Warsaw, day 30

November

2022

Decision

DKN.5112.5.2021

Based on Article. 104 § 1 of the Act of June 14, 1960 Code of Administrative Procedure (Journal of Laws of 2021, item 735, as amended) and art. 7 sec. 1 and 2, art. 60, art. 101 and art. 103 of the Act of May 10, 2018 on the protection of personal data (Journal of Laws of 2019, item 1781) and art. 57 sec. 1 lit. a) and h), Art. 58 sec. 2 lit. d) and point i) in connection with art. 5 sec. 1 lit. a), art. 6 sec. 1, art. 9 sec. 1 in connection with art. 9 sec. 2, as well as art. 83 sec. 1 - 3 and art. 83 sec. 5 lit. a) 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 Regulation) (Journal of Laws UE L 119 of 04/05/2016, p. 1, as amended), after administrative proceedings initiated ex officio regarding the violation of provisions on the protection of personal data in connection with the processing of personal data by Partners of a civil law partnership PIONIER [...] s.c. with the place of business in L [...], President of the Office for Personal Data Protection

stating that N.B. and T.M., partners in the civil law partnership Kancelaria PIONIER [...] s.c. with the place of business in L [...], as well as R. B., a former partner of this company, the provisions:

article 6 sec. 1 of Regulation 2016/679 consisting in the processing of personal data of their potential customers without a legal basis, and in particular without obtaining their consent to processing referred to in art. 6 sec. 1 lit. a) of Regulation 2016/679, which is a violation of the principle of processing personal data in accordance with the law, referred to in art. 5 sec. 1 lit. a) Regulation 2016/679,

article 9 sec. 1 in connection with art. 9 sec. 2 of Regulation 2016/679 consisting in the processing of data concerning the health of their potential customers without a legal basis, and in particular without obtaining their express consent to processing referred to in art. 9 sec. 2 lit. a) of Regulation 2016/679, which is a violation of the principle of processing personal data in accordance with the law, referred to in art. 5 sec. 1 lit. a) Regulation 2016/679,

orders N. B. and T. M., partners in the civil law partnership Kancelaria PIONIER [...] s.c., to adapt the processing operations to

the provisions of Regulation 2016/679 by ceasing to process personal data of potential clients without a legal basis, i.e. without obtaining consent to the processing of their personal data, which referred to in art. 6 sec. 1 lit. a) and art. 9 sec. 2 lit. a) of Regulation 2016/679, within 14 days from the date of delivery of this decision.

imposes on N. B. and T. M., partners in the civil law partnership Kancelaria PIONIER [...] s.c., and on R. B., former partner in the civil law partnership Kancelaria PIONIER [...] s.c., all jointly and severally liable for violation of the provisions indicated in points a) and b) of the conclusion of this decision, an administrative fine in the amount of PLN 45,697.00 (say: forty-five thousand six hundred and ninety-seven zlotys).

Justification

The President of the Personal Data Protection Office, hereinafter referred to as the "President of the Personal Data Protection Office", pursuant to art. 78 sec. 1, art. 79 sec. 1 item 1 and art. 84 sec. 1 point 1-4 of the Act of May 10, 2018 on the Protection of Personal Data (Journal of Laws of 2019, item 1781), hereinafter referred to as the "Act", in connection with Art. 57 sec. 1 lit. a) and h) and Art. 58 sec. 1 lit. b) and e) of Regulation 2016/679, in order to control the compliance of data processing with the provisions on the protection of personal data, performed control activities at R. B. and T. M., Partners of PIONIER [...] s.c. with the place of business in L [...], hereinafter referred to as "Partners of the Company" or "Administrators" (file reference number DKN [...]).

above control activities were carried out as a result of the receipt by the President of the UODO of information indicating a possible violation by the Administrators of the provisions on the protection of personal data. This information was provided to the President of the UODO in the letter of the Poviat Police Commander in L. of March 2021, in which, as part of the activities ordered by the District Prosecutor's Office in L., the Poviat Police Commander in L. asked the President of the UODO for carrying out control activities at the Administrators.

The President of the UODO, after receiving the above-mentioned of the letter, in the first place, he undertook checking activities against the Administrators, requesting by letters of [...] March and [...] May 2021 to deliver, in accordance with art. 58 sec. 1 lit. a) of Regulation 2016/679, all information needed by the supervisory authority to perform its tasks, i.e. information regarding primarily the method, purpose and legal basis for the processing of personal data by Administrators in connection with their business activity.

Due to the lack of sufficient cooperation of the Company's Shareholders with the supervisory authority in clarifying the

circumstances of this case, manifested in the delay in answering the questions addressed to the Company's Shareholders by the President of the UODO, as well as their non-exhaustive content, the President of the UODO decided that it is necessary to conduct an inspection in the enterprise of the Company's Shareholders pursuant to art. 78, art. 79 sec. 1 and art. 84 sec. 1 point 1-4 of the Act of May 10, 2018 on the protection of personal data (Journal of Laws of 2019, item 1781) in connection with joke. 57 sec. 1 lit. a) and h) and Art. 58 sec. 1 lit. b), e) and f) of Regulation 2016/679.

The scope of the inspection covered the processing of personal data of clients and potential clients of the Company's Shareholders by the Administrators. In the course of the inspection, oral explanations were received from the Administrators' employees. The facts were described in detail in the inspection report, which was signed by the Company's Shareholders.

Based on the evidence collected in the case, it was established that in the process of processing personal data, the Company's partners, as administrators, violated the provisions on the protection of personal data, i.e. art. 6 sec. 1 and art. 9 sec. 2 in connection with art. 5 sec. 1 lit. a) and Art. 9 sec. 1 of Regulation 2016/679, by processing without a legal basis personal data of potential clients of the Company's Shareholders, including data regarding their health, in particular without obtaining their consent to the processing of personal data referred to in art. 6 sec. 1 lit. a) and art. 9 sec. 2 lit. a) Regulation 2016/679.

In connection with the above, the President of the UODO initiated ex officio administrative proceedings regarding the identified deficiencies in order to clarify the circumstances of the case (letter of [...] February 2022, reference number:[...]). The Company's partners did not respond in writing to the identified violations of the provisions on the protection of personal data, which are the subject of the administrative proceedings, listed in the notification of the initiation of the proceedings. It should be noted that during the administrative proceedings regarding the case in question, R.B. ceased to be a party to the articles of association concluded by the Company's Shareholders and to conduct business activity within it. N.B., on the other hand, joined the partnership agreement with T. M., becoming a Partner of the Company, and has been conducting business activity within it since [...] April 2022. For the above reason, a letter of [...] October 2022 was sent to N. B. as a Partner of the Company (ref.: [...]) with a notification of the initiation of proceedings against her in the case in question. N.B., like the other Shareholders of the Company before, did not submit any explanations regarding the above-mentioned writings.

After reviewing all the evidence collected in the case, the President of the UODO considered the following.

