 Decision on appeal with reg. No. PPN-01-169/02.03.2022 DECISION no. PPN-01-169/2022 Sofia, 16/03/2023 Commission for the Protection of Personal Data composed of: Chairman - Ventsislav Karadjov and members - Tsanko Tsolov, Maria Mateva, Veselin Tselkov, at a regular meeting held on 12/10/2022 d., on the basis of Art. 10, para. 1 of the Personal Data Protection Act, Art. 57, § 1, b. "f" of Regulation 2016/679 and Art. 40, para. 1 of the Regulations for the activities of the CPLD and its administration /PDKZLDNA/ examined the merits of complaint No. PPN-01-169/02.03.2022, filed by V.I. Administrative proceedings are developed according to the Administrative Procedure Code /APK/ and Art. 38 of the Labor Code. The Commission for the Protection of Personal Data was referred to the complaint No. PPN-01-169/02.03.2022, filed by V.I. against a telecommunications operator (T.O.) for unlawful processing of personal data in order to create a profile of the applicant in "T.O. application" "The complaint states that from an electronic message received on 17.02.2022 from email-1, he learned that documents containing his personal data /three names, social security number, address, telephone number, email and handwritten signature/, were used were the creation of a profile in "an application of T.O. ". The initiating document was not signed by him, therefore on the same day he requested an explanation from the mobile operator, returning a reply to email-1 and email-2, in which he informed the administrator that he was not the one who signed the application and requested that the profile be cancelled. The complainant sent another objection to email-2 on 23.02.2022, contacting the call center of the mobile operator, but his case was not resolved. In accordance with Art. 26, para. 1 of the APC, the parties are notified of the initiated administrative proceedings, and they are requested to submit an opinion and evidence on the case. In the opinion of T.O. /letter No. ППН-01-169#5/22.06.2022/ it is stated that the applicant is a subscriber of the mobile operator, presenting a contract for the provision of mobile services No. *****, together with Annex No. 1 and No. 2 dated 02.04.2018. The Company has an alternative functionality, in addition to the conventional options for concluding a contract, which allows orders to be placed by means of the so-called "e-signature of the T.O.", representing a series of actions - authorization via mobile phone for contact, ordering via "T.O. application", obtaining a unique identification code for each individual activity. Based on this, to the lot of V.I. added a "consent form" regarding the described contracting mechanism. The mobile operator did not respond to the complainant's objection because his email was treated as malicious. The administrator indicates that, based on the results of the internal check, it was established that the application was not really signed by VI, in view of which measures were taken to remove it from his batch, for which they present a system screen. According to the procedural representative of T.O. there

were no adverse consequences for the applicant, insofar as the case does not concern the provision of a service, respectively V.I. does not owe remuneration. In the period provided for expressing an opinion on the basis of Art. 34, para. 3 of the APC, the applicant indicates / letters with entry No. PPN-01-169#3/07.06.2022 and No. PPN-01-169#8/30.06.2022/ that he did not receive a response from T.O., but was satisfied that the administrator acknowledged its error and that the functionality is disabled. Pursuant to Art. 38, para. 1 of the PDKZLDNA, the Commission issued a Decision on the regularity and admissibility of the complaint at a closed meeting held on 20.07.2022, and the complaint, as regular and admissible, was decided to be examined in substance on 12.10.2022. the administrative proceedings are constituted by the parties V.I. - applicant and T.O. with EIK ******* – defendant. The parties are regularly notified of the scheduled open hearing to consider the merits of the appeal. In additional statements of the defendant / letters with entry No. PPN-01-169#13/17.08.2022 and No. PPN-01-169#15/06.10.2022/ it is stated that the alleged violation became known in the course of the current administrative proceedings, and it was immediately carried out verification and actions are taken to stop the unwanted actions. According to the administrator, there is no violation of the security of personal data in T.O. It is explained that the additional functionality is activated after identification of the person in the physical store of T.O. and signing a consent document. In the specific case, it was found that the signature of the form was not put by the applicant, because the employee in the physical store did not follow the rules for identification of the individual. At the held open meeting of the CPLD, the applicant did not appear or represent himself. The defendant, represented by legal counsel Y.Z., contests the complaint. Presents evidence as follows: Instruction No. 1 for identification of persons in T.O. ; Instruction No. 10 – review of complaints about misuse of personal data; Instruction for identification of a natural person with application; work with sensitive information of T.O.; verification protocol for compliance with the rules for handling personal data and other sensitive information. Expresses the opinion that the evidence presented shows that the company has taken all possible measures. It confirms the expressed position that, based on the performed inspection, it was established that V.I. did not sign the application, respectively did not provide consent within the meaning of the Regulation on the processing of personal data for the purposes of the functionality "application of T.O. ". It represents an alternative method by which the person could enter into or terminate contractual relations with the company. When asked by the Commission, how was the profile in question created in the event that the data subject did not physically appear in a commercial establishment of T.O., and according to the administrator's own requirements, the natural person should be unquestionably identified, legal consultant Y.Z. states that he cannot say how this happened, but due to the fact that

