should be emphasized that the possible consequences of the event that occurred do not have to materialize - in the content of Art. 33 sec. 1 of Regulation 2016/679, it was indicated that the mere occurrence of a breach of personal data protection, which involves the risk of violating the rights or freedoms of natural persons, implies an obligation to notify the breach to the competent supervisory authority. Therefore, the fact raised by the Administrator with the quotation: "the impact of a human factor not aimed at causing a breach of the security of data processing" is irrelevant to the Administrator's finding that there is an obligation on the part of the Administrator to report this breach of personal data protection to the President of the Personal Data Protection Office, in accordance with Art. 33 sec. 1 of Regulation 2016/679. In the judgment of September 22, 2021, file ref. no. II SA / Wa 791/21, the Provincial Administrative Court in Warsaw, indicated that: “(...) it should be emphasized that the possible consequences of

the event that occurred do not have to materialize. In the wording of Art. 33 sec. 1 of Regulation 2016/679 indicates that the mere occurrence of a breach of personal data protection, which involves the risk of violating the rights or freedoms of natural persons, implies an obligation to notify the breach to the competent supervisory authority, unless it is unlikely that the breach would result in a risk of violation of the rights or freedoms of natural persons natural persons. " The Provincial Administrative Court in Warsaw made a similar opinion in the judgment of January 21, 2022 (file reference: II SA / Wa 1353/21), indicating that "(...) the possible consequences of the event of a personal data breach do not have to materialize - as in art. . 33 sec. 1 GDPR says that the very occurrence of a breach of personal data protection, which involves the risk of violating the rights or freedoms of natural persons, implies an obligation to notify the breach to the competent supervisory authority. The circumstance raised by the Company that the breach did not result in physical damage or damage to natural persons is irrelevant for the determination of the Company's obligation to notify the President of the Personal Data Protection Office of the breach of personal data protection, in accordance with the above-mentioned recipe ".

There are also reservations about the values adopted by the Administrator in the "Personal data breach impact assessment form", in the part concerning "specific breach factors - increasing or reducing the level of risk for data subjects" and "other criteria". First of all, the value indicated in the point "Is there a high risk of violation of the rights or freedoms of the data subject / persons?", Where the Administrator entered "0", should be questioned. The adoption of such a value in this point is incomprehensible in the context of the "YES" answer given to the question "Does the data subject to the infringement, due to their characteristics and properties, have a vulnerability, indicating that they are used for illegal purposes - e.g. financial data, data enabling the fraudulent credit / loan? ". There is no doubt that the possibility of using data to extort a loan or a loan, as causing a financial loss, poses a high risk of violating the rights or freedoms of natural persons, as indicated by the guidelines of the Article 29 Working Party. by the Administrator with a value of "0" in response to the question "Was the data to which the violation relates correct and up-to-date?". As it can be assumed, the Administrator entered this value due to an error on behalf of the person whose data was disclosed to an unauthorized person. Meanwhile, due to the high possibility of identifying this person based on the other disclosed data, as shown above, the Administrator should, when answering this question, first of all take into account whether the data that allow such identification are correct and up-to-date, i.e. name, address of residence or stay, PESEL number and data on health. In the opinion of the President of the Personal Data Protection Office, the Administrator incorrectly adopted the value of "0" in response to the question "Is there a limited possibility of identifying the

