Warsaw, on 07

February

2023

Decision

DKN.5131.31.2021

Based on Article. 104 § l of the Act of June 14, 1960 Code of Administrative Procedure (Journal of Laws of 2022, item 2000, as amended), 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, as amended), as well as art. 57 sec. 1 lit. a) and h), Art. 58 sec. 2 lit. e) and i), Art. 83 sec. 1-3, art. 83 sec. 4 lit. a) in connection with art. 28 sec. 1, 3 and 9, art. 33 sec. 1 and art. 34 sec. 1 and 2 and art. 83 sec. 5 lit. a) in connection with art. 5 sec. 1 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 regulations on the protection of of data) (OJ L 119 of 4.05.2016, p. 1, OJ L 127 of 23.05.2018, p. 2 and OJ L 74 of 4.03.2021, p. 35), hereinafter referred to as Regulation 2016/679, after conducting administrative proceedings initiated ex officio regarding the processing of personal data by the Housing Community "(...)" in S., President of the Office for Personal Data Protection

I. finding a violation by the Housing Community "(...)" in S. of the provisions of: a) Art. 5 sec. 1 lit. a) and Art. 28 sec. 1, 3 and 9 of Regulation 2016/679, consisting in entrusting by the Housing Community with its registered office in S., ul. (…), (…) M.G. conducting business activity under the business name “(…)”, ul. (…), processing personal data of members of this Community without a written entrustment agreement and without verifying whether the processor provides sufficient guarantees to implement appropriate technical and organizational measures so that the processing meets the requirements of Regulation 2016/679 and protects the rights of data subjects, b) 33 sec. 1 of Regulation 2016/679, consisting in failure to notify the President of the Office for Personal Data Protection by the Housing Community "(...)" in S. of a breach of personal data protection without undue delay, no later than 72 hours after finding this breach, c) art. 34 sec. 1 and 2 of Regulation 2016/679, consisting in the lack of notification by the Housing Community "(...)" in S. of a breach of personal data protection without undue delay to the data subjects, and failure to provide these persons with at least the information and measures about which referred to in art. 33 sec. 3 lit. b), c) and d) of Regulation 2016/679,

imposes on the Housing Community "(...)" in S. an administrative fine of PLN 1,556.28 (in words: one thousand five hundred and fifty-six zlotys and twenty-eight groszy).

II. orders to notify, within 3 days from the date of delivery of this decision, the persons whose data was processed on the stolen copy of the notarial deed, about the violation of the protection of their personal data, in order to provide these persons with the required information and measures in accordance with art. 34 sec. 2 of Regulation 2016/679, i.e.: • a description of the nature of the personal data breach; • name and surname and contact details of the data protection officer or other contact point from which more information can be obtained; • description of the possible consequences of a personal data breach; • a description of the measures taken or proposed by the administrator to remedy the breach - including measures to minimize its possible negative effects.

Justification

On [...] October 2020, the Office for Personal Data Protection received an anonymous notification regarding the possibility of a breach of the protection of tenants' personal data by the Housing Community "(...)" in S., hereinafter referred to as the Community, submitted according to properties by (...) the Tax Office in B. From contained in the above the notification of information showed that "(...) unauthorized disclosure of personal data (...)" could have taken place at (...) M.G., conducting business activity related to professional real estate management (including for the benefit of the above-mentioned Community) under the name "(...)" with its place of performance at ul. (...), hereinafter referred to as the Administrator. The case "(...) leak[u] of tenants' personal data (...)" was registered by the local Office under reference number DKN.[...].

The President of the Office for Personal Data Protection, hereinafter referred to as the President of the Personal Data Protection Office, on the basis of the received signal about the possibility of violating the provisions on the protection of personal data, on [...] November 2020, pursuant to art. 58 sec. 1 lit. a) and e) of Regulation 2016/679 to the Community for clarification whether, in connection with the security incident in question, an analysis was carried out in terms of the risk of violation of the rights or freedoms of natural persons necessary for the assessment and whether there was a data protection violation, resulting in the need to notify both the supervisory authority as well as the data subjects. In the response given to the authority on [...] November 2020, the Administrator confirmed that it provides real estate administration services to the Community and that in February 2020 the Community's documentation containing the following categories of personal data was stolen: "(...) names and surnames of individual owners, addresses of residences, account numbers from which the

owners paid rent, details of companies providing services in this building (...)". The Community Manager also reported that "(...) [s]law has been reported to the [Police] (...)", and "(...) the case of the theft of documents is dealt with by the Prosecutor's Office in B. (...)".

In connection with the response received from the Administrator, the President of UODO, in a letter of [...] November 2020, asked (...) M.G. to: inform whether the Administrator notified the data controller, which is the Community, about the breach of data protection in question, in accordance with joke. 33 sec. 2 of Regulation 2016/679, and if so, when and in what form; an indication of what kind of documents were stolen, as well as a presentation of the scope of the category of personal data of the owners of the premises processed in the stolen documentation. In the absence of a response, the President of UODO on [...] January 2021 again asked the Administrator to provide the above-mentioned information, and also to indicate whether he is in constant contact with the data controller, and in the case of an affirmative answer, to provide the address of the Community.

In the reply of [...] January 2021, the administrator informed that "(...) the case of the loss of documents of the housing community in S. was reported on [...] February 2020 (...)", he also mentioned that "(...) [on] February 2020 (...)" convened "(...) a meeting of the owners of the above-mentioned building, they were informed about the situation. The documentation that was lost included reports from the inspections carried out: gas, technical, chimney sweep, there were also bank statements of the community, invoices from suppliers (...)". He also indicated that "(...) the bank statements contained the names and surnames of the payers, their addresses of residence and, in some cases, bank account numbers if the owner paid the rent online. (…)"

On [...] February 2021 and [...] March 2021, the President of the UODO repeated requests to determine whether an analysis of the risk of infringement of the rights or freedoms of natural persons necessary to assess whether there was data protection breach, resulting in the need to report this fact to the President of the UODO and possible notification of the fact of its occurrence to data subjects, however, the above letters remained unanswered until [...] July 2021. At that time, in a letter sent to this Office, the Community, without directly referring to the issues raised by the President of the UODO in earlier letters, explained that "(...) [about] the loss of documentation we were notified immediately after the theft of documents - these were account statements community (there are the following data: name and surname, address of residence, community account number and payer's account number - if the transfer was made from his account. In one case, a notarial deed was lost - this person reported it to the Police in L. and issued a new ID The meeting of the housing community was held in February 2020 and concerned the above-mentioned case. The investigation into the theft of documents is conducted by the Police

Headquarters in L."

Transfer of the above information indicating a possible breach by the Community as the data controller of the obligations arising from the provisions of Regulation 2016/679, i.e. Art. 33 sec. 1 and art. 34 sec. 1 and 2, constituted - in the opinion of the President of the UODO - a sufficient premise to initiate administrative proceedings ex officio, of which the authority notified the Community in a letter of [...] July 2021, while registering these proceedings under reference number DKN.5131.31.2021. At the same time, the President of the UODO asked the Community to indicate the scope of the data category and the number of persons affected by the breach of personal data protection in connection with the lost copy of the notarial deed, including information whether the data subject or persons concerned have been notified by the Community of the fact breach of the protection of their personal data.

The President of UODO, in a letter of [...] July 2021, asked the Community to clearly indicate the form of the notification sent by it to the data subjects, and in the case of choosing the oral notification option, to provide circumstances that would sufficiently justify such a notification form of communication with data subjects in the context of the wording of art. 12 of Regulation 2016/679. In addition, the supervisory authority called for information whether, in connection with the occurrence of the breach of the protection of personal data of Community members, an analysis of the risk of infringement of the rights or freedoms of these persons was carried out, and in the event of an affirmative answer, to present the results of the evaluation carried out by the Community. In the aforementioned letter, the President of the UODO also requested information on whether, and if so, when and how the Administrator notified the Community of the occurrence of the personal data breach in question. The authority also requested a photocopy of the resolution on the appointment of the Management Board of the Housing Community "(...)" in S.

Without directly referring to the issues raised in the above-mentioned in writing, the Community, in a letter dated [...] August 2021, raised, inter alia, that "(...) information about the theft of documents, about notifying [the] police and that among these documents there was probably one photocopy of a notarial deed (...)" was obtained during a meeting of the Community convened by the Administrator, during which one of the persons whose data was shown in the document in question "(...) decided (...) to submit an individual application [note of the fact of its theft] to the [P]police (...) and application for a new identity card (...)". In the above-mentioned correspondence, the Management Board of the Community, citing ignorance of the provisions on the protection of personal data, also admitted that so far it was convinced that the notification submitted by the

Administrator to the law enforcement authorities about the possibility of committing a crime in connection with theft committed at its headquarters "(...) is sufficient (...)" in the scope of handling the personal data breach in question.

Due to the incompleteness of the explanations, the President of the UODO, in a letter of [...] September 2021, again asked the Community to precisely define the type of communication channel used to notify data subjects of the fact of a breach of the protection of their personal data, in during a meeting of Community members led by the Administrator. Notwithstanding the foregoing, the supervisory authority also requested information on the circumstances in which the Administrator notified the Community of the occurrence of the breach of personal data protection, including specific information provided to the Community in connection with the theft/loss of documents containing personal data, as well as the scope of information transferred during the meeting of Community members to persons whose personal data was included in the lost notarial deed.