the event took place in February of this year, the video recordings from the store are not stored. When asked by the Commission what actions the administrator has taken so that an incident with the security of personal data of this nature does not occur, legal advisor Ya.Z. indicates that the administrator tries to minimize the chance of abuse, but it is not possible to ensure this 100%. To the question of the Commission, what possibilities does the so-called "e-signature of the T.O." legal consultant Y.Z. indicates that this is an alternative method by which contracts could be concluded, amended or terminated, and the same can only be activated for existing customers of T.O. It indicates that after the personal data breach was detected, additional measures were taken. When asked by the Commission whether there are any follow-up actions for validation upon termination or creation of a new contract, legal counsel Ya.Z. indicates that after submitting a request to conclude, change or terminate the contract, it is visualized as text in the application and the subscriber can express his consent by pressing a button /and not by putting a manual or electronic signature/. Insofar as the mobile operator has prescribed a procedure that when concluding a new contract and applying for new services, as well as when purchasing devices, a text message is sent with prescribed conditions, the data subject should be notified of a possible contractual relationship or the lack thereof of such. When asked by the Commission how the person found out that the functionality in question was activated and whether he received a paper copy of the relevant documentation, the procedural representative of the defendant indicated that according to procedure he should receive a copy of the document, but in the present case the data subject did not receive such. Jurisconsult J.Z., supporting the previous opinions of the administrator, points out that in this particular case it is not a matter of providing some new service, based on which to generate income for the administrator or to create new legal relations between the parties, but it concerns for an alternative way of expressing wishes within the framework of the existing legal relationship between the parties. The applicant's personal data were processed in connection with the current legal relationship between the parties - a contract for the use of mobile services, which the applicant duly fulfilled and the parties have no claims against each other in relation to the implementation. The specific application does not contain any personal data other than those processed on a contractual basis. This method in no way leads to the conclusion of a contract, the provision of service or the purchase of devices, nor does the parameters of the existing service change. According to Ya.Z. no harm has occurred, nor have any malicious actions been taken regarding the signature method created. Upon verification, it was found that the request to create a profile was not signed by the complainant, after which the alternative functionality was deleted from the subscriber's profile. He believes that from the rules and procedures provided, it is clear that the mobile operator has taken numerous

measures with which it tries to minimize both the possibility of abuses and the repetition of similar hypotheses. For these reasons, he appeals to the Commission to adopt the thesis that there is no violation, and in the event of an eventuality - that the same is not essential. In response to a clarifying question by the Chairman of the Commission, in what period V.I. has filed a complaint with the administrator and, more specifically, whether this was done within the two-month period for storing the footage from the video surveillance in the commercial establishment, legal counsel Ya.Z. states that during the verification it was found that the objection to the administrator dated 23.02.2022 against the notification dated 02.17.2022 ended up in the "spam" folder and therefore was not considered, and that according to him the administrator did not was referred to with a complaint. In response to a clarifying question whether there is a requirement in the internal rules of the administrator, if a complaint is filed within the storage period of the video footage, that the same be preserved until the conclusion of the considered dispute, legal consultant Ya.Z. indicates that if there is a complaint, the footage is preserved, as long as this record is available at the time of the complaint being submitted and considered, and the practice indicates that complaints are considered monthly. The Commission draws the attention of the legal representative of the defendant that his defense thesis that the personal data of the complainant were processed on the basis of his contract with the mobile operator is false. In this case, the personal data of V.I. not processed for the purposes for which they were collected. They are collected on the basis of Art. 6, § 1, b. "b" of the Regulation, i.e. for the purposes of concluding a contract, and subsequently processed for a purpose other than the original one - for the creation of additional functionality through which alternative declarations of will can be made on behalf of the natural person, which could create the corresponding rights and obligations for the subject of data, even for reasons beyond his control, as well as without the same having expressed consent within the meaning of the Regulation. Legal consultant Ya.Z. points out that, in his opinion, there is no way to conclude a contract, because even if the "T.O. application" functionality is activated, the person must log in to his account by entering his password. When signing, changing or terminating such a contract is requested, an SMS with a verification code is sent again. With the fact thus established, from the legal point of view the appeal is admissible and well-founded. Regulation 2016/679 and the Personal Data Protection Act define the rules for the protection of natural persons in relation to the processing of their personal data, as well as the rules regarding the free movement of personal data, so that fundamental rights and freedoms are protected of natural persons and, in particular, their right to the protection of personal data. The subject of the complaint is an allegation of illegal processing of personal data by using them for a purpose other than that for which they were originally collected, namely - compiling a