data subject - e.g. due to the universality of the data? Or is there maximum certainty as to the identification of the person? ”, Pointing to the limited possibility of identifying the data subject. As has already been shown many times, the scope of the disclosed data determines the high possibility of identifying the person whose data was affected by the breach. In addition, when analyzing the risk of violating the rights or freedoms of natural persons in connection with the violation of personal data protection, the level of this risk should not be arbitrarily lowered in a situation where the violation concerns only one person, as did the Administrator by entering the value "-1" in response to the question "Does the infringement concern a small number of people, ie less than 10?". The level of this risk is determined primarily by the scope of the data covered by the breach, and not by the number of people affected by it. This is clear from the guidelines which state that "(...) depending on the nature of the personal data and the context in which they were disclosed, a breach may have serious consequences for even one person". Finally, one cannot agree with the Administrator who assumed the value "-1" in response to the question "Does the entity that obtained access to the data as a result of the breach have features / properties indicating that it is a trusted entity and it can be expected that it will not be will further use and process the data? ”. According to the guidelines, "due to the fact that the administrator is in a permanent relationship with trusted entities and may know the procedures used by them, their history and other important details concerning them - the recipient can be considered" trusted ". In other words, the administrator can trust the recipient enough to be able to reasonably expect that the party will not read the mistakenly sent data or gain access to it, and that it will follow the instruction to send it back. Even if the data has been consulted, the controller can still have confidence in the recipient that he will not take any further action with the data and that he will promptly return the data to the controller and cooperate in its recovery. In such cases, the controller may take this into account in the risk assessment following a breach - the fact that the recipient is trusted may result in a breach not having a serious effect, but that does not mean that a breach has not taken place. ' However, the administrator has not shown that there are grounds for considering an unauthorized recipient as a trusted recipient, indicated in the above-mentioned guidelines. The fact that the entity to which the data of another person has been unauthorizedly disclosed "is positively interested in the level of personal data protection as well as the patient's rights" raised by the Administrator in the "Form for assessing the effects of a breach of personal data protection" does not clearly determine the existence of this type of feature on his side.

Acceptance by the Administrator of the underestimated values in the above-mentioned areas, in accordance with the methodology adopted by him to analyze the level of risks of threat to the rights or freedoms of data subjects (severity of the

violation), had a key impact on the final assessment of the level of risk of violating the rights or freedoms of a natural person resulting from a violation of the protection of his personal data, and consequently failure to report breach of personal data protection to the President of the Personal Data Protection Office and failure to notify the data subject of this breach, pursuant to the obligations set out in Art. 33 sec. 1 and art. 34 sec. 1 of Regulation 2016/679.

In view of the above, it should be considered that as a result of the event in question, the confidentiality of the data of the person indicated in the referral to a specialist clinic was breached, which was issued to an unauthorized person (another patient). In addition, due to the wide scope of the disclosed data (including the name and PESEL registration number, as well as information on the state of health), it should be stated that as a result of the incident, there was a high risk of violating the rights or freedoms of a natural person. As the Article 29 Working Party points out in the Guidelines: “This risk exists when a breach may lead to physical harm or damage to property or non-pecuniary damage to the persons whose data has been breached. Examples of such damage include discrimination, identity theft or fraud, financial loss and damage to reputation. " In addition, the Article 29 Working Party in the Guidelines indicated that the controller, when assessing the risk to individuals resulting from the breach, should take into account the specific circumstances of the breach, including the severity of the potential impact and the likelihood of its occurrence, and recommended that the assessment should take into account the criteria indicated in these Guidelines. . In the above-mentioned The guidelines also clarify that, when assessing the risks that may arise from a breach, the controller should collectively consider the severity of the potential impact on the rights and freedoms of individuals and the likelihood of their occurrence. Of course, the risk increases when the consequences of a breach are more severe and also when the likelihood of their occurrence increases. In case of any doubts, the controller should report the violation, even if such caution could turn out to be excessive.

It should also be pointed out that disclosure to an unauthorized recipient of the personal data of another person, due to the Administrator's doctor providing him with a referral to a specialist clinic with incorrect data, is also a violation of medical confidentiality referred to in art. 40 sec. 1 of the Act of December 5, 1996 on the professions of doctor and dentist (Journal of Laws of 2021, item 790). Pursuant to this provision, the doctor is obliged to keep confidential information related to the patient and obtained in connection with the exercise of the profession. The above circumstance additionally determines the legitimacy of assuming that in connection with the violation of personal data protection in question there was a high risk of violating the rights or freedoms of the natural person affected by this violation.

It should be emphasized that, in the opinion of the President of the Personal Data Protection Office, consistently for many years, the PESEL number is a unique identifier of a person, containing a lot of information about a given person, and its disclosure to an unauthorized person may have a number of consequences for such a person.

