THE CHAIRMAN OF PERSONAL DATA PROTECTION

Warsaw, day 12

November

2020

DECISION

DKN.5101.25.2020

Based on Article. 104 § 1 of the Act of 14 June 1960 Code of Administrative Procedure (Journal of Laws of 2020, item 256, as amended) in connection with Art. 7 and art. 60 of the Act of May 10, 2018 on the Protection of Personal Data (Journal of Laws of 2019, item 1781) and pursuant to Art. 58 sec. 2 lit. b) and e), in connection with Art. 5 sec. 1 lit. f, art. 24 sec. 1, art. 25 sec. 1, art. 32 sec. 1 lit. d, art. 32 sec. 2, art. 33 paragraph 1 and art. 34 sec. 1 of the Regulation of the European Parliament and of the EU Council 2016/679 of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46 / EC (general data protection regulations) (Journal of Laws UE L 119 of 04/05/2016, p. 1, as amended), after conducting administrative proceedings regarding the processing of personal data by U. Sp. z o.o. based in G., President of the Personal Data Protection Office,

1) finding an infringement by U. Sp. z o.o. based in G., the provisions of art. 5 sec. 1 lit. f, art. 24 sec. 1, art. 25 sec. 1, art. 32 sec. 1 lit. d, art. 32 sec. 2, art. 33 paragraph 1 and art. 34 sec. 1 of Regulation 2016/679 of the European Parliament and of the Council of the EU and of the EU Council 2016/679 of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46 / EC (general regulation on data protection) (Journal of Laws UE L 119 of 04.05.2016, p. 1 as amended), gives a reminder to U. Sp. z o.o. based in G .;

2) orders to notify data subjects of a breach of personal data protection in order to provide them with the information required in accordance with art. 34 sec. 2 of Regulation 2016/679 of the European Parliament and of the Council of the EU and of the EU Council 2016/679 of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46 / EC (general regulation on data protection) (Journal of Laws UE L 119 of 04.05.2016, p. 1 as amended), i.e .:

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

2) name and surname and contact details of the data protection officer or designation of another contact point from which more

information can be obtained;

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

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

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

Justification

The Office for Personal Data Protection received a letter from the Poviat State Sanitary Inspector in G. (hereinafter also referred to as "PPIS in G.") with information about the public disclosure of the list containing the addresses of residence of persons who are in quarantine ordered by the administrative decision of PPIS in G. and quarantine mandatory in connection with crossing the country border, as well as address details of people undergoing home isolation in connection with the confirmed infection with the SARS-CoV-2 coronavirus. According to the information provided, personal data regarding the above-mentioned persons were made available by the State Poviat Sanitary Inspector in G. to the following entities: the Poviat Police Headquarters in G., the Head of the Polish Post in G., Municipal and Communal Social Assistance Centers in the poviat The Sanitary Inspector in G. stated that he had undertaken explanatory activities on his own, as a result of which he stated that the source of the disclosure of the above-mentioned personal data was not the Sanitary Inspection in G ..

The President of the Personal Data Protection Office (hereinafter also referred to as the "President of the Personal Data Protection Office"), in a letter of [...] April 2020, asked the District Police Commander in G. to clarify, inter alia, whether he was aware of the incident described at: [...] and whether, in connection with this incident, an analysis was carried out in terms of a breach of personal data protection people. Moreover, the President of the Personal Data Protection Office called for clarification whether, as a result of the conducted analysis, a breach of personal data protection has been found, for what reasons it has not been reported to the supervisory authority so far. In a reply of [...] April 2020 (reference number [...]), the Poviat Police Commander in G. explained in particular that:

1) lists with personal data of quarantined persons were sent from the Sanitary and Epidemiological Station in G. to the Poviat Police Headquarters in G. electronically via e-PUAP to the e-PUAP KPP G address box;

2) due to the prevailing epidemiological situation, requests for information on the addresses of quarantined persons from the following entities were submitted to the Poviat Police Headquarters in G., G., U. Sp. z o. o. w G .. The need to obtain the

requested personal data was justified by the fear of exposing employees to the risk of COVID-19;

3) responses to requests submitted by the above-mentioned entities were sent electronically to the e-mail addresses indicated by them. Data was sent in the form of addresses of persons subject to quarantine, including: name of the town, street, number of property / premises, in the form of a table with the name: "CURRENT (as of ... at ...) LIST OF PEOPLE COVERED BY THE QUARANTINE IN CONNECTION WITH THE THREAT OF CORONAVIRUS";

4) the list of addresses of quarantined persons placed in the Messenger internet communicator is most likely prepared as of [...] April 2020. The photo in the M instant messenger and the article in the indicated link shows that the list was printed in a traditional paper form in vertically and then photographed. The graphic design of the documents is divergent. At the Poviat Police Headquarters in G. the list of quarantined persons was drawn up horizontally and was not printed. On the other hand, a printed list in a vertical layout appeared on the Internet, in the upper part of the document the table header overlaps the list of addresses.