request and activating the online functionality "T.O. application", respectively the creation of the so-called "T.O.'s e-signature", which is not equivalent to an electronic signature within the meaning of the Electronic Document and Electronic Authentication Services Act, but its activation could lead to legal consequences for the data subject. The respondent T.O. is a legal entity - administrator of personal data within the meaning of Art. 4, item 7 of the Regulation and processed the applicant's personal data through a set of operations such as storage and use for purposes other than those it can justify as legitimate, which is a violation of Art. 5, §1, b. "b" of the Regulation. With regard to the claims of the data subject that the mobile operator did not return an answer to his inquiry, it should be noted that the complainant did not submit a request for the exercise of rights within the meaning of Art. 12 et seq. of the Regulation, but has sent a free-text query, based on which the administrator was not obliged to provide an answer. The Commission was also not contacted with a complaint for failure to provide a response - in the data subject's request it was noted that he did not receive a response from the administrator, but the subject of the complaint was unlawful processing of personal data. Had it been properly referred, the administrator could not have relied on the complainant's email being treated as spam. The administrator is obliged to provide a reliable and secure channel for communication with its customers. Due to the fact that the email of V.I. is possibly identified as malicious mail, it follows that appropriate organizational and technical measures were not taken, insofar as the e-mail was received precisely from the e-mail address with which the applicant was identified by T.O. Moreover, the administrator had other data for correspondence with the data subject, such as a telephone number and a physical address, therefore he had the opportunity to contact the individual and cross-check the information that he claimed to be malicious mail, but did not has done The parties do not dispute that there is a contractual legal relationship between them and that on this basis the mobile operator initially processed the person's personal data. In the course of the existing contractual relationship, the administrator continued to process the subject's personal data, having significantly changed the purpose set out in the contract - his data /three names, social security number, address, e-mail address, telephone number and signature/ are accessible by an employee in a store at T.O., after which they are distributed and used for the generation of "Application-declaration for electronic identification and signing of contracts with an electronic signature". There is no dispute between the parties that the application was not signed by the applicant, respectively that he did not provide consent within the meaning of the Regulation for the use of his personal data for the purposes of the additional functionality. The personal data controller and defendant in the present proceedings pleads an error, admitting that the data subject was not properly identified, and that the functionality in question was disabled on

15.06.2022 in the course of an internal audit following the submission of the complaint /so e.g. Annex No. 2 to the opinion of T.O. with entrance No. PPN-01-169#5/22.06.2022 /. Insofar as there is no dispute between the parties that the applicant did not sign the procedural application, as well as due to the fact that there is no evidence to the contrary, it follows that his personal data were used unlawfully for the purposes of creating the additional functionality "e-signature of T.O. ". The same, regardless of the fact that it is not equivalent to an electronic signature in the sense of ZEDEP, represents a mechanism for expressing wills, on the basis of which the controller of personal data considers that contractual relations with the subject could arise, be amended or terminated data. The question of whether this alternative method of expressing wills, the verification of which is not carried out either by placing a handwritten signature or by using an electronic signature, is capable of giving rise to civil law consequences, is not the subject of the Commission's decision. In view of the above, the actions of the administrator in processing personal data were carried out in violation of the principle of "limitation of purposes", regulated in Art. 5, paragraph 1, letter "b" of Regulation 2016/679. The administrator has carried out a check on the case and found that it was not the complainant who signed the application and it was not he who made the request to activate the online functionality of the TO, and this happened due to non-compliance with the rules for the identification of the data subject in the physical mobile operator store /so e.g. Instructions for identifying customers in a store of T.O. /. The same is a violation of the principle of Art. 5, §1, b. "e" of the Regulation, because the personal data is processed in a way that does not guarantee an adequate level of security, including protection against unauthorized processing, which is done by the controller's store employee and not by the data subject. The personal data subject to illegal processing /three names, social security number, address, e-mail address, telephone number, signature/, are those that the administrator has at his disposal on another basis - that according to Art. 6, §1, b. "b" of the Regulation. In this case, special categories of personal data are not processed within the meaning of Art. 9 of the Regulation. In the course of the administrative proceedings and in the open hearing held to examine the complaint, it was found that the administrator had violated its own rules for the identification of natural persons. The administrator learned from the data subject's objection on the same day that V.I. did not sign the declaration requesting the activation of the additional functionality "e-signature of the T.O.", but did not take any action. It can be seen that the objection of the data subject and the request to cancel the created functionality has reached the official correspondence emails with T.O. already on the same day /17.02.2022/. The administrator would not be able to invoke possible doubts about the identity of the person from whom the request originates, insofar as this same administrator was able to carry out an indisputable identification of the data subject