In Art. 5 of Regulation 2016/679, rules for the processing of personal data are formulated, which must be respected by all

administrators, i.e. entities that individually or jointly with others determine the purposes and methods of personal data processing. Pursuant to art. 5 sec. 1 lit. a) of Regulation 2016/679, personal data must be processed in accordance with the law, fairly and transparently for the data subject ("lawfulness, reliability and transparency"). In addition, in accordance with art. 6 sec. 1 of Regulation 2016/679, processing is lawful only in cases where - and to the extent that - at least one of the following conditions is met:

the data subject has consented to the processing of his personal data for one or more specific purposes;

processing is necessary for the performance of a contract to which the data subject is a party or in order to take action at the request of the data subject prior to entering into a contract;

processing is necessary to fulfill a legal obligation to which the controller is subject;

processing is necessary to protect the vital interests of the data subject or another natural person;

processing is necessary to perform a task carried out in the public interest or in the exercise of public authority entrusted to the administrator;

processing is necessary for the purposes of the legitimate interests pursued by the administrator or by a third party, except for situations where such interests are overridden by the interests or fundamental rights and freedoms of the data subject, which require protection of personal data, in particular when the data subject is a child.

In turn, pursuant to art. 9 sec. 1 of Regulation 2016/679, it is prohibited to process personal data revealing racial or ethnic origin, political opinions, religious or ideological beliefs, trade union membership, and genetic and biometric data, processed for the purpose of uniquely identifying a natural person, or data concerning health, sexuality or orientation that person's sexuality.

Regulated in art. 9 sec. 1 of Regulation 2016/679, the processing of a special category of personal data, including health data, is therefore generally prohibited. However, the above-mentioned provision does not apply in the cases indicated in Art. 9 sec. 2, among others when the condition is met that the data subject has expressly consented to the processing of the above-mentioned personal data for one or more specific purposes, unless Union or Member State law provides that the data subject may not lift the said prohibition (Article 9(2)(a) of Regulation 2016/679). The catalog of conditions listed in art. 9 sec. 2 of Regulation 2016/679 is closed. Each of the premises legalizing the process of processing personal data subject to special protection, including health data, referred to in this provision, is autonomous and independent. This means that these

conditions are, in principle, equal, and therefore the fulfillment of at least one of them determines the lawful processing of personal data. In addition, the processing of personal data must comply with the principles laid down in art. 5 sec. 1 of Regulation 2016/679. These principles include, among others, the processing of personal data in accordance with the law (point a). The aforementioned principle requires that personal data be processed in accordance with the law, fairly and transparently for the data subject ("lawfulness, reliability and transparency").

The Company's shareholders and their employees, in the explanations submitted during the inspection, indicated that the predominant business activity conducted by the Company's Shareholders, in accordance with the entry in the Central Register and Information on Economic Activity, is activity related to risk assessment and estimation of incurred losses (PKD: 66.21.Z). As it was established in the course of the inspection, the activity carried out by the Company's Shareholders consists in providing legal assistance in the field of representing clients injured mainly in traffic accidents before insurance companies, courts and other entities, in order to obtain compensation, redress and pensions for them, and also reimbursement of treatment and rehabilitation costs. The activity of the Company's Partners also consists in mediating between clients and medical facilities in the field of obtaining medical services. As part of the services provided, persons employed by the Company's Shareholders represent clients in court proceedings, the subject of which are claims for damages.

During the first conversation with a potential client, he is first asked to give the Company's Shareholders oral consent to obtain and process his personal data until the possible conclusion of a contract for the provision of services. If the potential customer gives verbal consent to the processing of his data, the conversation is continued, and in the case of refusal, the conversation is interrupted. Thus, the acquisition and subsequent processing of the potential client's data by the Company's Shareholders occurs only if the representative of the Administrators receives from the potential client an oral statement of consent to the processing of his personal data.

In connection with the above, the consent given by the potential client is only oral, i.e. through a declaration of the potential client made during the first telephone conversation or the first direct conversation with the partners, representatives or employees of the Company's Shareholders. In order to obtain data from potential customers in the above-mentioned way is to ensure that the Company's Shareholders are able to contact these customers again and present them with an offer.

Activities leading to the acquisition of the above-mentioned personal data and establishing contacts with potential customers are carried out on the basis of press releases, internet publications, including content available in social media (e.g. the "[...]"

website), as well as information provided or disseminated by organizations engaged in charity activities (e.g. foundations). The Company's partners have not provided evidence confirming that they have obtained consent to obtain personal data of persons supported by the above. foundations.

Personal data of potential customers are also obtained on the basis of the content of publicly available private profiles of natural persons in the above-mentioned social media, containing information about the death of natural persons, accidents and other events relevant to the activities of the Administrators and suggesting that the above-mentioned persons may be potential clients of the Company's Shareholders. The activities referred to above are also carried out through environmental intelligence activities, i.e. obtaining information about potential clients of the Company's Shareholders and their personal data as a result of direct conversations with persons residing, working or otherwise functioning in the environment of the above-mentioned entities. customers (e.g. conversations with neighbors, the mayor, getting acquainted with the content of widespread obituaries in cemeteries, etc.). The places of conducting the environmental interview are also selected on the basis of press reports and online publications. On the basis of all the above activities, the Company's Shareholders, their representatives or employees obtain personal data of potential customers primarily in the form of information allowing them to identify the address of residence, which then allows them to establish direct contact with these customers and submit an offer of services by the Company's Shareholders (e.g. information about the color of the facade of the house , its topographical location, etc.).

In the case of reaching a potential customer, during a direct conversation, he is presented with the offer of services provided by the Administrators. In the event that a potential client expresses the will to establish contact with the Company's Shareholders or a contact person authorized by them, a personal conversation is conducted with him, during which other, more accurate personal data is obtained, i.e. telephone number, name and surname.

In addition, the Administrators' offer is presented to potential customers who voluntarily initiate the first contact with the Company's Shareholders via electronic communication channels. In the majority of cases, contact is made on the initiative of a potential client by phone.

These data are stored by the Company's Shareholders in electronic form (e.g. e-mail) or in paper form until a meeting with a potential client is held and the client makes a decision on establishing cooperation and concluding a contract for the provision of services. In a situation where no contract is concluded with a potential customer, his personal data is destroyed after a maximum of 5-7 days from the date of making the first contact with him and obtaining the data. After this time, the data is

permanently destroyed. In the case of potential customers, the Company's Partners obtain, even before concluding a contract with them, the following data: name, surname, telephone number, e-mail address, information about the death of another person and health data in connection with accident events.

It should be noted that, in accordance with recital 35 of Regulation 2016/679, "Personal data concerning health should include all data on the health of the data subject, revealing information about the past, present or future physical or mental health of the data subject concern. Such data include information about a given natural person collected during his registration for healthcare services or during the provision of healthcare services to him, as defined in Directive 2011/24/EU of the European Parliament and of the Council (1); number, symbol or designation assigned to a given natural person in order to uniquely identify that natural person for health purposes; information from laboratory or medical examinations of body parts or body fluids, including genetic data and biological samples; and any information, for example about a disease, disability, disease risk, medical history, clinical treatment or physiological or biomedical condition of the data subject, regardless of their source, which may be, for example, a doctor or other healthcare professional, hospital, device medical or in vitro diagnostic test."

Considering the subject and circumstances of the business activity conducted by the Company's Shareholders, the processing of personal data of potential customers within it, as done by the Company's Shareholders, may take place on the basis of the aforementioned art. 6 sec. 1 lit. a) and Art. 9 sec. 2 lit. a) in connection with art. 5 sec. 1 lit. a) of Regulation 2016/679, i.e. when the data subject has consented to the processing of his personal data for one or more specific purposes (in relation to data that is not subject to special protection) and when the above-mentioned the person has given explicit consent to the processing of data subject to special protection, in this case health data.