Then the President of the Personal Data Protection Office addressed letters of [...] April 2020 to the County Commander of the State Fire Service in G., the Municipal Social Assistance Center in G., U. Sp. z o.o. with its seat in G. (hereinafter also referred to as the "Company" or "administrator") and a letter of [...] May this year. to the Housing Cooperative in G., with the same questions as to the Poviat Police Commander in G., additionally indicating the correct ways of reporting a breach of personal data protection to the supervisory body. All these entities, with the exception of the Company, stated that, as a result of internal investigations, they did not find a breach of personal data protection in their organizations regarding the disclosure of data of persons who are in quarantine, ruled by the administrative decision of the PPIS in G., and a mandatory quarantine in connection with crossing the border. country, as well as address details of people undergoing home isolation in connection with the confirmed infection with the SARS-CoV-2 coronavirus.

In responses to the calls of [...] April and [...] May 2020, U. Sp. z o.o. with its seat in G., letters from [...] and [...] of May this year. (reference number [...] and [...]), explained in particular that:

received "lists of quarantine places in the city and the commune of G." only by electronic means from the Poviat Police Headquarters in G .. The lists were sent from [...] March to [...] April 2020, with varying frequency, to an individual address e-mail address of an employee of the Company These lists included only administrative (police) addresses, they did not include names, surnames and other data allowing the identification of a natural person;

The lists were submitted to the authorized employees of Zakład Oczyszczania Miasta, who were to verify whether the waste was to be collected in a given period from the places that appear on the above-mentioned lists. The above was dictated by the protection of the life and health of the Company's employees (employees of Zakład Oczyszczania Miasta), minimizing the risk of their contact with the risk factors associated with coronavirus while performing their work duties;

on [...] April 2020, the above-mentioned list was printed. In the course of performing employee duties, the person responsible on that day for supervision of the printed list left it for a short time without proper supervision (the list was on the person's desk, and the person turned to perform other activities in another part of the same room). At that time, there was also another employee of the Company in this room - a driver in Zakład Oczyszczania Miasta, who, taking advantage of the fact that the person responsible for supervising the printed list had his back directed at him, copied (recorded in the form of a photo) this list. The driver was to be informed by the person supervising the printed list whether, as part of his work, waste was to be collected from places that appear on the above-mentioned list. Then, this driver made the photos so made available to at least one person. The findings of the Company show that it was certainly another employee of the Company, also a driver at Zakład Oczyszczania Miasta (this driver was also to be informed whether, as part of his work, waste was to be collected from places that appear on the above-mentioned list);

leaving without the required supervision and improper securing of the documentation covered by special protection rules by the person responsible on that day for supervision of the printed list was classified by the administrator as failure to comply with the established organization and order in the work process, for which the person was issued a fine reprimand;

Recording by the driver of the City Cleansing Plant in the form of a photo of the documentation covered by special protection rules (list of quarantined addresses) and unauthorized, unauthorized sharing of photos taken in this way at least to one person was classified by the administrator as a serious breach of basic employee duties and resulted in the termination of the employment contract with the driver in disciplinary mode;

the abovementioned persons committed violations that resulted in the above-mentioned consequences. In the opinion of the Company, these violations were the result of failure to comply with the procedures established in the Company, however, at the time of providing the answers, it cannot be concluded that they fulfill the criteria of a violation of personal data protection as defined in Art. 4 point 12 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 data protection) subject to notification to the President of the Personal Data Protection Office.

In connection with the explanations provided by the administrator, in a letter of [...] September 2020 (ref. DKN.5101.25.2020), the President of the Office for Personal Data Protection initiated ex officio administrative proceedings regarding the possibility of infringement by U. Sp. z o.o. based in G., as the data controller, obligations under the provisions of Regulation 2016/679, i.e. art. 5 sec. 1 lit. f, art. 24 sec. 1, art. 25 sec. 1, art. 32 sec. 1 lit. d, art. 32 sec. 2, art. 33 paragraph 1 and art. 34 sec. 1, in connection with a breach of the protection of personal data of persons subject to medical quarantine by making available to unauthorized recipients a list containing the addresses of persons subject to medical quarantine. In addition, in this letter, the President of the Personal Data Protection Office summoned the administrator, inter alia, to clarify whether, while establishing the procedures related to the processing of personal data regarding the addresses of persons quarantined in connection with the threat of coronavirus, received from the Poviat Police Headquarters in G., the administrator conducted an analysis of the distribution method of the above-mentioned data in electronic and paper version (including storage on a desk) in terms of risks related to the loss of confidentiality of these data and to inform about the result of this analysis, or to indicate the reasons for withdrawing from its performance.

In response to the notice of initiation of the administrative procedure contained in the letter of [...] September 2020 ([...]), the controller explained, inter alia, that it had carried out an appropriate risk analysis, as set out in Annex 2 to the letter in question.