In view of the inaccuracies in the collected evidence regarding the actual number of people whose privacy was covered by the breach of personal data protection in question, the President of the UODO also asked for the Community to take into account the people whose data were shown on the lost bank statements and "(...) the protocol [ach] from the inspections (...)", including specifying the number of persons whose data was processed on the lost notarial deed. The authority also asked for disclosure - if it was concluded - the content of the existing agreement between the Community and the Administrator for entrusting the processing of personal data within the meaning of Art. 28 of Regulation 2016/679.

On [...] September 2021, the President of the UODO called on the Administrator to: provide the date of the Administrator's notification to the Community of the fact of the breach of personal data protection in question, along with a description of the information provided to the Community in connection with this event; informing how long after the theft/loss of documents the Administrator organized a meeting for the owners of the premises at ul. (...), including an indication of the specific date of providing information by the Administrator about the date of the planned meeting of Community members, along with a photocopy of the letter informing about the planned meeting and the date on which the meeting actually took place. In addition, the authority asked the Administrator to clearly indicate whether the data subjects were notified of a breach of the protection of their personal data in writing or orally during the above-mentioned meetings of Community members - and in the event of a decision to choose the second of these communication channels - to indicate the premises justifying such a choice in the context of the wording of art. 12 of Regulation 2016/679. In the letter in question, the authority also sought the scope of information about the breach of personal data protection provided to persons whose personal data was included in the lost

notarial deed, during the meeting of members of the Community, and also sought to determine whether a contract for entrusting the processing of personal data was concluded between the Community and the Administrator , in accordance with art. 28 of Regulation 2016/679 - the President of the UODO also requested disclosure of its possible content.

In the reply sent to the local Office on [...] September 2021, the Administrator indicated, among others, that "(...) [o]people attending this meeting [note. convened on [...] February 2020] were orally [note edited by him] informed about what happened, including the person whose documentation contained a photocopy of the notarial deed." At the same time, emphasizing his state of significant emotional agitation related to the occurrence of the breach of personal data protection in question, the Administrator admitted that although "(...) the regulations say one thing, none of us thought to report the matter to the Office for Personal Data Protection (...) ". He also raised the issue of the expiring - with a three-month notice period - the legal relationship between him and the Community.

It was only in the document dated [...] October 2021 that the Administrator commented in more detail on the issues raised by the President of the UODO in the letter of [...] September 2021, declaring that he had informed the Community about "(...) the theft documents (...)", which was supposed to take place "(...) [on [...] February 2020 (...)" "(...) [at] the meeting of (...) the Community convened on [...] .] February 2020." He also mentioned that the issue of informing members of the Community about the planned meeting regarding the breach of personal data protection in question was to be dealt with - at his request - by the Community Board, by "(...) posting information on the stairwells about the meeting (...)". Moreover, the Administrator noted that "(...) information about the theft of documents, including a notarial deed of one of the owners (...)" was provided "(...) orally (...)", and due to the fact that the stolen photocopy of the deed notarial, the categories of this person's data were visible in the form of their name and surname, series and ID card number, address of residence and PESEL number, "(...) the owner of the notarial deed (...) also reported the theft of a photocopy of the notarial deed to the [P]police in L. (theft of personal data) and submitted the relevant documents to change the identity card." Finally, the Administrator made a statement according to which "(...) between the Personal Data Administrator [note editors, i.e. the Community] and the data processor [note red., i.e. the Administrator], no contract for entrusting the processing of personal data has been concluded."

Following the aforementioned in a letter of [...] October 2021, the Community's response to the request of the President of the UODO of [...] September 2021 to provide further explanations in the case in question was received, which was largely a continuation of the Administrator's narrative regarding the circumstances of convening and of the meeting of members of the

Community, which took place on [...] February 2020. A certain novelty in relation to the explanations provided by him was the information that the stolen copy of the notarial deed contained the personal data of the wife of the owner of the property whose lost the document concerned. The information provided by the Community also did not show that at the meeting of Community members on [...] February 2020, "(...) the scope of information contained in the notarial deed was discussed in detail (...)". It was assured that the documentation regarding the settlements for 2020 lost as a result of theft contained "(...) the names of all tenants (...)" who made payments to the Community, while the inspection reports contained only "(...) data of the building." It was also indicated that the contract "(...) for real estate administration (...)" concluded between the Community and the Manager in (...) "(...) has not been drawn up an annex regarding entrusting the processing of personal data." It should be emphasized that despite the correspondence with the local Office from [...] July 2021 and the use of the phrase "personal data breach" of at least one of the tenants in the above-mentioned letter several times, the Community did not report this fact to the President UODO, in accordance with the provisions of art. 33 sec. 1 of Regulation 2016/679.

In view of the disclosure of new circumstances in this case in connection with the declarations of both the Community and the Administrator about the lack of parties to the personal data processing agreement, the President of the UODO, striving to restore compliance with the law, decided to extend the administrative proceedings conducted against the Community to include the possibility of its violation of art. 5(1)(a) a) and Art. 28 sec. 1, 3 and 9 of Regulation 2016/679, of which the supervisory authority notified the party in a letter of [...] October 2021. At the same time, the President of the UODO called on the Community to indicate the means and ways by which it demonstrated that the Administrator guarantees the implementation appropriate technical and organizational measures to ensure that the processing of personal data meets the requirements of Regulation 2016/679 and protects the rights of data subjects.

In response to the above letter from the President of UODO, the Community submitted a photocopy of the "Agreement (...)" concluded with the Administrator on (...), with the annotation that this is the only document specifying the rights and obligations of the parties to the indicated legal node. The community indicated that the attached document was "(...) sufficient for the management of ... the community." The administrator was also to receive "(...) an appropriate power of attorney to regulate (...) receivables and banking matters (...)".

In this factual state, after getting acquainted with all the evidence collected in this case, the President of the Office for Personal Data Protection considered the following.

In accordance with art. 34 of the Act of May 10, 2018 on the protection of personal data (Journal of Laws of 2019, item 1781, as amended), hereinafter referred to as the UODO, the President of the UODO is the competent authority for data protection and the supervisory authority within the meaning of Regulation 2016 /679. Pursuant to Art. 57 sec. 1 lit. (a) and (h) of Regulation 2016/679, without prejudice to other tasks defined under that Regulation, each supervisory authority in its territory monitors and enforces the application of this Regulation; conducts proceedings regarding the violation of this regulation, including on the basis of information received from another supervisory authority or other public authority.

However, pursuant to art. 4 point 7 of Regulation 2016/679, the administrator is a natural or legal person, public authority, unit or other entity that, alone or jointly with others, determines the purposes and methods of personal data processing; if the purposes and means of such processing are specified in Union law or in the law of a Member State, then also in Union law or in the law of a Member State a controller may be appointed or specific criteria for its appointment may be specified.

On the other hand, pursuant to Art. 4 point 12 of Regulation 2016/679, it should be indicated that the term personal data breach should be understood as such a security breach, the consequence of which is accidental or unlawful destruction, loss, modification, unauthorized disclosure or unauthorized access to personal data transmitted, stored or in otherwise processed.

Disposition of the standard of art. 33 sec. 1 of Regulation 2016/679 defines the procedure for the administrator in the event of a security incident that is a breach of personal data protection, imposing on the administrator the obligation to report it without undue delay - if possible, no later than 72 hours after finding the violation the supervisory authority competent in accordance with art. 55, unless it is unlikely that the breach will result in a risk of violating the rights or freedoms of natural persons, and the notification submitted to the supervisory authority after 72 hours is accompanied by an explanation of the reasons for the delay.

Pursuant to Art. 34 sec. 1 of Regulation 2016/679, in the event that a personal data breach may result in a high risk of violating the rights or freedoms of natural persons, the controller is obliged not only to notify the supervisory authority of the occurrence of a personal data breach, but also to notify the person without undue delay the data subject of such a breach. At the same time, pursuant to sec. 2 of the cited provision of law, this notification should describe the nature of the personal data protection breach in a clear and simple language and contain at least the information and measures referred to in art. 33 sec. 3 lit. b), c) and d), and therefore contain information regarding: name and surname and contact details of the data protection officer or designation of another contact point from which more information can be obtained, a description of the possible consequences

of a personal data breach and a description of the measures taken or proposed by the administrator to remedy the breach of personal data protection, including, where appropriate, measures to minimize its possible negative effects.

In these circumstances, the Housing Community with its registered office in S., ul. (...), for the administrator within the meaning of art. 4 point 7 of Regulation 2016/679, because there is no doubt that it is the above-mentioned the entity determined the purposes and methods of processing personal data. Thus, the arguments of the Community raised in the letter sent to the local Office on [...] July 2021, according to which "(...) the data controller of the residents of the Housing Community "(...)" is (...) M.G. [note . ed. The administrator] (…)". The evidence collected in the present case allows for the thesis that the phrase "administration of residents' data" used by the Community, in the sense in which the Community tries to assign it, cannot be identified with the state of actual control over these data, but rather with the activities of their actual processing carried out by (...) M.G. on behalf of and for the Community as part of the implementation of activities commissioned by the Community on the basis of the agreement of (...) activities related to the management of real estate belonging to it. The above findings, which are consistent with the well-established jurisprudence of the Supreme Administrative Court[1], precisely indicating that the status of personal data controller is not held by each data controller, but by the entity actually deciding "(...) on the purposes and means of processing (...)", are also coverage in the explanations provided by the Administrator in the letter of [...] October 2021, where it is referred to as the "processing authority", and indicates the Community as the "personal data controller".