It is worth mentioning here the Guidelines of the European Data Protection Board 01/2021 on examples regarding the notification of personal data breaches adopted on December 14, 2021, version 2.0 (hereinafter "EDPB Guidelines 01/2021"), namely example No. 14 , referring to the situation of "mistakenly sent by post highly sensitive personal data". In the aforementioned case, the social security number was disclosed, which is the equivalent of the PESEL number used in Poland. In the case at hand, the European Data Protection Board (hereinafter "EDPB") had no doubts that the disclosed data in the scope of: name and surname, e-mail address, postal address, social security number indicate a high risk of violating the rights or freedoms of natural persons ("The involvement of their [victims] social security number, as well as other, more basic personal data, further increases what can be described as high risk"). The EDPB recognizes the importance of national identification numbers (in this case the PESEL number), while stressing that this type of personal data breach, i.e. data in the form of: name and surname, e-mail address, correspondence address and social security number, requires the implementation of actions, i.e .: notification of the supervisory body and notification of the breach of data subjects.

From the last report of infoDOK (which is prepared as part of the social information campaign of the DOCUMENTS RESERVED system, organized by the Polish Bank Association and some banks, under the patronage of the Ministry of the Interior and in cooperation with, among others, the Police and the Consumer Federation) [1] shows that that in the first quarter of 2022 there were 1,915 attempts of extorting loans and credits. This means an average of 21 extortion attempts a day. Every day, attempts were made to steal someone else's data for a total of 575,000. zloty.

In turn, in the fourth quarter of 2021, attempts were made to extort 2,075 loans for a total amount of PLN 91.3 million. This is PLN 24 million more than in 2020, and the entire year 2021 in terms of numbers and amounts was significantly more dangerous than the previous one: a 17% increase in the number of fraud attempts and a 32% increase in total amounts. Moreover, as evidenced by the jurisprudence, judgments in cases of credit fraud are not uncommon and have been issued by Polish courts in similar cases for a long time - for confirmation, even the judgment of the District Court in Łęczyca of July 27, 2016 (file reference number I C 566/15), in which the fraudsters who borrowed someone else's data used the PESEL number, a fake address and an incorrect ID number (invalid). In the justification of the above-mentioned of the judgment, the Court

stated that: "In the present case, the plaintiff (...) with its seat in W. purchased the debt from (...) Spółka z ograniczoną odpowiedzialnością S.K.A. with its registered office in W. The party to the loan agreement of 5 May 2014 was a person who used the data of J. R. in an unauthorized way (...) Spółka z ograniczoną odpowiedzialnością S.K.A. based in W. transferred the amount of PLN 500 to the indicated bank account.

The key issue in the present case was the finding that the defendant did not conclude the loan agreement, which was the objection raised by the defendant throughout the proceedings.

The conducted evidence proceedings and the analysis of documents attached by the claimant result in the fact that it can be unequivocally stated that in the case under examination the defendant was not a party to the loan agreement concluded on May 5, 2014. Although it was concluded with the PESEL number of the defendant, J. R., the indicated place of residence does not correspond to the place of residence of the defendant. The defendant J. R. never lived in W. The loan amount was transferred to an account whose holder was not the defendant. On the date of concluding the loan agreement, the ID card No. (...) expired on March 15, 2014. The mobile phone number indicated on the loan agreement and its attachments is also inconsistent with the actual telephone numbers used and used by the defendant.

In the realities of the case under examination, the Court found that the defendant proved that it was not a party to the loan agreement being the subject of these proceedings. Agreements concluded by means of distance communication should require detailed, in-depth verification and such verification in the case in question leads to the conclusion that the party to the loan agreement was not the defendant ”.

The situation described above largely reflects the example No. 17 indicated in the EDPB Guideline 01/2021 showing an identity theft case. In this case, the situation is as follows: “The telephone company's contact center receives a call from someone who poses as a customer. The alleged customer is requesting the company to change the email address to which the billing information should be sent. A contact center employee confirms the customer's identity by requesting certain personal data in accordance with the company's procedures. The caller correctly indicates the fiscal number and mailing address of the desired customer (because he had access to these elements). After approval, the operator makes the requested change, and from that moment the billing information is sent to the new e-mail address. The procedure does not provide for any notification of the previous e-mail contact. The next month, an ordinary customer contacts the company, asking why they are not receiving invoices to their e-mail address, and denies any calls from him requesting a change in e-mail

contact. Later, the company realizes that the information has been sent to an illegal user and reverses the change. "

In the opinion of the EDPB, the above-mentioned the breach carries a high level of risk, as billing data may constitute information about the private life of the data subject (e.g. habits, contacts) and may lead to material damage (e.g. harassment, threats to physical integrity), and therefore necessary is both the notification of the supervisory authority as well as the notification of the data subject.