In a letter of [...] September 2020, the President of the Personal Data Protection Office again called on the Company to clarify whether, by establishing the procedures related to the processing of personal data regarding the addresses of persons quarantined in connection with the coronavirus threat, received from the Poviat Police Headquarters in G., the administrator carried out an analysis of the distribution method above data in electronic and paper version (including storage on a desk) in terms of risks related to the loss of confidentiality of these data and to inform about the result of this analysis, or to indicate the reasons for abandoning its performance, indicating that the analysis presented in the letter from [...] September this year. does not refer to the question on this issue contained in the letter of the President of the Personal Data Protection Office of [...] September 2020.

U. Sp. z o.o. based in G., in a letter of [...] September 2020, stated that "(...) when establishing procedures related to the processing of lists of quarantine facilities in the city and commune, G. performed an analysis, a copy of which was sent with

the Company's letter of [...] September 2020. In the course of this analysis, circumstances related to non-compliance by processors with the above-mentioned lists of procedures in force in the Company and circumstances related to the theft or removal of data by employees or associates. In both cases, the methods of securing data were taken into account, taking into account the channels of their distribution, i.e. e-mail correspondence and printouts. In each of these cases, as well as in the case of processing other data, the group of persons processing the above-mentioned the lists at each stage of their distribution were limited to the necessary minimum and other rules resulting from the Information Security Policy were applied.

The conclusion of this analysis was that the risks related to the processing of the above-mentioned the lists, including with regard to the possible loss of confidentiality, were at an average level. There was no high probability of causing a high risk of violating the rights or freedoms of natural persons. Therefore, an impact assessment of the planned processing operations on the protection of personal data has not been carried out. "

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

The EU legislator in art. 4 point 1 of Regulation 2016/679 included a legal definition of the concept of "personal data". According to it, "personal data" means any information relating to an identified or identifiable natural person ("data subject"). An identifiable natural person is a person who can be directly or indirectly identified, in particular on the basis of an identifier such as name and surname, identification number, location data, internet identifier or one or more specific physical, physiological, genetic, mental factors, the economic, cultural or social identity of a natural person. Recital 26 of Regulation 2016/679 indicates that data protection rules should apply to any information relating to an identified or identifiable natural person. In order to determine whether a natural person is identifiable, consideration should be given to any reasonably likely means (including the segregation of entries for the same person) that are reasonably likely to be used by the controller or another person for the direct purpose of or indirectly identifying a natural person. In order to determine whether a method can reasonably be used to identify an individual, all objective factors such as the cost and time needed to identify an individual should be taken into account, and the technology available at the time of data processing as well as technological advances should be taken into account. The data protection principles should therefore not apply to anonymous information, that is to say, information which does not relate to an identified or identifiable natural person, or to personal data rendered anonymous in such a way that data subjects cannot be identified at all or can no longer be identified. Therefore, this Regulation does not

apply to the processing of such anonymous information, including processing for statistical or scientific purposes.

As it results from the information provided by the State Poviat Sanitary Inspector in G. and the Poviat Police Headquarters in G., the document made available to unauthorized recipients contained a list of addresses at which persons who were in quarantine ordered by the administrative decision of PPIS in G. and compulsory quarantine in connection with with crossing the country border, as well as address details of people undergoing home isolation in connection with the confirmed infection with the SARS-CoV-2 coronavirus. The list included: the name of the town, street name, property / apartment number. In the explanations submitted, the administrator stated that these lists only included administrative (police) addresses, and did not include names, surnames and other data allowing the identification of a natural person.

In the opinion of the President of the Personal Data Protection Office, it is impossible to agree with the position of the administrator. When discussing the definition of personal data, it should be noted that the above-mentioned conditions for recognizing the processed information as personal data, i.e. (1) information (2) relating to (3) an identified or identifiable natural person (4), are the same as those that applied to land repealed by Regulation 2016/679 of Directive 95/46 / EC. Relevant guidance on the application and interpretation of the concept of personal data can be found in Opinion 4/2007 on the concept of personal data issued by the Art. 29, which included the Inspector General for Personal Data Protection, whose legal successor is the President of the Office for Personal Data Protection.

Considering the element of the first premise, i.e. (1) information, the President of UODO indicates that the Poviat Police Commander in G. in a letter of [...] April 2020, explained that he provided the Company with address information about persons subject to quarantine, including: name of the town, street, property / apartment number. It should be emphasized that in the case in question, the value of information is also given by the title appearing on the list made available to unauthorized recipients, ie "CURRENT (as at .... at ....) LIST OF PEOPLE COVERED BY THE QUARANTINE IN CONNECTION WITH THE THREAT OF CORONAVIRUS".

