Decision on appeal with registration № PPN-01-499 / 27.05.2019 DECISION» PPN-01-499 / 2019 Sofia, 27.03.2020 Commission for Personal Data Protection (CPDP, Commission) composed of, Chairman - Ventsislav Karadzhov and members: Tsanko Tsolov and Maria Mateva at a regular meeting held on 05.02. 2020 and objectified in protocol № 5 / 05.02.2020, on the grounds of art. 10, para. 1 of the Personal Data Protection Act (PDPA) in conjunction with Art. 57, § 1, b. "E" of Regulation (EU) 2016/679, considered on the merits a complaint with Reg. № PPN-01-499 / 27.05.2019, filed by R.D. against a health institution (ZZ). In the complaint filed by Ms. R.D. Allegations have been made that after checking the health file, with a unique access code (UCD) provided by RHIF - Sofia, she found that she was hospitalized in the Health Insurance Fund, tests were performed and money was withdrawn from the NHIF. The applicant alleged that she had never been hospitalized by Z.Z. and does not know the doctor who is said to have sent her to the said hospital. She informed that she had visited the hospital as a patient for an outpatient consultation with a cardiologist. She considers that her personal data has been misused. Asks for an inspection of Z.Z. and to impose a sanction. Attached is a copy of an excerpt from the NHIF's "hospitalization" system. In the conditions of the official principle laid down in the administrative process and the obligation of the administrative body for official collection of evidence and clarification of the actual facts relevant to the case, by letter ref. № PPN-01-499 # 1 / 25.07.2019 of Z.Z. EAD is given a deadline for expressing an opinion and presenting relevant evidence. In response, a statement was received from the hospital stating that no misuse of the applicant's personal data had been committed in the case, stating the following arguments: The applicant R.D. from Sofia, is a longtime patient of Z.Z. EAD, which was not hospitalized, including in March 2018. On March 19, 2018, a patient with the same name but from the town of K. and a different PIN was admitted to the hospital for planned treatment, and the referral was signed. by the lady from the town of K. At the registration of the patient R.D. from the town of K., in the Registry Department, her three names were entered in the hospital information system and the system automatically linked them to the data of an already existing patient with the same three names - those of the applicant from Sofia. The Registrar has registered Ms R.D. by K. with the PIN of the applicant from Sofia. For this reason, the hospitalization of R.D. from the town of K. and the related research and procedure are related to the hospital electronic file of the complainant R.D. from Sofia. Upon registration of R.D. from the town of K. for hospital treatment (hospitalization) the data from her ID card in the client part of the registration system of the NHIF "Registration system of events in hospitalization and dehospitalization" (Hadith) was checked, which immediately sends the data to the server part of

the system located in the Central Office of the National Health Insurance Fund. Attached is a printout from the Hospital Information System - reference from Gamma Codemaster - Data from the registration system of the NHIF for the day of hospitalization - March 19, 2018 and the day of hospitalization - March 20, 2018, which shows that the correct PIN is calculated of R.D. from the town of K. For the hospitalization of R.D. from the town of K. a History of the disease (IZ) № **** has been compiled for the period from March 19 to March 20, 2018, which is attached to the opinion according to the inventory. It is evident from the medical documentation that the actual hospital treatment (hospitalization) with the necessary tests were performed on R.D. from the town of K., and not to the applicant. In May 2019 the applicant R.D. from Sofia visited ZZ to conduct a cardiac examination. During the registration, an employee from the Registry Department entered the three names of the patient and information about hospital treatment was released from the hospital information system in the period 19.03. - 20.03.2018. The applicant was orally informed that the reason for entering information about hospital treatment, which she had not provided, would be checked. R.D. from Sofia, has requested and received its DQM for verification of the data in its electronic health file from the regional health insurance fund - Sofia (RHIF). During the inspection of the patient file in the Integrated Information System (IIS) of the NHIF it was established that hospital medical care was reported in her names and PIN to the NHIF in the period 19.03.2018 - 20.03.2018, an excerpt from her file is attached to the complaint of RD from Sofia). On May 25, 2019, R.D. from the city of Sofia has filed a complaint to the CPDP, and on 31.05.2019 has filed a complaint with the same content to the RHIF - Sofia city with ent. № *** / 31.05.2019 (a copy of her complaint to the RHIF in Sofia is attached). As a result of the complaint, the director of the Sofia RHIF has issued Order № *** / 03.07.2019 for an inspection in Z.Z. EAD. The inspection was carried out on 03.07.2019, and for the result of it a Protocol № **** / 18.07.2019 was issued. The mentioned protocol describes in detail how the entered incorrect PIN of the patient R.D. from the town of K. led to incorrect reporting of her medical activity on the clinical path along which she was treated, in the electronic files of the applicant - in the hospital and in the Central Office of the NHIF (copies of the order and protocol are attached). As a result of the findings reflected in the protocol of the inspection, the examiner issued a Protocol for unreasonably received amounts № ***** dated 18.07.2019 - due to the mistake made by the medical institution in the reporting information about the patient R.D. from the town of K. and a sanction was imposed on Z.Z. EAD, which was paid for the treatment of R.D. from the town of K. (a copy of the protocol is attached). From the stated circumstances, they consider that it is evident that due to a technical error, made by chance, in the electronic file of the complainant are reflected medical activities that were performed on Ms. R.D. by K. Inform