In the light of the above, it is irrelevant the fact that the Administrator claims that "The aggressive behavior of the patient towards Mr. data ". The reason indicated by the Administrator of the breach of personal data protection may not release him from the obligations specified in this regard by the provisions of art. 33 sec. 1 and art. 34 sec. 1 and 2 of Regulation 2016/679, since its consequence was the disclosure of personal data to an unauthorized person (another patient) in the scope involving a high risk of violating the rights or freedoms.

In a situation where, as a result of a breach of personal data protection, there is a high risk of violation of the rights or freedoms of natural persons, the controller is obliged to implement all appropriate technical and organizational measures to immediately identify the breach of personal data protection and promptly inform the supervisory authority, as well as persons data relate to. The administrator should fulfill this obligation as soon as possible.

Recital 85 of the preamble to Regulation 2016/679 explains: "In the absence of an adequate and prompt response, a breach of personal data protection may result in physical damage, property damage or non-material damage to natural persons, such as loss of control over own personal data or limitation of rights, discrimination, theft or falsification of identity, financial loss, unauthorized reversal of pseudonymisation, breach of reputation, breach of confidentiality of personal data protected by professional secrecy or any other significant economic or social damage. Therefore, as soon as it becomes aware of a personal data breach, the controller should notify it to the supervisory authority without undue delay, if practicable, no later than 72 hours after the breach has been discovered, unless the controller can demonstrate in accordance with the accountability principle that it is unlikely to be that the violation could result in a risk of violation of the rights or freedoms of natural persons. If the notification cannot be made within 72 hours, the notification should be accompanied by an explanation of the reasons for the delay and the information may be provided gradually without further undue delay. '

In turn, recital 86 of the preamble to Regulation 2016/679 explains: "The controller should inform the data subject without undue delay of the breach of personal data protection, if it may result in a high risk of violating the rights or freedoms of that

person, so as to enable that person to take necessary preventive actions. Such information should include a description of the nature of the personal data breach and recommendations for the individual concerned to minimize the potential adverse effects. Information should be provided to data subjects as soon as reasonably possible, in close cooperation with the supervisory authority, respecting instructions provided by that authority or other relevant authorities such as law enforcement authorities. For example, the need to minimize the imminent risk of harm will require the immediate notification of data subjects, while the implementation of appropriate measures against the same or similar data breaches may justify subsequent notification. '

By notifying the data subject without undue delay, the controller enables the person to take the necessary preventive measures to protect the rights or freedoms against the negative effects of the breach. Art. 34 sec. 1 and 2 of Regulation 2016/679 is intended not only to ensure the most effective protection of the fundamental rights or freedoms of data subjects, but also to implement the principle of transparency, which results from Art. 5 sec. 1 it. a) Regulation 2016/679 (cf. Chomiczewski Witold [in:] GDPR. General Data Protection Regulation. Comment. ed. E. Bielak - Jomaa, D. Lubasz, Warsaw 2018). Proper fulfillment of the obligation specified in art. 34 of Regulation 2016/679 is to provide data subjects with quick and transparent information about a breach of the protection of their personal data, together with a description of the possible consequences of the breach of personal data protection and the measures that they can take to minimize its possible negative effects. Acting in accordance with the law and showing concern for the interests of data subjects, the controller should, without undue delay, provide data subjects with the best possible protection of personal data. To achieve this goal, it is necessary to indicate at least the information listed in Art. 34 sec. 2 of Regulation 2016/679, which the administrator did not fulfill. Therefore, when deciding not to notify the supervisory authority and the data subjects of the breach, the administrator in practice deprived these persons of reliable information about the breach and the possibility of counteracting potential damage, provided without undue delay.