As it was established during the inspection, in the case of potential customers, i.e. persons to whom the Company's Shareholders are just addressing an offer regarding the services they provide and with whom contracts in this regard have not yet been concluded, the above consent is obtained, according to the Administrators' statement and its employees, only in oral form. In this case, also due to the fact that data concerning the health of potential customers are processed (e.g. information about injuries suffered by accident victims), the premise indicated by the Administrators under Art. 6 sec. 1 lit. b) of Regulation 2016/679 does not apply as the legal basis for processing (processing necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract).

It should be recalled that pursuant to art. 6 sec. 1 of Regulation 2016/679, processing is lawful only in cases where - and to the

extent that - at least one of the following conditions is met:

the data subject has consented to the processing of his personal data for one or more specific purposes;

processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract;

processing is necessary to fulfill a legal obligation to which the controller is subject;

processing is necessary to protect the vital interests of the data subject or another natural person;

processing is necessary to perform a task carried out in the public interest or in the exercise of public authority entrusted to the administrator;

processing is necessary for the purposes of the legitimate interests pursued by the administrator or by a third party, except for situations where such interests are overridden by the interests or fundamental rights and freedoms of the data subject, which require protection of personal data, in particular when the data subject is a child.

In turn, in accordance with the content of art. 9 sec. 1 of Regulation 2016/679, it is prohibited to process personal data revealing racial or ethnic origin, political opinions, religious or ideological beliefs, trade union membership, and to process genetic data, biometric data for the purpose of uniquely identifying a natural person or data concerning health, sexuality or orientation that person's sexuality. sec. 1 does not apply if one of the following conditions is met:

the data subject has expressly consented to the processing of such personal data for one or more specific purposes, unless Union or Member State law provides that the data subject may not lift the prohibition referred to in paragraph 1;

processing is necessary for the fulfillment of obligations and the exercise of specific rights by the controller or the data subject in the field of labor law, social security and social protection, to the extent permitted by Union or Member State law, or a collective agreement under Member State law providing for appropriate safeguards for the fundamental rights and interests of the data subject;

processing is necessary to protect the vital interests of the data subject or another natural person, and the data subject is physically or legally incapable of giving consent;

processing is carried out as part of the authorized activity conducted with appropriate safeguards by a foundation, association or other non-profit entity with political, ideological, religious or trade union goals, provided that the processing concerns only members or former members of this entity or persons maintaining permanent contacts with it in in connection with its purposes

and that personal data is not disclosed outside this entity without the consent of the data subjects;

the processing concerns personal data obviously made public by the data subject;

processing is necessary to establish, pursue or defend claims or as part of the administration of justice by the courts;

processing is necessary for reasons related to important public interest, on the basis of Union or Member State law, which are proportionate to the intended purpose, do not violate the essence of the right to data protection and provide for appropriate and specific measures to protect the fundamental rights and interests of the data subject ;

processing is necessary for the purposes of preventive or occupational medicine, to assess the employee's ability to work, medical diagnosis, the provision of health or social care, treatment or management of health or social care systems and services on the basis of Union or Member State law or in accordance with an agreement with a healthcare professional and subject to the conditions and safeguards referred to in section 3;

processing is necessary for reasons related to the public interest in the field of public health, such as protection against serious cross-border health threats or ensuring high standards of quality and safety of healthcare and medicinal products or medical devices, on the basis of Union or Member State law that provide for appropriate specific measures to protect the rights and freedoms of data subjects, in particular professional secrecy; 4.5.2016 L 119/38 Official Journal of the European Union EN;

processing is necessary for archival purposes in the public interest, for scientific or historical research purposes or for statistical purposes in accordance with art. 89 sec. 1, on the basis of Union law or Member State law, which are proportionate to the intended purpose, do not violate the essence of the right to data protection and provide for appropriate, specific measures to protect the fundamental rights and interests of the data subject.

In the light of the evidence collected in the course of the inspection carried out at the Company's Shareholders by the President of the Personal Data Protection Office, as well as considering the special circumstances of obtaining and processing data of potential customers by the Company's Shareholders, as well as due to the wording of the provision of art. 6 sec. 1 of Regulation 2016/679, it should be considered that in the case of the so-called ordinary data, i.e. personal data of potential customers of the Company's Shareholders, such as: name, surname, telephone number and e-mail address, the only premise legitimizing the processing of such data by the Company's Shareholders is obtaining consent from the data subject, i.e. from potential customer. The evidence collected in the course of the inspection, including the explanations of the Company's Shareholders and their employees, shows that the processing of data of potential customers by the Administrators is not

necessary for the performance of the contract to which the data subject is a party (it is not yet concluded at all with a potential client), or to take action at the request of potential clients, before concluding contracts with them (Article 6(1)(b) of Regulation 2016/679), since at the stage of contact between the Administrators and potential clients there is no mention of their "requests", and the data is obtained and processed by the Administrators only for the purpose of determining by him, for his needs, the degree of profitability of concluding a contract with a potential client and in order to re-establish contact with him and express his will whether he wants to conclude a contract with the Administrators at all or not. It should be noted that during the inspection, the Company's Shareholders did not provide evidence to confirm the fact that potential customers submitted "demands" to them to take specific actions before concluding the contract.

In addition, in the case in question, there can be no question of the necessity for the Administrators to process data of potential customers to protect their vital interests or other natural persons in a situation where these potential customers would be physically or legally unable to give consent (Article 6(1)(a) of the GDPR). d of Regulation 2016/679). The said processing is also not necessary to fulfill the legal obligation incumbent on the Administrators (Article 6(1)(c) of Regulation 2016/679), perform a task carried out in the public interest or in the exercise of public authority entrusted to them (Article 6(1)(c) of Regulation 2016/679) 1 letter e of Regulation 2016/679), or for purposes arising from legitimate interests pursued by Administrators or by a third party (Article 6 paragraph 1 letter f of Regulation 2016/679).

Please note that data processing for the purposes of the legitimate interests pursued by the Administrators of personal data, as a rule, cannot be carried out in any situation and for any purposes of the Administrators. When processing data pursuant to art. 6 sec. 1 lit. f) of Regulation 2016/679, it should be taken into account whether such processing is necessary and proportionate to the purpose specified by the Administrators. In addition, the rights and freedoms of persons whose data are to be processed and their possible priority in relation to the Administrators' goals should also be taken into account. In order to resolve the above issues, each administrator should carry out the so-called balance test, the aim of which is to obtain a balance of weighing of the above-mentioned goods on the part of both the data subject and their Administrators. If, as a result of such a test, it turns out that the purpose specified by the given Administrators can be achieved in a different way than by processing personal data in a specific way and in a specific scope, and in particular when it violates the rights or freedoms of the data subject, it should be considered that the administrator does not has grounds for data processing pursuant to art. 6 sec. 1 lit. f) Regulation 2016/679.