before refusing to consider his request. As far as the storage period for the video surveillance records had not expired at that time, the administrator should, after ascertaining the identity of the data subject, take the appropriate measures to verify the complaint. As can be seen from the evidence presented in the open session, the administrator has internal rules and procedures for the protection of personal data, but from the actions taken in the case it is clear that no systematic control was implemented. The inspection carried out could have been carried out at a much earlier stage, in which the administrator had the opportunity to check the video cameras in the commercial establishment, so that he could certify that V.I. was not inside, respectively – that he did not sign the request for activation of the additional functionality. Regardless of the fact that the applicant immediately notified the administrator of his unwillingness to have his personal data used for the purposes of the alternative method of communication with the mobile operator through the "T.O. application", the latter did not take the necessary actions to stop the violation. The violation is due, in addition to the lack of appropriate organizational and technical measures, as well as the lack of sufficient control over the activities of the employees in T.O.'s store, which did not allow the administrator to process the information in a timely manner and perform the necessary actions in a reasonable time term. The untimely check that the administrator carried out actually led to the ineffectiveness of the measures taken. They do not lead to prevention, as are the requirements of the Regulation, which is why the Commission considers that in order for the imposed measure to have a preventive and deterrent effect, the administrator should be subject to a pecuniary sanction. Corrective measures have been repeatedly imposed on the same administrator in order to improve the organizational and technical conditions with him. In the present case, it was established that the introduced rules were not followed by the employees, which leads to the conclusion of a violation under Art. 5, §1, b. "e" and Art. 24, §1 and §2 of the Regulation, precisely because the introduction of organizational and technical measures includes the control of their implementation.The administrator admits its error, and it is also clear that the measures for the indisputable identification of natural persons, implemented by the administrator, have proved to be inadequate. Even if the contrary were true, the necessary control was not exercised over their compliance.

In the relationship between the mobile operator and the data subject, the actions performed in the "T.O. application" functionality have the force of electronic identification and could have adverse legal consequences for the data subject. The administrator himself does not carry out subsequent identification and verification of the possibly performed actions / pressing a button after "reviewing" the contract does not constitute an action for identification of the data subject/. Nevertheless, it

should be noted that there were no adverse consequences for the data subject, but not because the administrator took appropriate measures allowing the undisputed identification of the data subject, but because V.I. has not entered into a contractual relationship with the administrator.

The Commission has powers according to expediency, on the basis of which it assesses which of the corrective powers under Art. 58, § 2 of Regulation 2016/679 to exercise. The violation expressed in the processing of personal data for purposes incompatible with those originally created - non-compliance with the principle of Art. 5 § 1, b. "b" of the Regulation, was suspended with the deactivation of the created functionality "e-signature of the T.O." on 15.06.2022, therefore the Commission's corrective powers of a warning or suspension nature could not apply, but an administrative penalty should have been imposed, a pecuniary sanction under Art. 58, § 2, b. "and" of the Regulation.