When applying the provisions of Regulation 2016/679, it should be borne in mind that the purpose of this regulation (expressed in Article 1 (2)) is to protect the fundamental rights and freedoms of natural persons, in particular their right to the protection of personal data, and that the protection of natural persons in connection with the processing of personal data is one of the fundamental rights (first sentence of Recital 1). In case of any doubts, e.g. regarding the performance of obligations by administrators - not only in a situation where there has been a breach of personal data protection, but also when developing

technical and organizational security measures to prevent them - these values should be taken into account in the first place. The above reasoning is confirmed by the judgment of the Provincial Administrative Court in Warsaw of September 22, 2021 (file reference number II SA / Wa 791/21), in which the Court, when deciding on the imposition of an administrative fine in connection with the violation of the provisions on the protection of personal data, referred to the above-mentioned of the above issue, additionally pointing out that "When assessing whether there are risks of violating human rights or freedoms, the administrator should take into account all possible damage and harm that may result from a given event for natural persons (such as: S. Jandt [in:] DS.-GVO ..., edited by J. Kuhling, B. Buchner, p. 617; Y. Reif [in:] DS.- GVO ..., edited by P. Gola, p. 496). They may in particular consist in losing control over your own personal data, negative image consequences, the possibility of another person concluding contracts using the personal data of another natural person, financial losses or, finally, negative social perception that may be a consequence of making some personal data public. For the risk to occur, it is not necessary for the final loss or harm resulting from a given breach of personal data protection (as above, p. 616) ”.

Consequently, it should be stated that the Administrator did not notify the supervisory body of the breach of personal data protection pursuant to the obligation under Art. 33 sec. 1 of Regulation 2016/679 and did not notify the data subject without undue delay of a breach of data protection, in accordance with art. 34 sec. 1 of the Regulation 2016/679, which means the Administrator's violation of these provisions.

Pursuant to Art. 34 sec. 4 of Regulation 2016/679, if the controller has not yet notified the data subject about the breach of personal data protection, the supervisory authority - taking into account the probability that this breach of personal data protection will result in a high risk - may request it or may state that that one of the conditions referred to in sec. 3. In turn, from the content of Art. 58 sec. 2 it. e) of Regulation 2016/679 shows that each supervisory authority has the right to remedy the need for the controller to notify the data subject about a breach of data protection.

Moreover, pursuant to Art. 58 sec. 2 it. i) of 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 of Regulation 2016/679, an administrative fine under Art. 83 of the Regulation 2016/679, depending on the circumstances of the specific case. The President of the Personal Data Protection Office states that in the case under consideration there are premises justifying the imposition of an administrative fine on the Administrator pursuant to Art. 83 sec. 4 it. a) of Regulation 2016/679 stating, inter alia, that the breach of the administrator's obligations referred to in art. 33 and 34 of Regulation 2016/679, is subject to an administrative

fine of up to EUR 10,000,000, and in the case of an enterprise - up to 2% of its total annual worldwide turnover from the previous financial year, with the higher amount being applicable. However, with Art. 102 paragraph. 1 of the Act of May 10, 2018 on the Protection of Personal Data (Journal of Laws of 2019, item 1781), it follows that the President of the Personal Data Protection Office may impose, by way of a decision, administrative fines of up to PLN 100,000 on: units of the public finance sector, referred to in Art. 9 points 1-12 and 14 of the Act of 27 August 2009 on public finance, a research institute or the National Bank of Poland. From the paragraph 3 of this article also shows that the administrative pecuniary penalties referred to, inter alia, in para. 1, the President of the Office shall impose on the basis and under the conditions specified in Art. 83 of the Regulation 2016/679.