In turn, to be considered personal data, information must (2) relate to a natural person (be related to a natural person). As indicated by the Working Party of Art. 29 in its Opinion 4/2007 on the concept of personal data, this link must be examined in the light of three independent circumstances, ie content, purpose or effect. These circumstances do not have to be combined. This means that the information does not have to "focus" on someone to be considered as relevant. Therefore, the question of whether or not data relates to a specific person should be considered on a case-by-case basis. While the address information,

based on its content itself, is difficult to associate with a natural person (the address literally applies to real estate), however, looking through the prism of the purpose and effect, it should be considered that this information, along with information about being in medical quarantine, concerns a person physical. A "purpose" occurs when data is or can be used, taking into account all the circumstances of a case, to evaluate an individual, treat him or her in a particular way, or influence his status or behavior. Information can also be considered as relating to a natural person if its use will have an "effect" on its rights and interests, taking into account all the circumstances of the case. A potential effect need not be a major influence. It is enough for a certain person to be treated differently from others as a result of the processing of such data. According to the administrator's explanations, the information on the addresses of the quarantined persons was obtained in order to protect the life and health of the Company's employees (employees of Zakład Oczyszczania Miasta).

The third and fourth prerequisites for the concept of personal data require that the information concerns (3) an identified or identifiable (4) natural person. The ability to identify a given person does not have to be tantamount to finding out their surname, it is enough to be able to indicate them or distinguish them from a specific community. The doctrine indicates that "[r] the risk related to the assessment of specific information held by the administrator in terms of its eligibility as a personal data is borne by the administrator, also when he provides certain information on the basis of which he cannot identify himself, even unconsciously. , entity or entities (e.g. by making it available on the Internet), which will be able to make such identification with the use of additional information available to them. In such a situation, the act of sharing will already be the processing of personal data, due to the fact that the information provided will be personal data. This statement can be derived directly from the phrase 3 of recital 26, stating the likely methods of identification used not only by the administrator, but also by another person ”(Bielak-Jomaa Edyta (ed.), Lubasz Dominik (ed.), GDPR. General Data Protection Regulation. Comment). As already indicated above, the possibility of identifying a given person does not have to be the same as finding out his surname. In the opinion of the President of the Personal Data Protection Office, publishing the list of addresses at which persons subject to medical quarantine are located allows for the identification of specific persons by persons in a specific community, e.g. neighbors or family.

The view of the Company that "(...) [in] these lists only included administrative (police) addresses, they did not include names, surnames and other data allowing the identification of a natural person", one cannot agree also because, as it has already been the above-mentioned list, made available to unauthorized recipients, contained the following title: "CURRENT (as of ... at

...) LIST OF PEOPLE COVERED BY THE QUARANTINE IN CONNECTION WITH THE RISK OF CORONAWIRUS".

Therefore, it should be stated that the controller, having obtained information that a person under quarantine resides at the indicated address, also processed data of a specific category regarding the health of the person subject to it.

Pursuant to Art. 4 point 15 of Regulation 2016/679 "data concerning health" means personal data concerning the physical or mental health of a natural person - including the use of health care services - revealing information about his or her health status. In addition, recital 35 of Regulation 2016/679 clarifies that personal data relating to health should include all data related to the health status of the data subject which reveal information about the past, present or future physical or mental health of the data subject. Such data include, among others information about a given natural person collected during his registration for healthcare services or during the provision of healthcare services to him, information from laboratory or medical tests of parts of the body or body fluids, including genetic data and biological samples; and any information, for example about the disease, disability, disease risk, medical history, clinical treatment, or the physiological or biomedical condition of the data subject, irrespective of its source, which may be, for example, a doctor or other healthcare professional.

Pursuant to Art. 34 point 2 of the Act of 5 December 2008 on preventing and combating infections and infectious diseases in humans (Journal of Laws of 2019, item 1239, i.e.) people who were exposed to an infectious disease or were in contact with a biological source the pathogen, and they do not show disease symptoms, are subject to compulsory quarantine or epidemiological supervision, if so decided by the sanitary inspection authorities for a period not longer than 21 days, counting from the day following the last day of exposure or contact, respectively.

In the light of the content of recital 35, it should be clearly stated that the information on quarantining a person who was exposed to an infectious disease or who was in contact with a source of a biological pathogen constitutes data on the health of that person, due to the risk of disease. It is irrelevant in this context whether the person shows symptoms or not.

In connection with the above, it should be stated that U. Sp. z o.o. based in G., as the controller, processed within the meaning of Art. 4 point 2 of Regulation 2016/679, personal data regarding: the name of the city, street name, property / premises number and health data. Therefore, the Company is the addressee of the obligations arising from the provisions of Regulation 2016/679.

Article 5 of Regulation 2016/679 lays down rules regarding 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 ensuring adequate security of personal data, including protection against unauthorized or unlawful processing and accidental loss, destruction or damage, by appropriate technical or organizational measures ("confidentiality and integrity") . Further provisions of the regulation make this principle more specific.