When imposing a pecuniary sanction, the supervisory authority is limited by the relevant limits under Art. 83, § 5, b. "a", in accordance with Art. 5, § 1, b. "b" and b. "e" of the Regulation. In the present case, an effective, proportionate and dissuasive measure would be a pecuniary sanction in an amount close to the minimum – the controller has corrected its error, the data subject has not suffered harm, and the infringement has been stopped in a relatively short period of time. The breach is the processing of personal data of a data subject by storage and use for purposes other than those for which the personal data were originally collected by the controller, and the same continued for a relatively short period of time / less than 4 months or from 17.02.2022 to 15.06.2022/. The personal data of the natural person have not been disseminated to persons outside the employees of the controller. Regardless of the fact that the breach is not accompanied by harm to the data subject, this is due not to the measures taken by the administrator, but to an accidental event. The violation could have resulted in property damage for the individual. By disclosing a profile in the application, private law consequences could arise, and the statement that only the relevant subscriber can use the functionality is not true, insofar as T.O. does not carry out subsequent identification of the natural person, except that in the case under consideration he did not carry out a preliminary one.

A mitigating circumstance is that the administrator stopped the violation on his own initiative during the current administrative proceedings. An annoying circumstance is that the controller has not taken action on the objection of the data subject, insofar as the same does not have scheduled effective mechanisms for subsequent control, or at least has not proven the existence and compliance with such.

The degree of responsibility of the administrator should be categorized as relatively high, bearing in mind that the technical and

organizational measures introduced by him, as well as the control exercised over them, are not sufficient to avoid or stop the violation, given that due to the lack of appropriate organizational and technical measures, and the failure to exercise sufficient control, the person's personal data were accessed by an employee in a T.O. store, he processed them for purposes incompatible with the lawful processing of personal data, and this remained without relevant consequences.

The administrator did not take the necessary measures to stop the violation after already on the same day and subsequently on 23.02.2022 the data subject submitted a feedback communication to T.O. /regardless of the fact that the same does not constitute a request to exercise rights under the Regulation/ that he never signed the documents, and that he does not know how his personal data got into the request to use "e-signature of T.O." . The violation has not been stopped, which means that the administrator does not have properly scheduled internal mechanisms for the prevention and control of the removal of data security violations. The administrator has provided assistance to the supervisory authority to remedy the breach, while mitigating its possible adverse consequences for the data subject by deactivating the functionality. In the current scenario, the administrator did not realize direct or indirect financial benefits, nor did he avoid losses as a result of the violation / this did not happen because of the measures taken by the administrator, but because the functionality was not used by the individual/.

The personal data administrator T.O. has previous violations related to the security of personal data, his actions have repeatedly been subject to sanctions by the Commission, which in a number of its decisions has clarified the application and meaning of the Regulation on the protection of personal data / so e.g. in Decision No. PPN-01-130/2019 the administrator was sanctioned for non-compliance with the conditions for granting consent by the data subject, and in Decision No. PPN-01-313/2019 the administrator was sanctioned for failure to comply with appropriate organizational and technical measures/.

In view of the above and on the basis of Art. 38, para. 3 of the Personal Data Protection Act

RESOLVE:

1. Announces Complaint No. PPN-01-169/02.03.2022 of V.I. against T.O. with EIK **** for a reasonable violation of Art. 24, §1 and §2, in conjunction with Art. 5, § 1, b. "b" and b. "e" of Regulation (EU) 2016/679.

2. Based on Art. 58, § 2, b. "and" and Art. 83, § 5, b. "a" of Regulation (EU) 2016/679 for violation of Art. 5, § 1, b. "b" and b. "f" of the Regulation imposes on the administrator a telecommunications operator with EIK ***** an administrative penalty, a property sanction in the amount of BGN 2000 /two thousand/.

The pecuniary sanction should be paid within 14 days from the entry into force of this Decision to the following bank account of the CPLD in the BNB:

IBAN: BG18BNBG96613000158601 BIC BNBGBGSD

Owner: Commission for Personal Data Protection, BULSTAT 130961721,

otherwise enforcement measures will be taken.

This decision can be appealed within 14 days of its delivery through the Personal Data Protection Commission to the Administrative Court of Sofia - city.

_____

1 "Consent" in the sense of recital 32 of the Regulation means "a freely given, specific, informed and unequivocal statement of consent by the data subject to the processing of personal data related to him ... silence, pre-ticked boxes or inaction shall not to constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. When the processing pursues several purposes, consent must be given for all of them. If the data subject's consent is to be given following an electronic request, the request must be clear, concise and not unduly disrupt the intended use of the service."

CHAIRMAN:

MEMBERS:

Vencislav Karadjov /p/

Tsanko Tsolov /p/

Maria Mateva /p/

Veselin Tselkov /p/

Download files

Decision on appeal with reg. No. PPN-01-169/02.03.2022

print