In the case in question, the Company's Shareholders, as Administrators, acquire and process data of potential customers in order to maintain contacts with them in order to obtain a declaration as to the conclusion or non-conclusion of a contract for the provision of services by the Company's Shareholders. During the processing, the Company's Shareholders also assess the degree of economic risk related to the conclusion of the contract. In the opinion of the President of the UODO, achieving the purpose referred to above does not require obtaining personal data from potential customers, in particular health data. The above-mentioned goal Administrators would be able to achieve, for example, by leaving a leaflet informing the potential client about his services and the possibility of concluding a contract for the provision of services regarding seeking compensation (redress).

Thus, it should be considered that the processing of data of potential customers by the Administrators in the case in question is disproportionate to the desired result that they want to achieve and is not necessary for this purpose. It should be noted that the "necessity" in this case should be understood as a factual situation in which, without processing the data of potential customers in the above-mentioned way the Administrators would not be able to conclude contracts for the provision of services at all. In the case in question, in the opinion of the President of the UODO, such a state of necessity does not exist.

In particular, the activities of the Administrators described above related to the processing of their potential customers' data cannot be considered direct marketing referred to in the final sentence of recital 47 of Regulation 2016/679. In accordance with the content of the above of the sentence, "the processing of personal data for direct marketing purposes can be considered as an action performed in a legitimate interest". According to the commonly accepted theory of direct marketing, it consists in directing specific content to selected customers, including through individual contact, in order to obtain their statements regarding the perception of specific goods or services or their willingness to purchase them.

Direct marketing allows consumers to buy products through the use of various communication and advertising methods. In addition to shaping the image of the entrepreneur, the purpose of direct marketing is to obtain information directly from the consumer regarding his perception of specific goods and services.

In the case in question, both due to the type of part of the data of potential customers processed by the Administrators (health data) and the purpose of their processing, in the opinion of the President of the UODO, there can be no question of processing for direct marketing purposes. The processing of health data for marketing purposes without the consent of the person concerned should be considered unacceptable and disproportionate to other customer interests that could potentially be

implemented through such processing. It should be noted that health data is subject to special protection in the light of the content of art. 9 of Regulation 2016/679, which does not contain premises enabling their processing analogously to the premise related to the legitimate purpose pursued by the Administrators referred to in art. 6 sec. 1 lit. f of Regulation 2016/679. From the above reason, and also due to the fact that the protection of extremely important personal rights of a natural person, i.e. their privacy, which also includes information about health, excludes the possibility of processing data containing the above-mentioned information for marketing purposes without prior consent, because these purposes are related to the implementation of goods of disproportionately lower value than the privacy of a natural person. It should also be noted that the offer of cooperation addressed by the Company's Shareholders to potential clients is closely related to the acquisition of health data by the Company's Shareholders, so without obtaining this data, the Company's Shareholders would not contact potential clients with an offer of cooperation in the way they do when establishing personal, direct contact with the above-mentioned people.

At the same time, it should be noted that the Company's Shareholders obtain and then process the data of potential customers in special circumstances, because this happens in connection with insurance events, about which the Company's Shareholders obtain knowledge from publicly available sources (social media, local press, etc. .). Thus, reaching a potential customer is based on the above-mentioned information, and the purpose of a visit to a potential customer is to obtain and process his data for further contact with him regarding the conclusion of the contract and assessment of the business risk of its conclusion, not marketing activities consisting in presenting an offer of services.

It should be noted that if the acquisition and further processing of data of potential customers by the Company's Shareholders were to be carried out for direct marketing purposes, the Company's Shareholders would basically have to have this data at the moment of establishing the first contact with these customers. In the present case, however, the data is obtained only when contact is made with a potential customer, and further processing is not related to marketing activities (study of customer attitude, advertising, presentation of the offer, etc.), but is only related, as mentioned above, to obtaining from above the client's statement regarding his will to conclude an agreement with the Company's Shareholders, on the one hand, and on the other hand, an estimation of the business risk related to the conclusion of the agreement for the Company's Shareholders.

It should also be remembered that the activity of the Administrators largely boils down to the provision of legal services, consisting in the operation of professional legal representatives (solicitors, attorneys) for persons seeking compensation from

entities providing insurance services, representing them in court proceedings, etc. How testified in the course of the inspection, the Partner of the Company T. M., the activity carried out by the Partners of the Company "consists in providing legal assistance in the field of representing clients injured mainly in traffic accidents before insurance companies, before courts, as well as other entities in order to obtain compensation, compensation and pensions for them , as well as reimbursement of treatment and rehabilitation costs".

Referring to the above, it should be noted that pursuant to § 23 of the Collection of Principles of Ethics for Advocates and the Dignity of the Profession (Code of Ethics for Advocates) (Resolution No. 2/XVIII/98 of the Polish Bar Council of October 10, 1998, as amended), an advocate is prohibited from using from advertising, as well as a ban on acquiring customers in a manner contrary to the dignity of the profession and cooperation with entities acquiring customers in violation of the law or principles of social coexistence. In addition, pursuant to § 23b section 1 of the Code, an attorney is not allowed to offer services to potential clients in the form of an offer addressed to persons who have not previously expressed such a clear wish, while according to § 23b sec. 4 and sec. 5 of the Code, it is unacceptable to address potential clients in order to provide information about one's activities, also during uninvited visits, telephone conversations and in correspondence to persons who do not turn to a lawyer for legal assistance, and it is also unacceptable to commission third parties to disseminate information about the lawyer .

In turn, in accordance with the content of art. 32 sec. 1 item 6 of the Code of Ethics for Legal Advisors (annex to Resolution No. 3/2014 of the Extraordinary National Convention of Legal Advisors of November 22, 2014 on the Code of Ethics for Legal Advisors, as amended), it is forbidden to inform about the practice of the profession contrary to the law, decency and constituting a violation of the provisions of the Code, including imposing, in particular violating the sphere of privacy, insistent, in the wrong place, which may affect the decision to use legal assistance.

In view of the above argument regarding the subject of the Administrators' activity and the quoted provisions of the codes of ethics of professional barristers and legal advisers, it should be assumed that the acquisition and processing of data of the Administrators' potential clients in the manner described above cannot also be justified by the legitimate interests pursued by the Administrators or by a third party referred to in Art. 6 sec. 1 lit. f) Regulation 2016/679. The above-mentioned provisions regulating the rules for informing legal advisers and advocates about their activities, in the opinion of the President of the UODO, are in contradiction with the way in which the Administrators do it. And although it is not within the competence of the

President of the UODO to assess the manner in which Administrators provide services in the field of legal advice, including presenting their offer to potential clients, as well as analyzing the internal legal provisions of professional self-governments, the wording of the said provisions is an additional indication in this case draw the conclusion that the Administrators cannot rely on the legitimate interests pursued by them in the form of direct marketing, since the above-mentioned the regulations, as a rule, do not allow acquiring customers in the manner in which Administrators do it, apart from the very issue that their actions taken towards potential customers cannot be considered direct marketing at all in this case.

During the inspection, the Administrators did not prove that any of the above the conditions were met, which would justify the acquisition and processing of personal data of potential customers without obtaining their consent that could be demonstrated before the supervisory authority.