Considering the above arguments, it should be pointed out that it was the Community and only it, as the entity exercising actual control over the processing of data, that was under Art. 33 sec. 1 of Regulation 2016/679, the obligation to notify the President of the UODO of a breach of personal data protection that occurred "(...) [on [...] February 2020 (...)", as a result of "(....) theft of documents from the apartment (...)" rented by the Administrator. There is no doubt that the consequence of the loss of the documentation in question in the form of reports "(...) on the inspections carried out: gas, technical, chimney sweep (...)", bank statements of the Community, invoices from suppliers, as well as "(...) photocopies[i] of the notarial (...)", containing the following categories of personal data - according to the analysis of evidence - 18 members of the Community: PESEL number, series and number of ID card, names and surnames, date of birth, address of residence or residence, bank account number, specimen signature, there was such a breach of the security of the data processed on the above-mentioned data carriers of the data category in the mentioned scope, which led to unauthorized access by unauthorized persons to the set of these personal data processed on behalf of and for the Community by the Administrator. Thus, this incident constitutes a

violation of the protection of personal data of members of the Community as defined in art. 4 point 12 of Regulation 2016/679. Importantly, the premise that requires the controller to report a personal data breach to the supervisory authority is - pursuant to Art. 33 sec. 1 of Regulation 2016/679 - the very fact of a personal data breach. However, this obligation is not absolute, because the administrator may free himself from it, provided that, based on his analysis of the possible impact of this breach on the rights or freedoms of natural persons, in other words, the balance of possible material and immaterial damage that may be associated with the occurrence of this breach for data subjects, demonstrates in accordance with the accountability principle that the risk of updating these negative effects for data subjects on the basis of objectively adopted criteria in a given context of processing is negligible. As indicated by the Article 29 Working Group in the "WP 250 Guidelines for reporting personal data breaches under Regulation 2016/679", hereinafter referred to as the WP 250 Guidelines: "[th]is risk exists where the breach may lead to physical or material or non-material damage to persons whose data has been breached. Examples of such harm include discrimination, identity theft or fraud, financial loss, and damage to reputation." In such a case, the controller should make an appropriate notification to the supervisory authority without undue delay, however, if possible, not later than within 72 hours after finding the breach and provide all the information required under Art. 33 sec. 3 of Regulation 2016/679. At the same time, it should be pointed out that the update of this obligation is not affected by the occurrence of real material or intangible losses in the goods of the data subject, and the appearance of the inherent risk of their occurrence is sufficient. The above statement is reflected in the well-established jurisprudence of the Provincial Administrative Court in Warsaw, hereinafter referred to as the Provincial Administrative Court, which, for example, in the judgment of September 22, 2021[2] considered (he also ruled in a similar way in the judgments of January 21, 2022[3] and July 1, 2022[4]): "It should be emphasized that the possible consequences of the event do not have to materialize. In the content of art. 33 sec. 1 of Regulation 2016/679 indicates that the mere occurrence of a personal data breach, which involves the risk of violating the rights or freedoms of natural persons, implies the obligation to notify the breach to the competent supervisory authority, unless it is unlikely that the breach will result in a risk of violating the rights or freedoms natural persons". On the basis of the arguments cited so far, it can be concluded that the "risk-based approach" shaped by the EU legislator creates obligations of controllers related to personal data breaches. As the President of the UODO explains in his publication on this issue[5]: "Depending on the level of risk of violating the rights and freedoms of natural persons, the administrator is faced with different obligations towards the supervisory authority, as well as persons whose data concern. If, as a result of the analysis, the controller found that the

likelihood of a risk of violating the rights and freedoms of natural persons is low, he is not obliged to report the infringement to the President of the Office for Personal Data Protection. The indicated infringement must only be recorded in the internal register of infringements. In the event of a risk of violation of the rights and freedoms of natural persons, the administrator is obliged to notify the data protection breach to the President of the UODO, as well as to enter an entry in the internal register of violations. The occurrence of a high risk of violation of the rights and freedoms of natural persons, in addition to an entry in the records of violations, requires the administrator to take appropriate action, both towards the supervisory authority (notification of a data protection breach), but also in some cases also towards the data subjects. In the case of breaches that may cause a high risk of violating the rights or freedoms of the data subject, the GDPR introduces an additional obligation to immediately notify the data subject by the controller, unless the latter has taken preventive measures before the breach or remedial measures after the breach (Article 34 section 3 of the GDPR).

Meanwhile, the analysis of the presented facts provides more than enough arguments to support the thesis that the exemplary catalog of negative effects referred to in the WP 250 Guidelines for persons whose data was processed on the basis of a stolen photocopy of a notarial deed may materialize in relation to these persons. Of course, it is not without significance for the implementation of this scenario that these persons can be easily distinguished from the community based on the categories of data covered by the breach, which in particular include the PESEL number, i.e. an eleven-digit numeric symbol that uniquely identifies natural persons, containing m among others: their date of birth and gender designation, i.e. information closely related to the private sphere of these people. In addition, it should be taken into account that as a result of the breach of personal data protection, the confidentiality of this registration number along with the names and surnames of Community members was lost to undetermined perpetrators of burglary and theft, and after all, this list of personal data alone is sometimes sufficient to "impersonate to the data subject and incurring on her behalf and to her detriment e.g. monetary obligations (vide: (...) - where a case was described in which: "Only the name, surname and PESEL number were enough for fraudsters to extort several loans in total for tens of thousands of zlotys. Nothing else matched: neither the ID card number nor the address of residence"). It cannot be overlooked that the breach of personal data protection in question concerned an even wider catalog of personal data, covering - according to the statement of persons whose data was processed on the stolen notarial deed of [...] July 2021 - also such categories as: series and ID card number, address of residence or stay, as well as a specimen signature, which, combined with the criminal activity of persons who came into possession of the above-mentioned information

concerning members of the Community only raises the potential seriousness of the risk of infringement of the rights and freedoms of data subjects. Therefore, expressed on the basis of Art. 87 of Regulation 2016/679, the postulate that the national identification number as a category of data of this special nature should be subject to exceptional protection. The issue of breaches of confidentiality of national identification numbers and the resulting obligations of controllers, both in relation to the supervisory authority and the data subjects, was also addressed by the European Data Protection Board, hereinafter referred to as the EDPB, in its adopted on December 14, 2021. "Guidelines 01/2021 on examples of personal data breach notification, version 2.0" (hereinafter referred to as the EDPB Guidelines 01/2021). Discussing in the document cited the case of "highly confidential personal data sent by mistake by post", in which the social security number was disclosed, which, by the way, is the equivalent of the PESEL number used in Poland, the EDPB decided beyond any doubt that the disclosure of data in the field of: name and surname, e-mail address, postal address and social security number, indicates a high risk of violating the rights or freedoms of natural persons ("involvement of their [injured persons] social security number, as well as other, more basic personal data, additionally increases the risk that can be determined as high"), which thus implies the need to notify the supervisory authority and notify the data subjects of the breach. A similar position was expressed by the Provincial Administrative Court in the cited ruling of July 1, 2022, regarding the case with the reference number: II SA/Wa 4143/21, where in the justification of this judgment it stated that: "One should agree with the President of the UODO that the loss of confidentiality of the number PESEL in conjunction with personal data such as: name and surname, registered address, bank account numbers and the identification number assigned to the Bank's customers - CIF number, is associated with a high risk of violating the rights or freedoms of natural persons. In the event of a breach of such data as name, surname and PESEL number, identity theft or falsification is possible, resulting in negative consequences for the data subjects. Therefore, in the case in question, the Bank should, without undue delay, pursuant to Art. 34 sec. 1 of the GDPR, notify the data subjects of a breach of personal data protection, so as to enable them to take the necessary preventive measures."

Referring the arguments cited above to the presented facts, it must be emphasized that in the event of any doubts as to the performance of duties by administrators - including in situations where the protection of personal data has been breached - it should first be referred to the teleological interpretation of Regulation 2016 /679, take into account the expressed in art. 1 section 2 of this legal act, the rule according to which the basic purpose of the regulations contained therein is always the protection of the fundamental rights and freedoms of natural persons, in particular their right to the protection of personal data.

Thus, in an attempt to meet the above postulate, the Community, being - as it has already been shown - the administrator of the personal data of its members, should have analyzed the risks associated with its occurrence for legally protected values, and about these people. In turn, this analysis, guided - in accordance with the WP 250 Guidelines - by the criteria of the type of personal data breach, the nature, sensitivity and amount of personal data, the ease of identification of natural persons and the seriousness of the consequences for data subjects in connection with this breach, should have taken into account specific circumstances of a personal data breach, including, in accordance with recitals 75 and 76 to the preamble to Regulation 2017/679, the seriousness of the potential effects and the likelihood of their occurrence. This is because a high level of any of these factors affects the level of the overall assessment, which determines the fulfillment of the obligations set out in Art. 33 sec. 1 and art. 34 sec. 1 of Regulation 2016/679. Bearing in mind that due to the scope of the disclosed personal data in the analyzed case, there was - as shown above - the possibility of materializing significant negative consequences for persons whose data was processed on a stolen copy of a notarial deed, the importance of the potential impact on the rights or freedoms of a natural person should be considered high. At the same time, the probability of a high risk arising from the breach in question is not small and has not been eliminated. Thus, it should be stated that in connection with the breach in question, there was a high risk of violating the rights or freedoms of data subjects, which consequently determines the obligation to notify the breach of personal data protection to the supervisory authority and notify data subjects of the breach. The Article 29 Working Party in the WP250 Guidelines indicates that "(...) 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 on the rights and freedoms of natural persons and the likelihood of its occurrence. Of course, the risk increases when the consequences of a breach are more severe, as well as when the likelihood of their occurrence increases. In case of any doubts, the administrator should report the breach, even if such caution could turn out to be excessive."