Pursuant to Art. 24 sec. 1 of Regulation 2016/679, taking into account the nature, scope, context and purposes of processing as well as the risk of violating the rights or freedoms of natural persons of varying probability and seriousness, the controller implements appropriate technical and organizational measures to ensure that the processing is carried out in accordance with this Regulation and to be able to demonstrate it . These measures are reviewed and updated as necessary.

Pursuant to Art. 25 sec. 1 of Regulation 2016/679, both when determining the methods of processing and during the processing itself, the controller 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. d of 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, regular testing, measurement and evaluation of the effectiveness of technical and organizational measures to ensure the security of processing, where appropriate.

Pursuant to Art. 32 sec. 2 of Regulation 2016/679, the administrator, 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.

As indicated in art. 24 sec. 1 of Regulation 2016/679, 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 severity are factors that the controller is obliged to take into account in the process of building a data protection system, also in particular from the point of view of other obligations indicated in art. 25 sec. 1, 32 sec. 1 or 32 sec. 2 of Regulation 2016/679. Any legal and organizational changes affecting the processing of personal data are circumstances to which the administrator should pay special attention, and any

significant changes in this respect should be preceded by an appropriate analysis. The context of the processing is a factor that the controller must address in the process of determining the likelihood and severity of the risk of violating the rights or freedoms of natural persons (recital 78 of Regulation 2016/679). In the present case, the circumstances related to the processing of the personal data concerned by the infringement concern the global threat and sense of fear related to the epidemiological situation. Such a social situation and potential harm to a natural person related to the disclosure of information related to it are one of the elements that the controller should take into account in the risk analysis (recital 75 of Regulation 2016/679). As already explained above, the address together with the information about being in medical quarantine determines the classification of published data as data of a special category. In view of the indicated context, the administrator should, in particular, take into account the risk related to inconveniences that are difficult to overcome, such as discrimination, social ostracism, a sense of stigmatization, stress, or potential material losses related to the negative reaction of the community in which the person operates. The occurrence of such threats due to the scale of the epidemic, in the opinion of the President of the Personal Data Protection Office, is highly predictable for each administrator and should be taken into account as one of the factors required by Regulation 2016/679 in the process of assessing the adequacy of technical and organizational measures to properly protect processing of personal data.

The administrator, despite the expressed position that the data in question does not constitute data allowing the identification of a natural person, as indicated in the explanations, decided to protect them, including presenting the risk analysis of [...] March 2020 relating to the lists of quarantine facilities in the city and the commune of G .. In the letter of [...] September 2020, the Company also indicated that the conclusion of this analysis indicates an average level of risk of loss confidentiality of this data, and there was no high probability of causing a high risk of violating the rights or freedoms of natural persons.

As it results from the submitted risk analysis, the administrator pointing to threats in the form of breach of confidentiality of data on an average level refers to the item entitled "theft or removal of data by employees or associates". For this threat, safeguards have been indicated, in the form of obliging employees to comply with procedures, signing statements or confidentiality agreements, statements about reading the provisions on the protection of personal data, signing relevant authorizations, periodic training in the field of personal data, as well as equipping the rooms with a system burglar alarm and data encryption.

In view of the provisions formulated in this way in the risk analysis, the President of the Personal Data Protection Office, in the notice of initiation of the procedure and again in the letter of [...] September 2020, called the Company to clarify whether, when

establishing the procedures related to the processing of personal data concerning the addresses of persons subject to quarantine in connection with coronavirus threat, conducted an analysis of the distribution method of the above-mentioned data in electronic and paper version (including storage on a desk) in terms of risks related to the loss of confidentiality of these data and to inform about the result of this analysis, or to indicate the reasons for abandoning its performance, indicating that the analysis presented in the Company's letter from [...] September 2020 does not refer to this issue in its content.

U. Sp. z o.o. based in G., in a letter of [...] September 2020, stated that the analysis took into account the circumstances related to the non-compliance by processors with the abovementioned lists of procedures in force in the Company and circumstances related to the theft or removal of data by employees or associates. In both cases, the methods of securing data were taken into account, taking into account the channels of their distribution, i.e. e-mail correspondence and printouts. In each of these cases, as well as in the case of processing other data, the group of persons processing the above-mentioned the lists at each stage of their distribution were limited to the necessary minimum and other rules resulting from the Information Security Policy were applied.

In the opinion of the President of the Personal Data Protection Office, the security measures indicated in the analysis by the administrator are general formulations and do not refer to specific events related to activities undertaken by authorized employees. In the present case, the confidentiality of the processed data was breached in the course of the performance of the employee duties of the person responsible for supervising the printed list left on the desk without proper supervision. During this time, another employee, who was the driver, recorded the list in the form of a photo and shared it with another person. The driver was to be informed by the person supervising the printed list whether, as part of his work, waste was to be collected from places that appear on the above-mentioned list.

In the above circumstances, the employee was not the recipient of the entire list, which was supervised by the designated employee, therefore it should be stated that the administrator applied the principle of minimization, because for the performance of the driver's official activities, the necessary scope of information that he had to have at his disposal were only those residential addresses. from which waste is collected by it.