On the other hand, in the case of specific data of potential customers processed by the Administrators, i.e. regarding their health or the health of other people, the more the only premise legitimizing the processing of the above. of the data is the consent of these customers, and this is the "explicit" consent, as provided for in art. 9 sec. 2 lit. a) Regulation 2016/679. None of the other premises stipulated in the above-mentioned the provision does not constitute a legal basis for the processing of data on the health of potential customers by the Company's Shareholders. The processing of this data is not necessary for the Administrators to fulfill their obligations and exercise the specific rights of the Administrators or by the data subject in the field of labor law, social security and social protection (Article 9(2)(b) of Regulation 2016/679). Processing of the above specific data is also not necessary to protect the vital interests of the data subjects or other natural persons, since the Company's Shareholders have not demonstrated during the inspection that the data subjects, i.e. potential clients of the Company's Shareholders, are physically or legally incapable of consent to processing (Article 9(2)(c) of Regulation 2016/679).

The processing of data on the health of potential customers by the Administrators is also not justified by doing so as part of authorized activities conducted with appropriate safeguards by a foundation, association or other non-profit entity with political, ideological, religious or trade union goals. The Company's partners do not act in legal forms or for the purposes referred to above and listed in Art. 9 sec. 2 lit. d) Regulation 2016/679.

The administrators have also failed to demonstrate that their processing of data on the health of potential customers concerns personal data obviously made public by the data subject (Article 9(2)(e) of Regulation 2016/679) or that it is necessary to determine pursuing or defending claims or as part of the administration of justice by the courts (Article 9(2)(f) of Regulation

2016/679). It is true that the activity of the Company's Partners is related to determining, pursuing and defending claims for clients, but the nature of the relationship between the Administrators' potential clients and themselves does not authorize them to process health data without obtaining express consent. The processing of data of potential customers by the Company's Shareholders without their consent is not necessary to establish, pursue and defend claims on their behalf. The premise indicated in art. 9 sec. 2 lit. f) of Regulation 2016/679 applies to cases where processing is necessary for the purposes indicated therein, so the data must be processed without the voluntary consent of the data subject. In a situation where a potential customer, according to the findings of the inspection carried out at the Administrators, starts a conversation with a representative of the Administrators only for the purpose of establishing possible cooperation and submitting the Administrators' initial offer, there are no grounds for the Administrators to obtain and then process even short-term data of a potential customer without his consent, because obtaining it in such a case is, on the one hand, necessary due to the purpose of data processing, and on the other hand, it can be obtained without the need to incur greater expenditure and, most importantly, without infringing any interests of the potential client related to the possibility of pursuing claims. As indicated by the Administrators in the explanations obtained in the course of the inspection, the data of a potential customer is stored in electronic form (e.g. an e-mail) or in paper form until a meeting is held with him and he decides to establish cooperation and conclude a contract for the provision of services with the Company's partners. In the event of a potential customer's resignation from concluding a contract, the personal data of such a customer is stored in the above-mentioned forms up to a maximum of 5 - 7 days. It follows from the above that the acquisition and processing of data of potential customers by the Company's Shareholders before the conclusion of the contract serves only to enable them to familiarize themselves with the offer and decide to establish cooperation with the Company's Shareholders, therefore it is not necessary to establish, pursue and defend claims of potential customers.

The processing of data on the health of potential customers by Administrators is also not necessary for reasons related to important public interest, on the basis of Union law or Member State law (Article 9(2)(g) of Regulation 2016/679), or for the purposes of preventive health or occupational medicine, to assess the employee's ability to work, medical diagnosis, provide health care or social security, treatment or manage health or social care systems and services on the basis of Union law or Member State law or in accordance with a contract with a health professional (art. 9 section 2 letter h of Regulation 2016/679). above processing is also not necessary for reasons related to the public interest in the field of public health, such as protection

against serious cross-border health threats or ensuring high standards of quality and safety of healthcare and medicinal products or medical devices, on the basis of Union or Member State law, which provide for appropriate, specific measures to protect the rights and freedoms of data subjects, in particular professional secrecy (Article 9(2)(i) of Regulation 2016/679).

In the case of the Company's Shareholders, due to the nature and scope of their business activity, there can also be no question of the necessity to process data of potential customers for archival purposes in the public interest, for scientific or historical research purposes or for statistical purposes in accordance with Art. 89 sec. 1 of Regulation 2016/679, on the basis of EU or Member State law, which are proportionate to the intended purpose, do not violate the essence of the right to data protection and provide for appropriate, specific measures to protect the fundamental rights and interests of the data subject (Article 9(1) of Regulation 2016/679 2 letter j of Regulation 2016/679).

In this situation, it should be considered that the legal basis for obtaining and then further processing, including storage, of the above-mentioned data of potential customers can only be art. 6 sec. 1 lit. a) and Art. 9 sec. 2 lit. a) Regulation 2016/679 in connection with Art. 5 sec. 1 lit. a) Regulation 2016/679. The above means that the Company's Shareholders, due to the fact of obtaining health data from potential customers, were obliged to obtain explicit consent to the processing of their personal data. Because, as indicated above, the Company's Shareholders, in accordance with the content submitted by them and their employees in the course of auditing testimonies as witnesses, obtain only oral and unregistered consents for the processing of data of potential customers (e.g. in the form of sound recordings, registers or lists of obtained consents and persons who granted them, etc.), such action should be considered as violating the above-mentioned provisions of Regulation 2016/679.

In accordance with the content of art. 5 sec. 2 of Regulation 2016/679, the administrator is responsible for compliance with the provisions of art. 5 sec. 1 of Regulation 2016/679 and must be able to demonstrate compliance with them ("accountability"). In turn, pursuant to art. 7 sec. 1 of Regulation 2016/679, if the processing is based on consent, the administrator must be able to demonstrate that the data subject has consented to the processing of his personal data. However, in a situation where consents to data processing granted by potential clients of the Company's Shareholders are only oral, it is impossible to prove the consent to the processing of data of potential clients of the Administrators and the scope of the consent given, because the statements of the Company's Shareholders and persons employed by them are in this in terms of insufficient evidence. The above statement applies in particular to the consent to the processing of health data, which must be obtained, pursuant to art. 9 sec. 1 lit. a) of Regulation 2016/679, express nature.

It should be noted that in the matter of consent to the processing of the so-called ordinary data (pursuant to Article 6(1)(a) of Regulation 2016/679), the Article 29 Working Party in the Guidelines on consent under Regulation 2016/679 (WP259 rev. 01) indicated that "in Article 7 sec. 1 of the GDPR clearly indicates the clear obligation for the controller to demonstrate that the data subject has given consent. In accordance with art. 7 sec. 1 the burden of proof rests with the administrator." In addition, the above The Working Group referred to recital 42 of Regulation 2016/679 in its explanations, which states that "if processing is based on the consent of the data subject, the controller should be able to demonstrate that the data subject has consented to the processing operation ". The Working Party also stressed that 'it is up to the controller to prove that the data subject has given valid consent. The GDPR does not specify exactly how this should be done. However, the administrator must be able to demonstrate that the data subject has given consent in a given case. As long as the data is processed, there is an obligation to demonstrate the correct consent. (…) For example, the controller may keep a record of obtained statements of consent, so that it can demonstrate how and when consent was obtained and what information was provided to the data subject at the time of consent. The controller must also be able to demonstrate that the data subject has been informed and the procedure used by the controller met all the relevant criteria for obtaining valid consent. The argument for such a requirement in the provisions of the GDPR is the fact that the controller is responsible for obtaining valid consent from data subjects and the consent mechanisms implemented."