Summarizing the above, it should be stated that in the case in question there is a high risk of violating the rights or freedoms of persons whose data was shown on the stolen copy of a notarial deed, which in turn results in not only the obligation to report a breach of personal data protection to the supervisory authority, in accordance with art. 33 sec. 1 Regulation 2016/679, which must contain the information specified in art. 33 sec. 3 of this source of law, but also to notify these persons of a violation of the confidentiality of their personal data, in accordance with art. 34 sec. 1 of Regulation 2016/679, taking into account all those indicated in art. 34 sec. 2 of Regulation 2016/679 elements. Undoubtedly, in this case, the Community will not be required to

notify other persons affected by the breach of personal data protection in question, because - taking into account the scope of information regarding these persons, i.e. "(...) name and surname, address of residence, community account number and account of the depositor (…)" – the high-risk condition does not apply to these data subjects. However, in a situation where, as a result of a personal data breach, there is a high risk of violating the rights or freedoms of natural persons, the controller is obliged to implement all appropriate technical and organizational measures to immediately identify a personal data breach and quickly inform the supervisory authority, and in cases of high the risk of violating the rights or freedoms of the data subjects. As an exemplification of the opposite situation to that postulated by the EU legislator, the content of the statement "(...) of persons related to the lost notarial deed (...)", submitted to the authority on [...] July 2021, stored "(...) in the archives of the Housing Community "(...)" in S. by the data administrator (…) M.G. "(...)" (…)", in which these persons indicated that although they had been informed about the scope of the category of personal data covered by the breach in question, in the form of PESEL numbers, series and numbers of ID cards, names and surnames, address of residence or stay, as well as specimen signatures, but "(...) about the loss of data (...)" they found out "(...) with a 7-day delay during the meeting of the Community (…)".

As has already been signaled, the implementation of the above obligation should take place as soon as possible, which is confirmed in recital 85 to the preamble to Regulation 2016/679, where it is explained: "In the absence of an appropriate and prompt response, a breach of personal data protection may result in physical damage, material or non-material damage to natural persons, such as loss of control over their own personal data or limitation of rights, discrimination, theft or falsification of identity, financial loss, unauthorized reversal of pseudonymisation, damage to reputation, breach of confidentiality of personal data protected by professional secrecy or any other significant damage economic or social. Therefore, immediately after becoming aware of a personal data breach, the controller should report it to the supervisory authority without undue delay, if feasible, no later than 72 hours after becoming aware of the breach, unless the controller can demonstrate in accordance with the accountability principle that it is unlikely that the breach could result in a risk to the rights and freedoms of natural persons. If the notification cannot be made within 72 hours, the notification should be accompanied by an explanation of the reasons for the delay, and the information may be provided gradually, without further undue delay."

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

to enable that person to take necessary preventive actions. Such information should contain a description of the nature of the personal data breach and recommendations for a given natural person as to minimizing 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. (…)".

The Community, refraining from notifying the President of the UODO of the fact of a breach of the protection of personal data of all its members, and withdrawing from notifying two persons whose data was processed on a stolen photocopy of a notarial deed concerning their real estate, in practice deprived these persons of the possibility of counteracting potential damage. By notifying the data subject without undue delay, the controller enables the natural person to take the necessary preventive measures to protect rights or freedoms against the negative effects of the breach. Article 34 par. 1 and 2 of Regulation 2016/679 aims 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) of Regulation 2016/679 (cf. Chomiczewski Witold (in:) GDPR. General Data Protection Regulation. Comment. edited by E. Bielak - Jomaa, D. Lubasz, Warsaw 2018). Proper fulfillment of the obligation specified in Art. 34 of Regulation 2016/679 is to provide data subjects with quick and transparent information about a breach of the protection of their personal data, together with a description of the possible consequences of a breach of personal data protection and the measures they can take to minimize its possible negative effects, which - taking into account note that both the scope of the categories of personal data covered by the personal data breach in question, as well as the context of processing in which it occurred - may turn out to be fraught with consequences, e.g. by incurring financial liabilities to the detriment of Community members. An excellent example of the materialization of the above-mentioned risk is included - prepared as part of the Social Information Campaign of the RESERVED DOCUMENTS System, organized by the Polish Bank Association and some banks, under the auspices of the Ministry of the Interior and in cooperation with, among others with the Police and the Consumer Federation - infoDOK report[6]. It shows that in the first quarter of 2020, i.e. during the occurrence of this breach of personal data protection, 1,373 attempts to defraud credits and loans for a total amount of PLN 62.1 million were recorded, which means that 15 attempts were made to theft of someone else's personal data for a total of PLN 682,000. PLN, which, in turn, in the light of the negligence shown by the Community consisting in not notifying the President of the UODO of the occurrence of the personal data protection breach in question and not notifying the persons whose personal data was on the stolen copy of the notarial deed, is undoubtedly of great importance.

For comparison, in the fourth quarter of 2021, 2,075 loans were attempted to be extorted, for a total amount of PLN 91.3 million, and the entire year 2021 in terms of the number and amounts was significantly more dangerous than the previous one: a 17% increase in the number of extortion attempts and 32 % increase in total amounts.

In addition, according to the jurisprudence, judgments in cases of fraudulent loans are not uncommon and have been issued by Polish courts in similar cases for a long time - for confirmation, you can even quote the judgment of the District Court in Łęczyca of July 27, 2016 (file reference number I C 566/15), in which fraudsters taking out a loan for someone else's data used a PESEL number, a made-up address and an incorrect ID number (invalid).

It should be emphasized that, acting in accordance with the law and showing care for the interests of data subjects, the Community should have provided data subjects with the best possible protection of personal data without undue delay. To achieve this goal, it was necessary to at least indicate the information listed in Art. 34 sec. 2 of Regulation 2016/679, which the Community failed to fulfill. After all, it cannot be otherwise than in the categories of the Community's failure to fulfill the obligation specified in Art. 34 sec. 1 and sec. 2 of Regulation 2016/679 to consider a situation where data subjects "(...) have been [note by the Administrator] orally informed about what happened, including the person whose documentation included a photocopy of the notarial deed ", because pursuant to the regulation contained in Art. 12 sec. 1 of Regulation 2016/679, the Community was obliged to provide data subjects with all information specified in art. 34 sec. 2 of Regulation 2016/679 in connection with Art. 33 sec. 3 lit. b), c) and d) of Regulation 2016/679, in addition, in a form that allows these persons to read the content of the message sent to them even multiple times. In addition, on the basis of the facts cited, a picture emerges in which only one of the persons whose data was processed on the copy of the notarial deed lost as a result of theft was notified, while the Community's explanations clearly show that "(...)[originally] one person was listed in the notarial deed, and only the second person was added to the missing one." Undoubtedly, in this light, it is useless to look for the Community to fulfill the obligation to notify this person of a breach of confidentiality of his personal data, even assuming that he was properly informed by the tenant present at the meeting, whose personal data was also on the lost copy of the notarial document. This is not only due to the literal interpretation of Art. 34 sec. 1 of Regulation 2016/679, which requires the administrator to be treated as the recipient of the above-mentioned provision of the standard, and not another natural person whose personal data was also affected by the breach. Secondly, the notification should be in the form of a message addressed individually to that person, in a form consistent with the provisions of Art. 12 of Regulation 2016/679, which - in the light of the disclosed circumstances of

the case - did not take place. Finally, neither the Community nor the Administrator were able to present the specific content of the message sent to the data subjects at the meeting of Community members organized on [...] February 2020, which was already in itself determines the inability of the Community to demonstrate that it duly fulfills the information obligation towards data subjects, in accordance with the principle of accountability, and taking into account the statement contained in the letter of [...] October 2021, in which the Management Board Community pointed out that he does not remember "(...) whether the scope of information contained in the notarial deed was thoroughly discussed at the meeting (...)", the method and level of detail of providing information during the above-mentioned meetings as insufficient.

At the same time, it should be emphasized again that when applying the provisions of Regulation 2016/679, it must be borne in mind that the purpose of this regulation (expressed in Article 1(2)) is to protect the fundamental rights and freedoms of natural persons, in particular their right to the protection of personal data, and that protection of individuals in connection with the processing of personal data is one of the fundamental rights (first sentence of recital 1 to the preamble of Regulation 2016/679). In case of any doubts, e.g. as to the performance of duties by administrators - not only in a situation where personal data protection has been breached, but also when developing technical and organizational security measures to prevent them - these values should be taken into account in the first place.