Taking into account these circumstances and the analysis carried out by the administrator, it should be expected that the administrator, when implementing the procedure for providing such information, will make a detailed analysis, e.g. the legitimacy of printing such a list, and if he chooses to do so, then it will make an appropriate analysis of the organizational and

technical measures to be taken. reduce the risk of breach of confidentiality of data included in the list. In a letter of [...] May 2020, the Company presented an extract from the information security policy of [...] May 2018, part of which is a list of physical, technical and organizational personal data protection measures applied by the data controller. As part of the physical measures, it has been indicated, inter alia, that in the case of processing data files traditionally (manually) in a room where unauthorized persons may be present to process such data (e.g. customers or other employees), the processing is carried out in such a way that unauthorized persons they did not have access to this data. These provisions and the entire policy are related to confidentiality statements and authorizations to process data issued to employees by the administrator. Bearing in mind that these provisions are largely general in nature, they cannot be assessed unequivocally in terms of the application of adequate technical and organizational measures as part of the processing of data included in the list of addresses of persons in quarantine.

In the opinion of the President of UODO, in the risk analysis, the controller should take into account both the specific nature of the data being processed, which has already been clearly indicated by the President of UODO, and the human factor, which is one of the sources of risk in the process of personal data processing, in accordance with Art. 24 sec. 1 and art. 32 sec. 1 of Regulation 2016/679 and is a basic element reflecting the intrinsic essence of the personal data protection system. When mentioning the human factor, one should have in mind, inter alia, recklessness (groundless assumption that no damage will occur) or carelessness (the employee does not anticipate the possibility of damage, although in the circumstances of the case he could and should have foreseen its occurrence). As indicated in the jurisprudence, it is typical for employment relationships to cause damage due to unintentional fault, which is usually the result of the employee's lack of due diligence in the performance of employee duties (see judgments of the Supreme Court of 9 March 2010, I PK 195/09 and of February 9, 2016, II PK 316/14). For this reason, the controller, in accordance with the risk-based approach resulting from the provisions of Regulation 2016/679, should minimize and limit the possibilities of violating the rights or freedoms of natural persons whose data is processed, in particular as a result of recklessness or carelessness. In the case subject to this decision, this applies both to the employee entrusted with the supervision of personal data on a given day and the employee to whom a limited scope of information was to be provided. In addition, the controller should also take into account the specific context of the situation (state of epidemiological threat) and the possibilities available to a potential person taking actions, even reckless, that may expose the processed data to breach of confidentiality and loss of control by the administrator over the processed data.

The President of the Personal Data Protection Office points out that the risk-based approach introduced by Regulation 2016/679 obliges the controller to independently conduct 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 (see judgment Provincial Administrative Court of September 3, 2020, file ref. II SA / Wa 2559/19). However, the fact that the Company identifies a medium level of risk of losing the confidentiality of this data and the failure to identify a high probability of the possibility of causing a high risk of violating the rights or freedoms of natural persons does not release the controller from further monitoring a given risk and taking further actions to minimize potential undesirable effects, because only such an approach allows you to maintain a level of security that significantly reduces the likelihood of a breach of personal data protection.

In connection with the above, the provisions in the risk analysis relating to a large extent only to the signing of relevant statements and documents by employees are, in the opinion of the President of the Personal Data Protection Office, insufficient and inadequate to the risks related to the processing, as indicated above, of special category data, such as addresses of persons located in the in quarantine.

In the opinion of the President of the Personal Data Protection Office, the controller did not fully assess whether the level of security is appropriate, taking into account in particular the risk of unauthorized disclosure of the processed personal data, which constitutes a violation of Art. 32 sec. 2 of Regulation 2016/679. In addition, the administrator should perform an analysis in advance, taking into account the criteria set out in Art. 25 sec. 1 of Regulation 2016/679, whether the implemented measure is effective and provides the processing with the necessary safeguards to meet the requirements of Regulation 2016/679 and protect the rights of data subjects, which in turn constitutes a breach of this provision. In the opinion of the President of the Personal Data Protection Office, a one-off and cursory analysis regarding the provision of information constituting the subject of a breach of personal data protection, also proves that the controller does not undertake any actions aimed at, inter alia, ensuring regular testing, measurement and evaluation of the effectiveness of technical and organizational measures to ensure the security of processing, which constitutes a violation of art. 32 sec. 1 lit. d of Regulation 2016/679, reflecting measures to ensure compliance with the confidentiality principle expressed in Art. 5 sec. 1 lit. f of the Regulation 2016/679.

Pursuant to Art. 4 point 12 of Regulation 2016/679, a 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. Article 33 (2) 1 of Regulation 2016/679 provides that in the event of a breach of personal data protection, the 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 breach would result in a risk of violation of the rights or freedoms of natural persons.