In turn, the European Data Protection Board (EDPB) in Guidelines 05/2020 on consent under Regulation 2016/679 explained that "in art. 4 point 11 of the GDPR clarifies that valid consent requires an "unambiguous" indication of will in the form of a "declaration or clear affirmative action" in accordance with the previous guidelines issued by the WP29. "Explicit affirmative action" means that the data subject must have taken a deliberate action to consent to the specific processing. Recital 32 provides additional guidance in this regard. Consent may be obtained in the form of a written or (recorded) oral statement, including electronically. Perhaps the most literal way to meet the "written statement" criterion is to ensure that the data subject sends a letter or email to the controller explaining exactly what he or she agrees to (…). Written statements may take various forms and sizes that could be compliant with the GDPR. Without prejudice to existing (national) contract law, consent may be obtained in the form of a recorded oral statement, although the information available to the data subject must be duly considered before giving consent. The use of pre-ticked boxes with consent is invalid under the GDPR. Silence or inaction on the part of the data subject, as well as simply continuing to use the service, cannot be considered as an active indication of a

choice.”.

In addition, regarding the requirements for obtaining explicit consent in the case of processing specific data listed in art. 9 sec. 1 of Regulation 2016/679, and thus also health data, the European Data Protection Board (EDPB) in its Guidelines 05/2020 on consent under Regulation 2016/679 indicated: "The term "explicit" refers to the method of expressing consent by the person whose data applies. This means that the data subject must make a clear declaration of consent. The obvious way to ensure that consent is explicit would be to expressly confirm it in a written statement. In appropriate cases, the controller could ensure that a written statement is signed by the data subject in order to dispel any possible doubts and prevent a possible lack of evidence in the future. However, such a signed statement is not the only way to obtain explicit consent, and it cannot be said that the GDPR provides for the obligation to obtain written and signed statements in all circumstances where valid explicit consent is required. For example, in a digital or online context, the data subject may be able to make the required declaration by completing an electronic form, sending an e-mail, uploading a scanned document bearing the data subject's signature, or affixing an electronic signature. In theory, the use of oral statements may also be considered a sufficiently explicit means of obtaining valid explicit consent, but it may be difficult for the controller to prove that all conditions for valid explicit consent were met at the time the statement was accepted.” In the opinion of the President of the UODO, the content of the above-mentioned EDPB Guidelines indicates that an oral statement on consent to data processing, both in the case of "ordinary" and, even more so, "special" data, is not a form that sufficiently guarantees demonstrating unambiguity, and even more so consent. Such a form, in the case of "ordinary" data, could be considered sufficient exceptionally in the event that it would be followed by other, additional actions of the administrator, e.g. by drawing up an appropriate register of consents or audio recording of conversations with data subjects. However, such actions were not taken in the case of Administrators.

Thus, the acquisition and then further, several-day (from 5 to 7) processing of personal data in the scope also including data on the health of potential customers by the Company's Shareholders was carried out without a legal basis and constituted a violation of Art. 6 sec. 1 lit. a) regulation 2016/679 and art. 9 sec. 1 in connection with art. 9 sec. 2 lit. a) Regulation 2016/679. It should be emphasized again that pursuant to Art. 9 sec. 1 of Regulation 2016/679, the processing of data subject to special protection, which includes health data, is generally prohibited, and the Company's Shareholders have not met the conditions for their processing, which are an exception to the above rule, set out in art. 9 sec. 2 of Regulation 2016/679, in the absence of obtaining explicit consent for this processing, referred to in letter a) of the above-mentioned recipe.

In addition, in accordance with the content of art. 4 point 11 of Regulation 2016/679, the "consent" of the data subject means a voluntary, specific, informed and unambiguous indication of will by which the data subject, in the form of a statement or a clear affirmative action, allows the processing of personal data concerning him . Taking the above indication into account, it should be considered that in the case of obtaining personal data of potential customers by the Company's Shareholders, there is no clear evidence that these customers have consented to the processing of their data not only in the form of an unambiguous statement, but also a clear action. The testimonies of witnesses obtained in the course of the inspection clearly indicate that the Company's Shareholders, when obtaining personal data of potential customers, limit themselves only to receiving an oral statement.

It should be noted that in the business relationship between the Company's Shareholders and their potential clients at the stage of submitting the initial assumptions of the offer by the Company's Shareholders to the latter, there are also no clear actions of potential clients that would confirm their consent to the processing of their personal data. Such consent cannot be considered, for example, for potential customers to report to the Company's Shareholders by telephone on their own initiative, since the Company's Shareholders are unable to demonstrate the purpose of such contact or the circumstances that during the telephone conversation or in connection with its initiation, potential customers consent to the processing their data. It should be mentioned that the above telephone conversations were one of several ways of establishing contact with potential customers, and moreover, they were not recorded by the Company's Shareholders, which makes it impossible to verify their content and statements made during them by the Company's Shareholders and potential customers.

In view of the above, it should be considered that the Company's Shareholders processed and continue to process personal data of potential customers without a legal basis (without meeting the conditions set out in Article 6(1)(a) of Regulation 2016/679, and in the case of data concerning their health - Art. 9 sec. 2 lit. a) of Regulation 2016/679, i.e. without obtaining the prior express consent of the data subjects. Due to the fact that the Company's Shareholders do not have any of the prerequisites for data processing, they thus violate Art. 5 sec. 1 lit. a) of Regulation 2016/679 expressing, among others, the principle of processing personal data in accordance with the law.

As indicated in the commentary to Regulation 2016/679 edited by Edyta Bielak-Jomaa and Dominik Lubasz ("GDPR General Data Protection Regulation", published by Wolters Kluwer Polska S.A., 2018, p. 326), "Requirement to ensure compliance with the law data processing operations means not only the need to meet the conditions for the legality of data processing, which

are set out in art. 6 and 9, but also the need to ensure compliance with other provisions on the protection of personal data. This requirement also means the need to ensure compliance with all the provisions governing the activities of data processors."

Administrative proceedings conducted by the President of the UODO are used to control the compliance of data processing with the provisions on the protection of personal data and are aimed at issuing an administrative decision in order to apply corrective powers set out in art. 58 sec. 2 of Regulation 2016/679. Pursuant to art. 58 sec. 2 lit. d) of Regulation 2016/679, the President of the UODO may order the controller or processor to adapt the processing operations to the applicable provisions. Given the fact that the Administrators process personal data, including health data, of potential customers without a legal basis, the President of the UODO ordered them to cease the above-mentioned activities, while reserving that if he obtains the prior express consent of potential customers, said processing may be continued or resumed.

In addition, in accordance with art. 58 sec. 2 lit. i) of Regulation 2016/679, each supervisory authority has the power to apply, in addition to or instead of other corrective measures provided for in art. 58 sec. 2 of this regulation, an administrative fine under Art. 83 of Regulation 2016/679, depending on the circumstances of a particular case. The President of the UODO states that in the case under consideration, there were premises for imposing an administrative fine on the Company's Shareholders. Pursuant to the content of art. 83 sec. 2 of Regulation 2016/679, administrative fines are imposed, depending on the circumstances of each individual case, in addition to or instead of the measures referred to in art. 58 sec. 2 lit. a)-h) and point. j) Regulation 2016/679. Recital 148 of Regulation 2016/679 states that in order to make enforcement of the Regulation more effective, sanctions, including administrative fines, should be imposed for violations of the Regulation - in addition to or instead of appropriate measures imposed by the supervisory authority under this Regulation. If the infringement is minor, the fine may be replaced by a warning. However, due consideration should be given to the nature, gravity and duration of the infringement, whether the infringement was intentional, the actions taken to minimize the damage, the degree of responsibility or any significant previous infringements, the manner in which the supervisory authority became aware of the infringement, compliance with the measures imposed on the controller or processor, the application of codes of conduct and any other aggravating or mitigating factors.