Thus, on the basis of the evidence gathered in the case in question and in the light of the arguments cited above, the allegation of breach by the Community of its obligations under Art. 33 sec. 1 of Regulation 2016/679, in the absence of reporting the breach of personal data protection to the President of the Personal Data Protection Office, and art. 34 sec. 1 and sec. 2 of Regulation 2016/679, due to the failure to notify the persons whose data were contained in the stolen photocopy of the notarial deed of the violation of the confidentiality of their personal data, it should not raise any doubts. It is clear from the factual findings made in the case in question that the Community was - based on the information provided by the Administrator on [...] February 2020 - fully aware of the violation of the protection of personal data of its members, and yet it did not take then no steps to properly report this fact to the supervisory authority within the time limit prescribed by the standards. What is particularly reprehensible, she has not taken such an initiative to this day, despite the fact that from [...] July 2021 she exchanged correspondence with the President of the UODO on the subject matter. In this context, the reference by the Community in the letter of [...] October 2021 to the lack of knowledge of the provisions on the protection of personal data, i.a. in the form of lack of "GDPR sensitivity".

The analysis of the presented facts also revealed that the Community did not take any action to provide persons whose personal data were extensively processed on the basis of a stolen notarial deed, of full value, i.e. taking into account all those listed under Art. 34 sec. 2 of Regulation 2016/679 in connection with Art. 33 sec. 3 lit. b), c) and d) of Regulation 2016/679, the communication, limiting itself only to unsubstantiated assurances suggesting that "(...) (...) M.G. [note. editor], the administrator] provided information about the theft of documents orally at the meeting on [...].02.2020 (...)". The fact that one of the tenants affected by the loss of confidentiality of personal data contained in the lost notarial deed made "(...) a decision during the meeting to individually report to the [P]police (...) and apply for a new ID card the next day (...)" in in no way relieved the Community of sending an individualized message to that person in writing, in the content of which it could propose to the data subject a wider range of measures than those that actually happened to him, mitigating the existing risk of negative effects on the well-being of this person. Instead, the Community, recognizing that reporting the fact of the theft of documentation by the Administrator to law enforcement authorities "(...) is sufficient (...)", preferred to count on the common-sense approach of the data subject, de facto also shifting the obligation to notify the breach to the second of persons whose data were shown in the stolen notarial deed.

Regardless of the findings so far, it should be pointed out that the President of the UODO, in the course of these administrative proceedings, also found shortcomings on the part of the Community in the form of entrusting the processing of personal data of its members to the Administrator without concluding a written agreement to entrust the processing of such data and without verifying the processing entity whether it provides sufficient guarantees for the implementation of appropriate technical and organizational measures so that the processing meets the requirements of Regulation 2016/679 and protects the rights of data subjects.

As it has already been shown above, the Community, being the administrator within the meaning of Art. 4 sec. 7 of Regulation 2016/679, entrusted the Administrator - having the status of a processing entity referred to in art. 28 in fine of Regulation 2016/679 - based on joint declarations of will of both parties "(...) as of [...].05.2014 (...) administration of the common property located in S., ul. (…) (…)". The transfer of the mandate to the Administrator to "(...) deal with issues and services within the scope of ordinary management of the common property (...)", in consequence was tantamount to actually entrusting this entity with the processing of personal data of members of the Community, which was reported by the latter in a letter from of [...] October 2021, informing that the Administrator, i.e. (...) M.G. conducting business activity under the name "(...)", ul. (…), "(…)

had access to our data." The fact of entrusting the processing - as established - in a wide range of personal data of members of the Community without maintaining the required - pursuant to art. 28 sec. 3 and sec. 9 of Regulation 2016/679 - content and form was also confirmed by the Administrator, who in the letter of [...] October 2021 informed that "(...) that no data processing agreement has been concluded between the Personal Data Administrator and the data processor personal data processing." At the same time, the analysis of the "Agreement (...)" concluded on (...) between the Community and the Administrator showed that its content is devoid of any mention referring to the protection of personal data of Community members. The evidence collected in this case also does not show that the parties to the aforementioned contract ever sought to regulate mutual rights and obligations in the field of ensuring an appropriate level of protection for the personal data processing processes they carry out, i.e. taking into account the requirements expressed in art. 5 sec. 1 lit. a) and f) of Regulation 2016/679.

Meanwhile, Art. 28 sec. 1 of Regulation 2016/679 clearly indicates that if the processing is to be carried out on behalf of the administrator, he uses only the services of such processors that provide sufficient guarantees for the implementation of appropriate technical and organizational measures so that the processing meets the requirements of this regulation and protects the rights of persons whose data applies. In turn, according to art. 28 sec. 3 of Regulation 2016/679, the processing by the processor takes place on the basis of a contract or other legal instrument that is subject to Union law or Member State law and binds the processor and the controller, specifies the subject and duration of processing, the nature and purpose of processing, the type of personal data and categories of data subjects, obligations and rights of the administrator. Whereas Art. 28 sec. 9 of Regulation 2016/679 defines the form of the legal bond between the controller and the processor, stating that it should be in writing, including electronic form.

Referring the above-mentioned sources of law to the facts disclosed in this case, it should be noted in the first place that the fact of not concluding an agreement to entrust the processing of personal data within the meaning of Art. 28 sec. 3 of Regulation 2016/679 does not deprive the Community or the Administrator of their status, i.e. respectively: controller and processor. It follows from the Guidelines 07/2020[7] that "The concepts of the controller (...) and the processing entity are functional concepts in the sense that their purpose is to divide duties in accordance with the actual roles of the parties and autonomous concepts in the sense that they should be interpreted mainly in accordance with Union data protection law". Assigning sole responsibility for the selection of the processor to the Community, as the controller of its members' data, should

therefore not raise any doubts, especially since Art. 28 in sec. 1 states directly that it is the administrator who entrusts the processing of personal data to a natural or legal person of his choice. The importance of the role of the controller's selection of the appropriate entity that will perform personal data processing operations on its behalf and on its behalf is added by the interpretation of art. 5 sec. 1 lit. a) and f) of Regulation 2016/679, which indicates the need to ensure that the processing of personal data is carried out not only lawfully, reliably and in a transparent manner for the data subject ("lawfulness, reliability and transparency"), but also in a manner that ensures adequate security of personal data, including protection against unauthorized or unlawful processing and accidental loss, destruction or damage, using appropriate technical or organizational measures ("integrity and confidentiality"). Concern for the implementation of the above principles, in particular in the aspect of entrusting the processing of personal data to another entity, should be in the eyes of each administrator, especially in the context of art. 5 sec. 2 of Regulation 2016/679, the accountability principle, which states that the controller is responsible for the processing of personal data in accordance with these principles and must be able to demonstrate compliance with them ("accountability"). Continuation and, at the same time, development of this thought can be found in Art. 28 sec. 1 of Regulation 2016/679, containing the implication that, if the processing of personal data is carried out on behalf of and for the administrator by another entity, then its foundation should be the use by the administrator only of the services of such processing entities that provide sufficient guarantees for implementation appropriate technical and organizational measures so that the processing meets the requirements of this regulation and protects the rights of data subjects. An exemplary catalog of elements that the controller should take into account when selecting a processor that meets the requirements outlined above is included in the Guidelines 07/2020, and these include: "professional knowledge of the processor (e.g. technical knowledge in the field of security measures and data breaches); credibility of the processor; the processor's resources and the processor's adherence to an approved code of conduct or certification mechanism'. Moreover, "the reputation of the processor in the market may also be an important factor that controllers should take into account". In the above-mentioned the source also expressed the view that "The controller is (...) responsible for assessing the adequacy of the guarantees provided by the processor and should be able to prove that he seriously took into account all the elements provided for in the GDPR. The guarantees "provided" by the processor are those that the processor is able to demonstrate to the satisfaction of the administrator, because these are the only guarantees that the administrator can effectively take into account when assessing the fulfillment of its obligations. This will often require the exchange of relevant documentation (e.g. privacy policy, terms of service, register of processing activities,

documentation management policy, information security policy, external data protection audit reports, recognized international certificates such as ISO 27000 standards). The administrator's assessment of whether the guarantees are sufficient is a form of risk assessment, which largely depends on the type of processing entrusted to the processing entity and must be made individually for each case, taking into account the nature, scope, context and purposes of processing, as well as threats to the rights and freedom of individuals. Only this in-depth examination of the competence of the selected processing entity (which, by the way, is also an element of the risk assessment related to the processing of personal data), the traces of which cannot be found when reading the explanations submitted in the course of these proceedings - both by the Community and the Administrator - may only constitute a starting point for the administrator to conclude an appropriate contract for entrusting the processing of personal data. The Guidelines 07/2020 emphasized that "Any processing of personal data by the processor must be regulated by an agreement or other legal act under Union or Member State law concluded between the administrator and the processor, in accordance with the requirements of Art. 28 sec. 3 GDPR. Such a legal act shall be in writing, including electronic form (…)". Importantly, the consequence of not observing the written form of concluding a contract for entrusting the processing of personal data, in the event that no other appropriate legal instrument is in force, the above-mentioned the document requires to be treated as an unambiguous "(...) violation of the GDPR", which, of course, does not diminish the arguments raised above, on the basis of which "the administrator-processor relationship continues to exist in the absence of a written data processing agreement. However, this would mean a violation of Art. 28 sec. 3 of the GDPR".