In the opinion of the President of the Personal Data Protection Office, the controller should find a breach of personal data protection before the first letter of the supervisory authority of [...] April 2020. There are many circumstances resulting from the material collected in the course of the proceedings. In the above-mentioned letter, the President of the Personal Data Protection Office called on the Company to provide information as to whether the incident described at the address [...] is known. In the response of [...] May 2020, it was indicated that the Company is aware of the media reports referred to in the article available at the above-mentioned address. In the indicated article, marked with the publication date [...] April 2020 [...], there are anonymised photos of a document that is a few pages long, which is a list of data available, inter alia, Company. All entities that have such data, except for the Company, clearly demonstrated that, as a result of internal explanatory proceedings, they did not find any breach of personal data protection in their organizations regarding the disclosure of data of persons who are in quarantine. In addition, according to the employer's information on the imposition of an order penalty on the employee - a reprimand and termination of the employment contract without notice with the driver, attached to the Company's letter of [...] May 2020, the employer informed about the event on [...] April 2020. results from the guidelines of the Article 29 Working Party - Guidelines on the reporting of personal data breaches in accordance with Regulation 2016/679, adopted on 3 October 2017, when assessing the risk that may arise as a result of a breach, the controller should take into account the weight of the potential impact together on the rights or freedoms of natural persons and the probability of its 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. This is undoubtedly the case in the case at issue in this decision. The company stated in a letter of [...] May 2020 that it cannot be concluded that the breach of employee obligations fulfills the criteria of a breach of personal data protection.

In the opinion of the President of the Personal Data Protection Office, the above-mentioned misperception of the situation exposed persons under the disclosed addresses to negative consequences resulting from the controller's failure to comply with the provisions on the protection of personal data, including the obligation to notify the supervisory body about a breach of

personal data protection.

As indicated in recital 85 of Regulation 2016/679, in the absence of an appropriate and quick response, a breach of personal data protection may result in physical damage, property or non-material damage to natural persons, such as loss of control over own personal data or limitation of rights, discrimination, theft or falsification of identity. , financial loss, unauthorized reversal of pseudonymisation, breach of reputation, breach of confidentiality of personal data protected by professional secrecy or any other significant economic or social damage. Therefore, as soon as it becomes aware of a breach of personal data protection, 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 breach could result in a risk of violation of the rights or freedoms of natural persons.

In the case being the subject of this decision, there has been a breach of the protection of personal data processed by U. Sp. z o.o. based in G., consisting in providing unauthorized persons with personal data regarding: the name of the city, street, property / premises number and health data. On the basis of the above-mentioned arguments, it should be stated that the disclosure of the indicated categories of data undoubtedly resulted in the risk of violating the rights or freedoms of persons subject to medical quarantine, and the incorrect perception of the situation was the administrator's failure to comply with the obligations under Art. 33 and 34 of Regulation 2016/679, despite the awareness of the processing of information, the disclosure of which may have a negative impact on the rights or freedoms of natural persons.

In connection with the above, the controller was obliged to notify the infringement to the President of the Personal Data Protection Office pursuant to Art. 33 paragraph 1 of the Regulation 2016/679, however, it failed to comply with this obligation, in breach of the provision referred to above.

Moreover, Art. 34 sec. 1 of Regulation 2016/679 indicates that in a situation of high risk to the rights or freedoms of natural persons resulting from the breach of personal data protection, the controller is obliged to notify the data subject about the breach without undue delay. Pursuant to Art. 34 sec. 3 lit. c of Regulation 2016/679, the controller notifies individuals individually about the breach of their data, unless it would require a disproportionate effort. In this case, the controller issues a public notice or a similar measure to inform the data subjects in an equally effective manner. Guided by the need to effectively provide information to the data subjects, without exposing them to identification, the controller in the case in question, in the opinion of the President of the Personal Data Protection Office, should use the date of printing the list of addresses as the

criterion for determining the addressees of the message (persons staying in medical quarantine on that day).).

When considering the use of the Communication as a form of providing information on a breach to data subjects, the guidelines of the Article 29 Working Party on the reporting of personal data breaches in accordance with Regulation 2016/679 (WP250rev.01) should be taken into account, i.e. "controllers should choose methods to ensure the best chance of properly communicating information to all affected individuals. In some circumstances, this may mean that an administrator will use a range of communication methods rather than just one contact channel. " Therefore, it should be noted that the data controller does not have to be limited to one form of notification only, but may use such a form in each individual case that ensures effective notification of individuals about the occurrence of a breach. The message on the website should be visible directly on the website, without the need to open additional subpages. In the case at hand, it is also justified to use other communication channels, e.g. social networks, local websites, newspaper advertisements.

Pursuant to Art. 34 sec. 2 of Regulation 2016/679, the correct notification should:

describe the nature of the personal data breach in clear and plain language;

contain at least the information and measures referred to in Art. 33 paragraph 3 lit. b), c) and d) of Regulation 2016/679 (see table), that is:

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

b) a 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.