Pursuant to art. 83 sec. 2 of Regulation 2016/679, administrative fines shall be imposed, depending on the circumstances of each individual case, in addition to or instead of the measures referred to in Art. 58 sec. 2 it. a) - h) and it. j) Regulation 2016/679. When deciding to impose an administrative fine on the Administrator, the President of the Personal Data Protection Office - pursuant to Art. 83 sec. 2 it. a) - k) of Regulation 2016/679 - took into account the following circumstances of the case, which necessitate the application of this type of sanction in the present case and which had an aggravating effect on the amount of the fine imposed:

a) The nature and gravity of the breach (Article 83 (2) and improving the security of personal data processing. When reporting a breach to the supervisory authority, the administrators inform the President of the Personal Data Protection Office whether, in their opinion, there is a high risk of violation of the rights or freedoms of data subjects and - if such a risk occurred - whether they provided relevant information to natural persons affected by the breach. In justified cases, they can also provide information that, in their opinion, notification is not necessary due to the fulfillment of the conditions set out in Art. 34 sec. 3 it. a) - c) of Regulation 2016/679. The President of the Personal Data Protection Office (UODO) verifies the assessment made by the controller and may - if the controller has not notified the data subjects - request such notification from him. Notifications of a breach of personal data protection allow the supervisory authority to react appropriately, which may limit the effects of such breaches, because the controller is obliged to take effective measures to protect natural persons and their personal data, which on the one hand will allow for the control of the effectiveness of the existing solutions, and on the other for the assessment of modifications and improvements to prevent irregularities similar to those covered by the infringement. In addition, it should be emphasized that failure to notify the data subject about a breach of the protection of his personal data

may lead to material or non-pecuniary damage, and the probability of their occurrence is high. In the opinion of the President of the Personal Data Protection Office, the importance and nature of the breach is also influenced by the ease of identification of a specific natural person based on such data as name, address of residence or stay, PESEL number and health data, and the fact that, along with the disclosure of personal data to the wrong recipient, there was a breach of secrecy. ecology. According to Art. 40 sec. 1 of the Act of December 5, 1996 on the professions of doctor and dentist (Journal of Laws of 2021, item 790), the doctor is obliged to keep confidential information related to the patient and obtained in connection with the exercise of the profession.

b) Duration of the infringement (Article 83 (2) and (a) of Regulation 2016/679); The President of UODO considers the long duration of the infringement to be an aggravating circumstance. Several months have elapsed from the Administrator receiving information about the breach of personal data protection until the date of issuing this decision, during which the risk of violation of the rights or freedoms of the person affected by the breach could have materialized, and which could not be prevented by such person due to the Administrator's failure to fulfill the obligation notify her of the breach.

c) Intentional nature of the breach (Article 83 (2) and (b) of Regulation 2016/679); the Administrator made a conscious decision not to notify the President of the Personal Data Protection Office and the data subject about the breach, despite having received information about the incident from the Ombudsman The patient and the letters addressed to him by the President of the Personal Data Protection Office indicating the possibility of a high risk of violation of the rights or freedoms of the person affected by the violation in this case. Above the Administrator's obligations under Art. 33 sec. 1 and 3 and article. 34 sec. 1 and 2 have not been implemented. Such omission in this respect, despite the obligation to act "without undue delay", made it impossible for a natural person to take actions as soon as possible to protect himself against any negative effects of the breach, which in turn has an impact on their effectiveness if this is done. obligation by the Administrator.

d) The degree of cooperation with the supervisory authority in order to remove the infringement and mitigate its possible negative effects (Article 83 (2) and This assessment concerns the Administrator's reaction to the letters of the President of the Personal Data Protection Office indicating the possibility of a high risk of violating the rights or freedoms of the person affected by the violation in this case. Correct, in the opinion of the President of the Personal Data Protection Office (UODO), the actions (notification of the infringement to the President of the Personal Data Protection Office and notification of the person affected by the infringement) were not taken by the Administrator even after the President of the Personal Data Protection Office

initiated the administrative procedure in the case.

e) The categories of personal data concerned by the infringement (Article 83 (2) and (g) of Regulation 2016/679); Personal data made available to an unauthorized person, in addition to the data on the name, address of residence or stay and PESEL number, also include data belonging to special categories of personal data referred to in art. 9 of Regulation 2016/679, i.e. health data including information on the diagnosis and purpose of the advice. Their wide scope entails a high risk of violating the rights or freedoms of natural persons. In addition, it should be noted that these data fall within the scope of information related to the patient, obtained by a physician in connection with his profession, and as such are subject to the obligation of keeping them confidential.

f) The way in which the supervisory authority learned about the breach (Article 83 (2) and (h) of Regulation 2016/679); About the breach of personal data protection being the subject of this case, i.e. disclosure of personal data processed by the Administrator to an unauthorized person, President The Personal Data Protection Office has not been informed in accordance with the procedure provided for in such situations under Art. 33 of Regulation 2016/679 - this information was received from the Patient Ombudsman. The fact that there is no information about a breach of data protection coming from the controller obliged to provide such information to the President of the Personal Data Protection Office should be considered as incriminating this controller.