The administrator's obligations in the field of entrusting the processing of personal data to an entity that meets the requirements indicated in art. 28 sec. 1 of Regulation 2016/679, last at least as long as the entrustment period. As indicated in the abovementioned guidelines »The obligation to use only the services of processors "providing sufficient guarantees" contained in art. 28 sec. 1 of the GDPR is a continuous obligation. It does not end when the contract or other legal act is concluded by the controller and the processing entity. Rather, the controller should verify the processor's guarantees at appropriate intervals, including, where appropriate, through audits and inspections (...)". As follows from the above considerations, the decision to whom the controller should entrust the processing of personal data cannot be taken without grounds - on the contrary - it should be the result of a rational choice that meets the requirements of art. 28 sec. 1 and sec. 3 of Regulation 2016/679 and the criteria cited in the Guidelines 07/2020 as an example. The administrator's failure to comply with the appropriate form or content of the entrustment agreement, or his negligence regarding the obligation to constantly

verify the processor as to the guarantees referred to in art. 28 sec. 1 of Regulation 2016/679, may result in negative effects directly in the privacy sphere of persons whose personal data have been entrusted to the processing entity. And after all - as it has already been signaled - it should be borne in mind that the application of the provisions of Regulation 2016/679 cannot be carried out in isolation from the basic purpose of this normative act, which under Art. 1 section 2 is the protection of fundamental rights or freedoms of natural persons, in particular their right to the protection of personal data. The protection of individuals in connection with the processing of personal data is one of the fundamental rights (first sentence of recital 1 to the preamble of Regulation 2016/679). In case of any doubts, e.g. as to the performance of duties by administrators - not only in a situation where the protection of personal data has been breached, but also when making decisions regarding entrusting the processing of personal data to other entities - these values should be taken into account in the first place, whose protection is consistently served by the requirements set out in Art. 28 sec. 1, 3 and 9 of Regulation 2016/679. Therefore, their violation must be associated with a reaction of the supervisory authority proportionate to the specific circumstances.

As in the case in question, where - in the opinion of the President of the UODO - omissions on the part of the Community constitute a clear exemplification of the opposite situation to that postulated by the provisions of Regulation 2016/679 cited. The evidence collected in the course of these proceedings clearly shows that the Community has not made any checks as to whether the Administrator provides sufficient guarantees for the implementation of appropriate technical and organizational measures so that the processing meets the requirements of Regulation 2016/679 and protects the rights of data subjects. It is also impossible to state that the Community and the Administrator made even informal arrangements in this regard, which would include the elements listed in Art. 28 sec. 3 of Regulation 2016/679. Instead, based on the readings submitted by the above-mentioned entities of explanation, a picture is drawn in which the cooperation of the Community and the Administrator was based from (...) on the basis of a civil law agreement describing mutual rights and obligations only with regard to the management of the common property. This state of cooperation, excluding legally protected values and referring to the sphere of privacy of natural persons who are members of the aforementioned community, continued in an unchanged form until 2021, when the Administrator stated in a letter dated [...] September 2021 that is "(...) on a three-month notice period of the contract with the above-mentioned [C]Community" and this despite the fact that on May 25, 2018, the provisions of Regulation 2016/679 entered into force. The community, not having "sensitivity to the GDPR" and justifying its shortcomings in knowledge in the field of personal data protection regulations by referring to the fact that "(...) [no]one organized [announcement] her

editor] of such trainings [ed. in the field of provisions on the protection of personal data] (...)", refrained from verifying the processing entity in terms of its guarantees of implementing appropriate technical and organizational measures, so that the processing meets the requirements of Regulation 2016/679 and protects the rights of persons whose data concern. The consequence of the approach adopted by the Community to the issue of the protection of personal data of its members was, otherwise, a random event that took place on [...] February 2020. The Community, not caring about basing cooperation with the Administrator on the normative principles of the entrustment relationship processing of personal data, deprived itself of the de facto possibility of shaping its activities. It did not create such a space for its activity in which the processing of personal data of members of the Community by this entity would take place only on its documented instructions. Instead, the state of actual cooperation between the Administrator and the Processing Entity was characterized by discretion in the actions of the Administrator, who autonomously performed personal data processing operations, which is clear from the content of the Community's statement dated [...] October 2021, according to which "(...)[n]we have never requested any notarial deed from the tenants", and after all, the evidence collected in the course of these proceedings clearly shows that the Administrator also performed data processing operations enabling the unambiguous identification of a natural person, contained in the documentation of this kind. Contrary to the Administrator's intentions, this proves that he has failed to meet the requirements set out in Art. 28 sec. 1 and sec. 3 of Regulation 2016/679, which - following the Guidelines 07/2020, is tantamount to violating these provisions. The negligence revealed in the course of these proceedings on the part of the Community - which, after all, still remains the host of personal data processing processes carried out on its behalf and for its benefit - in the context of the lack of an appropriate framework for activity for the Administrator, led to the creation and then a long-term continuation of the state of freedom of its actions. The above gives rise to a thesis according to which the consequences of the breach of personal data protection of [...] February 2020 could be less significant for the members of the Community if the actually existing relationship between the Community and the Administrator was built on the foundation of entrusting the processing of personal data precisely defined rights and obligations of both parties to the contract, where this contract would also regulate the limits of the Administrator's liability for non-compliant with Art. 28 sec. 1 and sec. 3 of Regulation 2016/679, the fulfillment of its obligations and would define mechanisms for possible verification of the implementation of appropriate technical and organizational measures by it, so that the processing meets the requirements of Regulation 2016/679, protects the rights of data subjects and - referring to the above-mentioned Community statements - that the processing of personal data for and on

behalf of the Administrator actually constitutes the materialization of his decision. However, this did not happen in the examined case, and the lack of cyclical evaluations by the Community of the technical and organizational measures implemented by the Administrator to ensure the appropriate level of security, i.e. adequate to the inherently existing risk, of the personal data processing processes carried out on behalf of the Community, meant that The Administrator, without any arrangements with the Community and outside its control, processed the personal data of its members at their place of residence, without having any procedures that would minimize - even to the smallest extent - updating the risk related to the loss of confidentiality of personal data entrusted to it, which not only indicates a violation of Art. 28 sec. 1, 3 and 9, but at the same time indisputably determines the Community's violation of Art. 5 sec. 1 lit. a) Regulation 2016/679.

Considering the above findings, the President of the Office for Personal Data Protection, using the powers vested in him specified in art. 58 sec. 2 lit. i) of Regulation 2016/679, according to which each supervisory authority has the power to apply, in addition to or instead of other corrective measures provided for in art. 58 sec. 2 lit. a)-h) and point. j) of this Regulation, an administrative fine under Art. 83 sec. 4 lit. a) and art. 83 sec. 5 lit. a) of Regulation 2016/679, taking into account the circumstances established in the proceedings in question, stated that in the case under consideration there were premises justifying the imposition of an administrative fine on the Administrator.

In accordance with art. 83 sec. 4 lit. a) of Regulation 2016/679, violation of the provisions on the obligations of the administrator and the processing entity referred to in art. 8, 11, 25-39 as well as 42 and 43 are subject in accordance with sec. 2, an administrative fine of up to EUR 10,000,000, and in the case of an enterprise - up to 2% of its total annual worldwide turnover from the previous financial year, with the higher amount applicable.

In accordance with art. 83 sec. 5 lit. a) of Regulation 2016/679, violation of the provisions on the basic principles of processing, including the conditions of consent, referred to in art. 5, 6, 7 and 9 are subject, in accordance with sec. 2, an administrative fine of up to EUR 20,000,000, and in the case of an enterprise - up to 4% of its total annual worldwide turnover from the previous financial year, with the higher amount applicable.

Article 83 sec. 3 of Regulation 2016/679, on the other hand, provides that 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 penalty for the most serious infringement.

In turn, pursuant to the content of art. 103 uodo, 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 publish 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.

In the present case, an administrative fine against the Community was imposed for infringement of Art. 28 sec. 1, 3 and 9 and art. 33 sec. 1 and art. 34 sec. 1 and 2 of Regulation 2016/679 on the basis of the above-mentioned art. 83 sec. 4 lit. a) of Regulation 2016/679, while for violation of Art. 5 sec. 1 lit. a) Regulation 2016/679 - pursuant to art. 83 sec. 5 lit. (a) of this Regulation. At the same time, a fine in the amount of PLN 1,556.28, which - using the average euro exchange rate of January 30, 2023 (EUR 1 = PLN 4.7160) - the equivalent of EUR 330, was imposed on the Community in total for infringement of all the above provisions - pursuant to the provision of art. 83 sec. 3 of Regulation 2016/679 and does not exceed the amount of the fine for the most serious violation found in this case, i.e. violation of Art. 5 sec. 1 lit. a) Regulation 2016/679, which, pursuant to art. 83 sec. 5 lit. a) of Regulation 2016/679 is 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 worldwide turnover from the previous financial year.