Determining the nature of the violation consists in determining which provision of Regulation 2016/679 has been violated and classifying the violation into the appropriate category of violated provisions, i.e. indicated in art. 83 sec. 4 or in art. 83 sec. 5

and 6 of Regulation 2016/679. The assessment of the severity of the infringement (e.g. low, medium or significant) is indicated by the nature of the infringement, as well as the scope, purpose of the given processing, the number of data subjects affected and the extent of the damage suffered by them. The purpose of personal data processing is related to determining the extent to which the processing meets the two key elements of the "limited purpose" principle, i.e. defining the purpose and compliant application by the controller or processor. When choosing a corrective measure, the supervisory authority takes into account whether the damage has been or may be suffered due to a breach of Regulation 2016/679, although the supervisory authority itself is not competent to award specific compensation for the damage suffered. By circling the duration of the infringement, it can be stated that it was immediately removed, how long it lasted, which consequently allows for the assessment of, for example, the purposefulness or effectiveness of the controller's or processor's actions. The Article 29 Working Group in the guidelines on the application and determination of administrative fines for the purposes of Regulation 2016/679 adopted on October 3, 2017, referring to the intentional or unintentional nature of the infringement, indicated that, in principle, "intention" includes both knowledge and intentional action , in connection with the characteristics of the prohibited act, while "unintentionally" means no intention to cause a violation, despite the controller's or processor's failure to comply with the duty of care required by law. Intentional violations are more serious than unintentional ones, and as a consequence, they are more often associated with the imposition of an administrative fine.

The President of the UODO, when deciding to impose an administrative fine on the Company's Shareholders and determining its amount, in accordance with Art. 83 sec. 2 lit. a)-k) of Regulation 2016/679, took into account as circumstances considered to the detriment of the Company's Shareholders and aggravating the amount of the imposed penalty:

nature, weight and duration of the violation of the provisions of Regulation 2016/679, taking into account the nature, scope or purpose of processing (Article 83(2)(a) of Regulation 2016/679) - violation of the rules for the processing of personal data in connection with the processing of data of potential clients of the Shareholders companies without a legal basis (without demonstrable consent to the processing of personal data, including explicit consent in the field of health data), i.e. violation of the principle of data processing in accordance with the law, was of considerable weight and serious nature due to the fact that the principle the lawfulness of processing is of key importance for the protection of personal data. In addition, as it results from the evidence collected in the course of the inspection carried out at the Company's Shareholders, the processing of the above data collection took place and still takes place in a continuous and planned manner, from the date of entry into force of the

provisions of Regulation 2016/679, i.e. from May 25, 2018, to the date of this decision, i.e. long-term, for a period of at least 4 years. Attention should also be paid to the specific nature of the violation of the provisions of Regulation 2016/679 determined by the fact of processing data subject to special legal protection (concerning health), and also the circumstances of their acquisition and the life situation of the data subjects. Acquiring and then processing data of potential customers by Administrators takes place in conditions of mental and sometimes also physical trauma related to the tragic events that these customers have gone through. Events (mainly traffic accidents) in connection with which Administrators provide their services naturally have such a strong impact on the psyche of potential customers that they can make decisions, including consent to the processing of their data, in a way that is not always fully rational and aware. For this reason, in the above-mentioned conditions, it is of key importance that the Administrators exercise due diligence so that their potential customers have the opportunity to express, in a clear and unambiguous way as to the content of the declaration, their will regarding the processing of their data, including its purpose, manner and scope. Administrators should also make every effort to exclude the possibility of potential customers being under any pressure at the time of granting consent to the processing of their data, e.g. resulting from their poor mental state caused by a traumatic event, such as an accident in which certain people, most often very close to the above people, lost their lives or, to a large extent, their health. In a situation where potential customers express, according to the Administrators' declarations, consents only in oral form, apart from the very fact of violating the provisions of Regulation 2016/679 regarding the rules of expressing the above-mentioned consents and accountability of the Administrators' actions, there can be no question of exercising due diligence in this case, to which the Administrators are generally obliged, to the extent that takes into account the professional nature of the service activities undertaken by them;

unintentional nature of the violation of the provisions of Regulation 2016/679 by the Company's Shareholders, however, under the conditions of gross negligence on their part (Article 83(2)(b) of Regulation 2016/679), i.e. obtaining and processing data of potential customers despite not obtaining them from them , in an accountable manner and in accordance with the provisions of Regulation 2016/679, consents. The Company's partners, as entrepreneurs, should have exercised due diligence when processing the data of potential customers, the more so that this data also included special data, i.e. concerning health. Considering the above, the Company's Shareholders as administrators should take all actions resulting in the fulfillment of the obligations arising from the provisions of Regulation 2016/679. In particular, due to the nature of their business activity, they should have made sure what actions are necessary for the lawful processing of data of potential customers, and then

implement them. The shareholders of the Company abandoned the above-mentioned activities, and the processing of data of potential customers took place on the basis of unspecified and impossible to prove, in the light of the provisions of Regulation 2016/679, oral arrangements with them;

degree of cooperation with the supervisory authority in order to remove the infringement and mitigate its possible negative effects (Article 83(2)(f) of Regulation 2016/679) - due to the fact that the Administrators provided incomplete and general information in connection with the addressed to them by the President of the UODO with requests for explanations, which resulted in the need to conduct it, the degree of cooperation of the Administrators with the supervisory authority should be assessed as insufficient;

categories of personal data affected by the breach (Article 83(2)(g) of Regulation 2016/679) - among the personal data of potential customers processed by the Company's Shareholders, in addition to ordinary data, such as: name, surname, telephone number, etc., also included special data, i.e. health data, referred to in art. 9 sec. 1 of Regulation 2016/679. In view of the above, the Administrators, by processing the personal data of potential customers without provable consent, and in the case of specific data without their express consent, significantly violated the provisions of the abovementioned provisions. regulation. Processing of personal data specified in art. 9 sec. 1 of Regulation 2016/679 is particularly protected, which makes the failure of the Company's Shareholders to obtain relevant consents from data subjects to be assessed even more critically;

how the supervisory authority found out about the infringement, in particular whether and to what extent the controller or processor reported the infringement (Article 83(2)(h) of Regulation 2016/679) - the supervisory authority learned about the infringement of the provisions of Regulation 2016 /679 as a result of inspection activities carried out by him. In addition, it should be stated that the control of the supervisory body was carried out as a result of incomplete, general information received from the Administrators in the course of the supervisory body's explanatory activities preceding the control, conducted under reference number DKN.[...]. In other words, the control of the supervisory authority was carried out as a result of problems in obtaining full and unambiguous information from the Administrators on the processing of data by them as part of their business activity.