When determining the amount of the administrative fine, the President of the Personal Data Protection Office (UODO) considered as mitigating circumstances reducing the amount of the fine:

a) the number of injured data subjects (Article 83 (2) and (a) of Regulation 2016/679) - the infringement concerned one identifiable natural person; 83 (2) and (e) of Regulation 2016/679) - no previous infringements committed by the administrator were found.

The sanctions in the form of an administrative fine, as well as its amount, were not influenced in any way by the other sanctions indicated in Art. 83 sec. 2 of Regulation 2016/679, the circumstances:

a) actions taken to minimize the damage suffered by data subjects (Article 83 (2) and (c) of Regulation 2016/679) - in this case, no damage was found to be caused by the person affected by the infringement, therefore the Administrator was not obliged to take any actions aimed at minimizing them;

b) the degree of responsibility of the controller, taking into account technical and organizational measures implemented by him

pursuant to Art. 25 and 32 (Art.83 (2) and by the administrator with technical and organizational measures;

c) compliance with previously applied measures in the same case, referred to in Art. 58 sec. 2 of Regulation 2016/679 (Article 83 (2) and Regulation 2016/679) - in this case, the President of the Personal Data Protection Office has not previously applied the measures referred to in the aforementioned provision;

(d) 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) and (j) of Regulation 2016/679) - the Administrator does not apply approved codes of conduct or approved certification mechanisms;

e) financial benefits or losses obtained directly or indirectly as a result of the infringement (Article 83 (2) and (k) of Regulation 2016/679) - it was not found that the controller would obtain any benefits or avoid financial losses due to the infringement.

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 is effective, proportionate and dissuasive in this individual case.

It should be emphasized that the penalty will be effective if its imposition will result in the Administrator fulfilling his obligations in the field of personal data protection in the future, in particular with regard to reporting a personal data breach to the President of the Personal Data Protection Office and notifying about a breach of personal data protection. affected by the infringement. The application of an administrative fine in this case is necessary considering also the fact that the Administrator ignored the fact that we are dealing with a breach of data protection both when the event occurs as a result of deliberate action and when it is caused inadvertently.

In the opinion of the President of the Personal Data Protection Office, the administrative fine will fulfill a repressive function, as it will be a response to the Administrator's violation of the provisions of Regulation 2016/679. It will also fulfill a preventive function; in the opinion of the President of the Personal Data Protection Office (UODO), he will indicate to the administrator in question and to other data administrators the reprehensibility of disregarding the obligations of administrators related to the occurrence of a breach of personal data protection, and aimed at preventing its negative and often severe consequences for the persons affected by the breach, as well as removal these effects or at least limit them.

In connection with the above, it should be noted that the administrative fine in the amount of PLN 10,000 (say: ten thousand zlotys) meets the conditions referred to in Art. 83 sec. 1 of Regulation 2016/679 due to the seriousness of the infringement found in the context of the basic objective of Regulation 2016/679 - protection of fundamental rights and freedoms of natural

persons, in particular the right to the protection of personal data. At the same time, the amount of the administrative fine imposed by this decision on the administrator who is a unit of the public finance sector (an independent public health care institution - indicated in art.9 point 10 of the Act of 27 August 2009 on public finances) is within the scope specified in art. 102 paragraph 1 of the Act of May 10, 2018 on the Protection of Personal Data (Journal of Laws of 2019, item 1781) to the value of PLN 100,000.

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

[1] https://www.zbp.pl/raporty-i-publikacje/raporty-cykliczne/raport-infodok

2022-07-20