When deciding to impose an administrative fine on the Administrator, the President of the UODO, pursuant to art. 83 sec. 2 lit. a-k of Regulation 2016/679 - took into account the following circumstances of the case, aggravating and affecting the amount of the imposed financial penalty:

1) The nature, gravity and duration of the infringement, taking into account the nature, scope or purpose of the given processing, the number of data subjects affected and the extent of the damage suffered by them (Article 83(2)(a) of Regulation 2016/679) - when imposing the penalty, the fact that in the case in question the Community breached a number of provisions of Regulation 2016/679, defining its basic and at the same time key obligations in the field of compliance - expressed in art. 1 section 2 of Regulation 2016/679 - the demand to protect the fundamental rights or freedoms of 18 members of the Community, in particular the right to the protection of their personal data. Refraining from making an appropriate one, i.e. containing all required under Art. 33 sec. 3 of Regulation 2016/679 elements, notification of a personal data breach - and what needs to be emphasized - despite having full knowledge of the fact of its occurrence from [...] February 2020, the Community prevented the supervisory authority from taking a response in accordance with its competences which could lead to limiting the effects of the infringement in question. The above omission on her part, resulting in a reduction in the level of protection of

personal data processed by her and at the same time constituting the Administrator's failure to meet the deadline specified in art. 33 sec. 1 of Regulation 2016/679, should be assessed even more negatively in the context of the Community's failure to notify two persons whose data were processed on a stolen copy of a notarial deed, in accordance with art. 34 sec. 1 and 2 of Regulation 2016/679. Given the wide scope of the documentation of the category of personal data, in particular regarding the PESEL number, enabling unambiguous identification of natural persons and the associated high risk of material damage to the data subjects, the Administrator was even more obliged to notify all these persons without undue delay in a form enabling them repeatedly familiarizing themselves with the content of the message addressed to them, containing a set of all specified in art. 34 sec. 3 of Regulation 2016/679, information on the basis of which natural persons could take countermeasures adequate to the existing risk in order to effectively protect their goods. However, this desired and, at the same time, required by the provisions of Regulation 2016/679, the reaction on the part of the Administrator did not take place and, what is worse, it has not taken place to date, despite the fact that the occurrence of the breach of personal data protection in question was clearly related to the harm of persons whose data was recorded on a stolen copy of a notarial deed. The negative mental experiences of these people can be measured by the fact that one of them, on her own initiative, "replaced her identity card", which indicates a high level of anxiety associated with this person related to the need to protect her goods. What is worse, this person did not receive any support for their efforts from the Administrator, who, contrary to the provisions addressed to him in art. 34 of Regulation 2016/679, did not provide all victims with instructions to comprehensively protect their privacy, which in turn only increased the mental suffering of these people. Of course, it is not without significance for both unfavorable phenomena in the material and intangible spheres of the above-mentioned natural persons in connection with the Administrator's omissions, as well as for the assessment of the seriousness of the breach in question, the circumstances of the event that took place on [...] February 2020, manifested by the actions of third parties of a criminal nature, regarding whom, due to their modus operandi, remain ill will must be assumed as the motive for action.

Notwithstanding the foregoing, these proceedings have shown that the Community has failed to fulfill its obligations related to the verification of the processor and the conclusion of an agreement to entrust the processing of personal data in the appropriate form and content. As a consequence of violating the provisions of Art. 28 sec. 1, 3 and 9 of Regulation 2016/679 was the fact that the Community entrusted the processing of personal data of its members to the Processor, which did not provide any guarantees for the implementation of appropriate technical and organizational measures so that the processing

would meet the requirements of Regulation 2016/679 and protect the rights of data subjects . On the other hand, the result of a long-standing, since May 25, 2018, i.e. from the date of application of the provisions of Regulation 2016/679, the state of violation of the law was the processing by the Administrator of personal data of members of the Community, de facto beyond its control, as to the manner and scope of this processing, which in itself was detrimental to the interests of the data subjects. Nevertheless, the prohibited practice was continued with the consent of the Community until the end of 2021, despite the fact that on [...] February 2020 the breach of personal data protection occurred, which cannot be attributed to the Processor's failure to implement technical and organizational security measures for personal data processing.

The nature of the above-mentioned violations of the provisions of Art. 28 sec. 1, 3 and 9 and art. 33 sec. 1 and art. 34 sec. 1 and 2 of Regulation 2016/679, demands, in the opinion of the President of the UODO - apart from the aspect of duration, persistence and importance of each of these violations separately - also their joint consideration in the context of misappropriation by the Administrator expressed in art. 5 sec. 1 lit. a) of Regulation 2016/679, the principle requiring personal data processing operations to be carried out in accordance with the law, fairly and transparently for the person to whom they relate. There is no doubt that members of the Community had a reasonable right to expect that their personal data would be processed by the Administrator not only in a manner consistent with the rules contained in the abovementioned sources of law, but also with respect for their interests and in a transparent way for them. Of course, these postulates were not met by the pragmatics adopted by the Community, standing in clear opposition to the standards of due conduct set out in Art. 28 sec. 1, 3 and 9, art. 33 sec. 1 and art. 34 sec. 1 and 2 of Regulation 2016/679.

2) Intentional or unintentional nature of the breach (Article 83(2)(b) of Regulation 2016/679) - the evidence collected in the case in question does not show that the failure to notify the President of the UODO of the fact of the breach of personal data protection in question, or failure to notify of data subjects about a breach of the protection of their personal data according to the prescribed standards was an intentional act calculated to intentionally violate the provisions of Regulation 2016/679. We should rather be inclined to conclude that - as in the case of other infringements on the part of the Administrator - entrusting by the Community the personal data of its members to the Administrator without proper verification of this entity and without concluding a relationship of entrusting the processing of these persons' data in the form provided for by law in an agreement with appropriate content , was the result of negligence on the part of the Administrator, caused by insufficient knowledge of the provisions on the protection of personal data, which he reported himself. Nevertheless, the fact that the Administrator's actions

have not been proven to be expedient should not be tantamount to accepting that this premise should not be assessed as aggravating or even treated as a mitigating circumstance. The degree of negligence shown by the Community in the context of violations of the provisions of Art. 5 sec. 1 lit. a), art. 28 sec. 1, 3 and 9, art. 33 sec. 1 and art. 34 sec. 1 and 2 of Regulation 2016/679 is blatant and proves a lack of compliance with the basic principles of personal data protection. Raising the argument of ignorance of the law - or, as the Community prefers, "lack of feel for the GDPR", not only cannot constitute a justification for disregarding the provisions of Regulation 2016/679, and it should be clearly emphasized that attempts of this type of rationalization should undoubtedly always be perceived in aggravating categories, in accordance with the maxim ignorantia iuris nocet.

3) Actions taken by the controller or the processor to minimize the damage suffered by the data subjects (Article 83(2)(c) of Regulation 2016/679) - the controller not only failed to send two persons whose personal data are being processed were on a stolen photocopy of a notarial deed specified in Art. 34 sec. 1 of Regulation 2016/679 of the notification, thus preventing these persons from taking effective action to remedy the breach of the protection of their personal data in question and mitigate its potential negative effects, which already constituted the Community's failure to take action that could contribute to minimizing the damage suffered by these people harm. As fulfillment of the obligation specified in art. 34 sec. 1 and 2 of Regulation 2016/679, oral, incomplete information about the personal data breach in question cannot be considered to be provided to only one data subject, omitting an individual message in a form that allows it to be reproduced multiple times to the other person affected by this breach. Despite the fact that the scope of the categories of data contained in the documentation in question caused - in the opinion of the President of the UODO - a high risk of materializing negative effects on the rights or freedoms of these persons, the Administrator did not take any other actions related to, for example, covering the expenses incurred by at least one of the abovementioned . persons in connection with the need to obtain a new identity card, or the cost of the BIK Alert service, which would measurably reduce the costs incurred by the above. natural persons, damage directly related to the occurrence of the breach of personal data protection in question.

4) Level of Administrator's responsibility, taking into account the technical and organizational measures implemented pursuant to art. 25 and 32 (Article 83(2)(d) of Regulation 2016/679) - the findings made by the President of the UODO allow to conclude that the Community has failed to fulfill the obligations set out in Art. 28 sec. 1 of Regulation 2016/679, regarding the verification whether the Administrator provided sufficient guarantees for the implementation of appropriate technical and organizational

measures so that the processing meets the requirements of this regulation and protects the rights of data subjects, and has not concluded an entrustment agreement in the form provided for by law (Article 28 section 9 of Regulation 2016/679) and indicated in Art. 28 sec. 3 of Regulation 2016/679 of the content. Informally entrusting the processing of personal data to an entity that does not meet the standards set out in art. 28 sec. 1 of Regulation 2016/679 was conducive - in the period from May 25, 2018 to December 2021 - to increase the inherent level of risk related to the processes processed on behalf of the Personal Data Administrator and finally to the escalation of this risk and its materialization on [...] of February 2020, when the Administrator's apartment was broken into and unsecured documentation containing personal data of Community members was taken. It is also impossible to say that the processing of personal data was entrusted in accordance with the organizational measures introduced by the Administrator, i.e. procedures or regulations stipulating the obligation to verify the processing entity and specifying the manner of concluding contracts for entrusting the processing of personal data that would ensure compliance with the requirements of art. 28 of Regulation 2016/679, because neither the Community nor the Administrator presented the characteristics of these measures, which thus clearly determines the Community's violation of Art. 28 sec. 3 of Regulation 2016/679.

5) The 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) - in this case, the President of the Personal Data Protection Office found the cooperation with it on the part of the Community unsatisfactory. This assessment is the result of both the Administrator's lack of timeliness in responding to letters sent to him as part of the explanatory proceedings conducted by the authority, as well as the fragmentary nature of the answers provided. The negative assessment of the Administrator's cooperation with the authority was also undoubtedly influenced by the period associated with the lack of any reaction on the part of the Administrator, i.e. from [...] November 2020, i.e. the date of effective delivery of the first letter to the Community in the case until [...] July 2021, when the Community decided to respond to repeated requests from the President of the Personal Data Protection Office. At the same time, the premises that guided the Community, often formulating statements that do not directly relate to the issues raised by the authority in order to clarify the circumstances of the case in question, remain unknown, which consequently contributed to the extension of the explanatory activities conducted by the supervisory authority. At the same time, it is impossible not to notice that the Community increased the speed of its response to letters addressed to it only from the moment of initiating administrative proceedings by the President of the UODO in this case, and therefore it can

be assumed that, if it were not for this circumstance, hindering the authority's exercise of its powers under Art. 58 sec. 1 lit. a) and e) would be continued by the Community. To sum up, it should be pointed out that obtaining information from the Community corresponding to the minimum scope of the notification specified in Art. 33 sec. 3 of Regulation 2016/679 required sending letters to it several times informing about the obligations incumbent on the administrator and calling for clarification, and at a later stage of the procedure - to supplement and specify the information already provided to the President of the UODO, which undoubtedly determines the Community's failure to meet the deadline specified in article 33 sec. 1 of Regulation 2016/679. On the other hand, as regards the proper fulfillment of the obligation to notify data subjects of a breach (i.e. removing the breach of Article 34(1) and (2) of Regulation 2016/679), it should be pointed out that no action has been taken by the Community to date, despite the formal initiation by the President of the UODO of administrative proceedings in this case.