The following circumstances were considered mitigating circumstances in this case:

the number of injured data subjects and the extent of the damage they suffered (Article 83(2)(a) of Regulation 2016/679) - no damage caused by the Company's Shareholders to potential customers as a result of breaching the provisions of Regulation

2016/679 was found during the inspection;

previous violations by the Administrators (Article 83(2)(e) of Regulation 2016/679) - no previous violations of the provisions of Regulation 2016/679 by the Administrators have been found;

The imposition and the amount of the administrative fine were not affected by the following circumstances:

actions taken by the Administrators to minimize the damage suffered by the data subjects (Article 83(2)(c) of the Regulation 2016/679) - actions taken by the Administrators were not taken into account due to the fact that no damage was incurred by the persons whose the data concern;

the degree of responsibility of the Administrators, taking into account the technical and organizational measures implemented by them pursuant to art. 25 and 32 of Regulation 2016/679 (Article 83(2)(d)) - technical and organizational measures to protect personal data processed by the Administrators were not subject to control by the President of the UODO;

the fact that no corrective measures specified in art. 58 sec. 2 of Regulation 2016/679 (Article 83(2)(i) of Regulation 2016/679) - no decision by the President of the UODO of corrective measures specified in art. 58 sec. 2 of Regulation 2016/679;

the use of approved codes of conduct under Art. 40 or approved certification mechanisms under Art. 42 (Article 83(2)(j) of Regulation 2016/679) - the Company's shareholders do not apply approved codes of conduct pursuant to Art. 40 of Regulation 2016/679 or approved certification mechanisms under Art. 42 of Regulation 2016/679;

financial benefits achieved directly or indirectly in connection with the infringement or losses avoided (Article 83(2)(k) of Regulation 2016/679) - during the inspection, no impact of the violation of the provisions of Regulation 2016/679 on achieving financial benefits by the Administrators or avoiding losses was found .

When deciding whether to impose an administrative fine, as well as determining its amount, the President of the UODO considered the most important to be the serious nature of the infringement resulting from the violation of the principle of compliance with the law in connection with the failure to obtain express consent to the processing of data of potential customers by the Company's Shareholders, in particular their data regarding health, so that the processing of the above-mentioned data people without any legal basis.

When imposing a penalty in this case, the President of the UODO also took into account the content of Art. 83 sec. 3 of Regulation 2016/679, according to which, if the controller or processor intentionally or unintentionally violates several provisions of this regulation as part of the same or related processing operations, the total amount of the administrative fine

does not exceed the amount of the fine for the most serious infringement.

Referring to the amount of the administrative fine imposed on the Shareholders of the Company, the President of the UODO decided that in the circumstances of this case, i.e. in violation of the principle of compliance with the law expressed in Art. 5 sec. 1 lit. a) of Regulation 2016/679, art. 83 sec. 5 lit. a) Regulation 2016/679. In accordance with these provisions, violations of the basic principles of processing referred to in art. 5 of Regulation 2016/679, are subject to an administrative fine of up to EUR 20,000,000, and in the case of an enterprise - up to 4% of its total annual global turnover from the previous financial year, with the higher amount applicable.

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

Considering the above, the President of the Personal Data Protection Office, pursuant to art. 83 sec. 3 and art. 83 sec. 5 lit. a) Regulation 2016/679 in connection with Art. 103 of the Act on the Protection of Personal Data, for the infringements described in the operative part of this decision, imposed on the Company's Shareholders - using the average euro exchange rate announced by the National Bank of Poland on January 28, 2022 (EUR 1 = PLN 4.5697) - an administrative fine in PLN 45,697 (equivalent to EUR 10,000).

In the opinion of the President of the Personal Data Protection Office, the applied administrative fine in the amount of PLN 45,697 (forty-five thousand six hundred and ninety-seven zlotys) fulfills 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 considered that the penalty will be effective if its imposition will lead to the Company's Shareholders processing personal data of potential customers on the basis of their consents (and in the case of health data processing - explicit consents) granted in such a form that demonstrating their obtaining and their scope by the Company's Shareholders will not raise doubts in the event of another inspection by the President of the UODO.

In the opinion of the President of the UODO, the fine applied is proportional to the infringement found, especially due to the

failure to fulfill the obligations of the Company's Shareholders as Administrators at least from May 15, 2018, i.e. from the date of entry into force of the provisions of Regulation 679/2016.

Referring to the amount of the administrative fine imposed on the Company's Shareholders, the President of the UODO considered that it is proportionate both to the seriousness of the infringement found in this case and to the financial situation of the Company's Shareholders and will not constitute an excessive burden for them. The submitted profit and loss account shows that the revenues from the activities of the Company's Shareholders in the period from January 1, 2021 to December 31, 2021 amounted to PLN 3,868,531.36 (three million eight hundred and sixty-eight thousand five hundred and thirty-one PLN 36/100), therefore, the amount of the administrative fine imposed in this case is approximately 1.18% of the revenues earned by the Company's Shareholders in the period for which the Company's Shareholders presented financial data. At the same time, it is worth emphasizing that the amount of the fine imposed (PLN 45,697.00) is only approx. 0.05% of the maximum amount of the fine that the President of the UODO could - applying, in accordance with Art. 83 sec. 5 of Regulation 2016/679, the maximum threshold of EUR 20,000,000 (according to the average euro exchange rate of January 28, 2022 - PLN 91,394,000) - impose on the Company for violation of the provisions of Regulation 2016/679 found in this case.

The dissuasive nature of the fine is related to the prevention of future violations and paying more attention to the implementation of the Administrator's tasks. The penalty is intended to deter both Administrators from re-infringement and other entities involved in data processing. By imposing with this administrative decision a fine for violation of the provisions on the protection of personal data, the President of the UODO took into account both aspects: firstly - repressive nature (the Company's Shareholders violated the provisions of Regulation 2016/679), secondly - preventive nature (both the Company's Shareholders and other entities involved in the processing of personal data will be more attentive and diligent to fulfill their obligations under Regulation 2016/679). In other words, in the opinion of the President of the UODO, the administrative fine will fulfill a repressive function, as it will be a response to the violation by the Company's Shareholders of the provisions of Regulation 2016/679, but also a preventive one, as the Company's Shareholders themselves will be effectively discouraged from violating the protection provisions in this way personal data in the future.

The purpose of the imposed penalty is to oblige the Company's Shareholders to properly perform the obligations arising from Regulation 2016/679, and consequently to conduct data processing processes in accordance with applicable law. It should be emphasized that the penalty will be effective if its imposition will lead to the Company's Shareholders adapting their data

processing processes to a lawful state. The application of an administrative fine in this case is necessary also considering that the Company's Shareholders completely ignored the obligation to obtain explicit consent to the processing of their potential clients' data, in particular in the field of health data.

In the opinion of the President of the UODO, the applied administrative fine fulfills 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. In connection with the above, it should be indicated that the administrative fine in the amount of PLN 45,697.00 meets the conditions referred to in Art. 83 sec. 1 of Regulation 2016/679 due to the seriousness of the violation found in the context of the basic principle of Regulation 2016/679 - the principle of lawful data processing.

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

Print article

Metadata

Provider:

Inspection and Infringement Department

Produced information:

John Nowak

2022-11-30

Entered the information:

Lukasz Sierdzinski

2023-01-10 14:27:24

Recently modified:

Edith Magziar

2023-01-12 10:33:21