Pursuant to Art. 34 sec. 4 of Regulation 2016/679, if the controller has not yet notified the data subjects about the breach of personal data protection, the supervisory authority may request it or may state that one of the conditions referred to in para. 3 of this article.

U. Sp. z o.o. based in G. did not assess the risk of violating the rights or freedoms of natural persons and did not notify data subjects about the violation of personal data protection. Meanwhile, obtaining information by the administrator about the occurrence of a breach of personal data protection, within the meaning of art. 4 point 12 of Regulation 2016/679, obliges it to conduct an analysis in terms of the risk of violating the rights or freedoms of data subjects. This analysis makes it possible to

determine whether it is necessary for the administrator to fulfill the obligations under Art. 33 paragraph. 1 of Regulation 2016/679 (notification of breach to the supervisory authority) and with art. 34 sec. 1 of the Regulation 2016/679 (notification of the data subject about the breach).

As a result of the analysis of the breach of personal data protection, which took into account the nature of the breach, its duration, data categories, the number of persons affected by the breach and the remedial measures taken - the President of the Office for Personal Data Protection decided that the breach of data confidentiality, in particular data regarding: the name of the city, street, property / premises number and data on health in the form of information on medical quarantine, causes a high risk of violating the rights or freedoms of natural persons, therefore it is necessary to notify data subjects about the violation protect their personal data.

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 under Art. 34 of the Regulation 2016/679, notify the data subject of such a breach without undue delay. This means that the controller is obliged to implement all appropriate technical and organizational measures to immediately identify a breach of personal data protection and promptly inform the supervisory authority, and in cases of high risk of violation of rights or freedoms, also the data subject. The controller should fulfill this obligation as soon as possible. Recital 86 of Regulation 2016/679 explains: "The controller should inform the data subject without undue delay of the breach of personal data protection where it may result in a high risk of violation of the rights or freedoms of that person, so as to enable that person to take the necessary preventive measures. . 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 immediate risk of harm will require the immediate notification of data subjects, while the implementation of appropriate measures against the same or similar breaches of data protection 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 lit. a Regulation 2016/679 (cf. Chomiczewski Witold [in:] GDPR. General Data Protection Regulation. Comment. ed. E. Bielak - Jomaa, D. Lubasz, Warsaw 2018). Proper compliance with 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 at least indicate the information listed in Art. 34 sec. 2 of Regulation 2016/679, from which the administrator did not fulfill.

The breach of personal data protection should be an impulse for the controller to review the adopted procedures in order to update them and possibly clarify them, which the Company mentioned in point 4 of the letter of [...] September 2020. It is reasonable to take into account the human factor for which the President of the Personal Data Protection Office pointed out in this decision and thus limiting the possibility of processing personal data contrary to the principles adopted in the organization. The mitigating circumstances for the final resolution include taking disciplinary actions against employees who contributed to the infringement with their actions and the fact that, despite the difficult epidemiological situation, the controller undertook to conduct training on the protection of personal data for its employees. The above circumstances, in the opinion of the President of the Personal Data Protection Office, do not affect the final charge of infringement of the provisions of Regulation 2016/679 indicated in the decision conclusion. In view of the above, the President of the Personal Data Protection Office decided that in the established circumstances of this case, the appropriate remedy will be to grant U. Sp. z o.o. based in G., pursuant to Art. 58 sec. 2 lit. b) of Regulation 2016/679, reminders for failure to fulfill the obligations set out in Art. 5 sec. 1 lit. f, art. 24 sec. 1, art. 25 sec. 1, art. 32 sec. 1 lit. b and lit. d, art. 32 sec. 2, art. 33 paragraph 1 and art. 34 sec. 1 of Regulation 2016/679. In the opinion of the President of the Personal Data Protection Office, the admonition imposed will also be of a preventive nature, i.e. it will prevent violations of the provisions on the protection of personal data in the future by both U. Sp. z o.o. based in G. as well as other data administrators.

In view of the above, the President of the Personal Data Protection Office resolved as in the sentence.

I would like to inform you that pursuant to art. 41 of the Code of Administrative Procedure, in the course of the proceedings, the parties and their representatives and proxies are required to notify the public administration body of any change of their

address. In the event of neglect of this obligation, the delivery of the letter to the current address has legal effect.

The decision is final. Based on Article. 7 sec. 2 of the Act of May 10, 2018 on the Protection of Personal Data (Journal of Laws of 2019, item 1781, as amended) in connection with Art. 13 § 2, art. 53 § 1 and article. 54 § 1 of the Act of August 30, 2002 - Law on proceedings before administrative courts (Journal of Laws of 2019, item 2325), 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 to the party. The complaint is lodged through the President of the Personal Data Protection Office. The entry fee for the complaint is PLN 200. The party has the right to apply for the right to assistance, including exemption from court costs.

2020-11-23