6) Categories of personal data affected by the breach (Article 83(2)(g) of Regulation 2016/679) - personal data processed on the basis of stolen documentation, including a copy of a notarial deed, did not belong to the specific categories of personal data referred to in article 9 of Regulation 2016/679, however, their wide scope, including such categories of data of natural persons as: PESEL number, ID card series and number, names and surnames, address of residence or residence, as well as a specimen signature is associated with a high risk of violating the rights or freedoms of persons individuals affected by the breach. It should be emphasized that the unauthorized disclosure of such a category of data of a special nature as the PESEL number, i.e. an eleven-digit numerical symbol, uniquely identifying a natural person, containing the date of birth, serial number, gender and control number, remaining closely related to the sphere of privacy of the natural person and also subject to , as a national identification number, exceptional protection under Art. 87 of Regulation 2016/679, in particular when combined - as was the case in this case - with a wider set of personal data, may have a real and negative impact on the protection of the rights or freedoms of natural persons. The Provincial Administrative Court in Warsaw, in its judgment of July 1, 2022, stated that "in the event of violation of such data, such as name, surname and PESEL number, it is possible to steal or falsify identity resulting in negative consequences for the data subjects.

When determining the amount of the administrative fine imposed on the Community, the President of the UODO took into account as a mitigating circumstance the lack of relevant previous, i.e. until the moment of issuing this decision, violations of the provisions of Regulation 2016/679 on the part of the Administrator (Article 83(2)(e) of Regulation 2016 /679).

The fact that the President of the UODO applied sanctions in the form of an administrative fine to the Community in this case,

as well as its amount, was not affected by other ones indicated in art. 83 sec. 2 of Regulation 2016/679 circumstances, i.e.:

1) 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 President of the UODO learned about irregularities in the processes of personal data processing administered by the Community as a result of an anonymous notification from (...) the Tax Office in B. "(...) unauthorized access and disclosure of personal data, account numbers, customer debts, names of some customers, e.g. from the housing community at ul. (…) (…)", then transferred according to the properties to the attention of the President of the UODO. Thus, the Community, as the administrator of its members' data, failed to notify the supervisory authority of a personal data breach that took place on [...] February 2020. In accordance with the WP 253 Guidelines of the Data Protection Working Party, art. 29 on the application and determination of administrative fines for the purposes of Regulation No. 2016/679, "a controller/processor who has shown negligence by failing to comply with the notification obligation or at least failing to notify all details of the infringement as a result of an incorrect assessment of the extent of the infringement, may, according to the authority supervisory authority to merit a more severe sanction - in other words, such a breach is unlikely to be considered a minor one."

2) Observance of the measures previously applied in the same case, referred to in Art. 58 sec. 2 of Regulation 2016/679 (Article 83(2)(i) of Regulation 2016/679) - before issuing this decision, the President of the UODO did not apply any measures listed in art. 58 sec. 2 of Regulation 2016/679, therefore the Administrator was not obliged to take any actions related to their application, and which actions, subject to the assessment of the President of the UODO, could have an aggravating or mitigating impact on the assessment of the violation found.

3) Use of approved codes of conduct pursuant to Art. 40 of Regulation 2016/679 or approved certification mechanisms under Art. 42 of Regulation 2016/679 (Article 83(2)(j) of Regulation 2016/679) - The administrator does not use the instruments referred to in Art. 40 and art. 42 of Regulation 2016/679. However, their adoption, implementation and application is not - as stipulated in the provisions of Regulation 2016/679 - mandatory for controllers and processors, therefore the circumstance of their non-application cannot be considered to the disadvantage of the Controller in this case. In favor of the Administrator, however, the circumstance of adopting and applying such instruments as measures guaranteeing a higher than standard level of protection of personal data being processed could be taken into account.

4) Any other aggravating or mitigating factors applicable to the circumstances of the case, such as financial benefits achieved

directly or indirectly in connection with the infringement or losses avoided (Article 83(2)(k) of Regulation 2016/679) - the President of the UODO did not state for the Administrator to obtain any financial benefits or avoid such losses in connection with the infringement. Therefore, there are no grounds for treating this circumstance as incriminating the Administrator. The finding of measurable financial benefits resulting from the violation of the provisions of Regulation 2016/679 should be assessed definitely negatively. On the other hand, failure by the Administrator to achieve such benefits, as a natural state, independent of the infringement and its effects, is a circumstance that, by nature, cannot be a mitigating factor for the Administrator. This is confirmed by the wording of Art. 83 sec. 2 lit. k) of Regulation 2016/679, which requires the supervisory authority to pay due attention to the benefits "achieved" - occurred on the part of the entity committing the infringement.

Taking into account all the circumstances discussed above, the President of the Personal Data Protection Office decided that the imposition of an administrative fine on the Administrator is necessary and justified by the weight, nature and scope of the infringement of the provisions of Regulation 2016/679 alleged against this entity. At the same time, it should be stated that the application of any other remedy provided for in Art. 58 sec. 2 of Regulation 2016/679, in particular, limiting itself to a reminder (Article 58(2)(b) of Regulation 2016/679) would not be proportionate to the irregularities identified in the processing of personal data carried out by the Administrator and would not guarantee that the Community will not commit similar negligence in the future.

In the opinion of the President of the UODO, the administrative fine imposed on the Community in the amount of PLN 1,556.28 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 the opinion of the authority, the administrative fine imposed on the Community is proportionate not only to the seriousness of the deficiencies revealed in the course of these proceedings, which constitute a violation of a number of provisions of Regulation 2016/679, i.e. expressed in Art. 5 sec. 1 lit. a) of Regulation 2016/679, the principles of legality, reliability and transparency, and reflected in the obligations laid down in art. 28 sec. 1, 3 and 9 and art. 33 sec. 1 and art. 34 sec. 1 and 2 of Regulation 2016/679, but also in the context of the basic objective of Regulation 2016/679, which is the protection of fundamental rights or freedoms of natural persons, in particular the right to the protection of personal data. At the same time, in the opinion of the President of the UODO, the administrative fine in the amount imposed will be effective, because it will achieve the goal of punishing the Community for infringements of the provisions of Regulation 2016/679 with serious consequences, and at the same time it will perform a preventive function, causing the Community to fulfill its

obligations in order to avoid further sanctions in the future make every effort to duly fulfill its obligations related to informing without undue delay both the President of the UODO and the data subjects of the fact of a personal data breach, as well as the processing of personal data through and with the help of a processing entity in a manner taking into account the requirements of art. 28 sec. 1, 3 and 9 of Regulation 2016/679. To recapitulate, in the opinion of the President of the UODO, the administrative fine imposed in this case fulfills its functions 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 requirements and principles of Regulation 2016/679.

Notwithstanding the foregoing, recognizing that by the date of this decision, the breach of law consisting in the failure to notify the data subjects of the breach of the protection of their personal data has not been terminated by the Community, the President of the UODO could not act otherwise than to address it - appropriately to the content of art. 58 sec. 2 lit. e) of Regulation 2016/679 - an order to notify data subjects of a breach of the protection of their personal data in order to provide these persons with all the data required under art. 34 sec. 2 of Regulation 2016/679, information on: description of the nature of the personal data protection breach, name and surname and contact details of the data protection officer or designation of another contact point from which more information can be obtained, description of the possible consequences of the personal data protection violation and description of the measures applied or proposed by the administrator to remedy the breach - including measures to minimize its possible negative effects.

In view of the above, the President of the Office for Personal Data Protection resolved as in the operative part of this decision.

[1] Judgment of the Supreme Administrative Court of January 30, 2002, file ref. II SA 1098/01

[2] Judgment of the Provincial Administrative Court of September 22, 2021, file ref. II SA/Wa 791/21.

[3] Judgment of the Provincial Administrative Court of January 21, 2022, file ref. II SA/Wa 1353/21.

[4] Judgment of the Provincial Administrative Court of July 1, 2022, file ref. II SA/Wa 4143/21.

[5] "Duties of controllers related to personal data protection violations", available at: https://uodo.gov.pl/pl/134/1029.

[6] (...)

[7] Guidelines 07/2020 of the European Data Protection Board on the concepts of controller and processor contained in the GDPR (Version 2.0, adopted on July 7, 2021), hereinafter referred to as Guidelines 07/2020.

Provider:

Inspection and Infringement Department

Produced information:

John Nowak

2023-02-07

Entered the information:

Wioletta Golanska

2023-03-17 12:13:23

Recently modified:

Edith Magziar

2023-03-22 10:28:10