that in Z.Z. EAD uses the software products of G.K.K.P. “Board of Directors, which are for automated management of activities related to registration of medical and non-medical data for a patient, generated during his stay in a medical institution, for hospital and specialized pre-hospital medical care, as well as numerous validation and integrity checks of the entered data. Z.Z. EAD has with "G.K.K.P. “Board of Directors and contract for subscription support of software products. The medical institution has requested from “G.K.K.P. “The Board of Directors to perform the necessary actions for the division of the medical data for the two patients with identical three names, located in the Hospital Information System of Z.Z. EAD, in two separate patient files, as the software product of G.K.K.P. does not provide the possibility for the medical establishments to perform such actions independently. On 31.07.2019 from “G.K.K.P. "The Board of Directors has divided the two electronic patient files. Attached is a certified copy of the Medical History of the patient RD, from the town of K., which contains medical documents issued initially with the wrong PIN and medical documents with the corrected PIN. In conclusion, they consider that it can be concluded that in case of a technical error during the registration of the patient from the town of K. in the hospital information system of Z.Z. EAD, there was an accidental change in her PIN, incorrectly reflected in her epicrisis as the PIN of the applicant from Sofia. The wrong PIN was incorrectly filled in the report submitted to the Integrated Information System of the NHIF. This accidental change has so far not had any negative consequences for the applicant. Both women are patients of Z.Z. EAD, as their personal data appear in the hospital information system of the medical institution. With a letter ex. № PPN-01-499 # 3 / 25.-7.2019 from the Regional Health Insurance Fund is required to provide information. In response, an opinion was submitted, which shows that after an inspection it was actually established that the case concerned a technical error made by an employee of the hospital. The considered complaint is fully compliant with the requirements for regularity, according to Art. 28, para. 1 of the Rules of Procedure of the Commission for Personal Data Protection and its administration (PDKZLDNA), namely: there are data about the complainant, the nature of the request, date and signature. The provisions of Art. 38, para. 1 of LPPD deadlines are met, given the provision of para. 44, para. 2 of the Transitional and Final Provisions to the Law on Amendments to the LPPD. The subject-matter is an allegation of unlawful processing of the complainant's personal data and is directed against a personal data controller, which requirement is an absolute procedural prerequisite. In Art. 27, para. 2 of the APC, the legislator links the assessment of the admissibility of the request with the presence of the requirements specified in the text. The competence of the Commission in dealing with complaints is related to the protection of individuals in connection with the processing of their personal data by persons having the quality of "personal data controllers" within the

meaning of Art. 4, item 7 of Regulation (EU) 2016/679 (General Data Protection Regulation, GDPR). At a meeting of the Commission held on 18 December 2019, the complaint was accepted as procedurally admissible and the following were constituted as parties in the administrative proceedings: complainant: R.D., respondent Z.Z. EAD, in the capacity of personal data controller and stakeholder National Health Insurance Fund - Sofia. The parties have been regularly notified of the meeting of the Commission for consideration of the complaint on the merits scheduled for 05.02.2020, and they have been instructed to distribute the burden of proof. According to Art. 10, para. 1 of the Personal Data Protection Act in connection with Art. 57, § 1, b. "E" of the Regulation and Art. 38, para. 3 of the Personal Data Protection Act, the Personal Data Protection Commission considers complaints against acts and actions of personal data controllers, which violate the rights of individuals under the LPPD, as well as complaints of third parties in connection with their rights under this law. In essence, the complaint is well-founded. According to the definition in Article 4 (1) of the Regulation, "personal data" means any information relating to an identified natural person or an identifiable natural person ("data subject") is an identifiable person, directly or indirectly, in particular by an identifier such as name, identification number, location data, online identifier or one or more features specific to the physical, physiological, genetic, mental, intellectual, economic, cultural or social identity of that individual. Undoubtedly, the three names in combination with one civil number represent personal data within the meaning of the Regulation. It is not disputed in the administrative file that the applicant, Ms R.D. from Sofia with PIN 57 ****** is a patient of ZZ, as she was not hospitalized in the period March 2018. It is not disputed that on 19.03.2018 in hospital ZZ EAD has admitted a patient for planned treatment, named - R.D. from the town of K., identical with the names of the applicant, but with a different unique civil number PIN 53 ********. During the registration of the patient in the "Registry" sector in the hospital information system, the three names of Mrs. R.D. from the town of K., identical with the names of Mrs. R.D. from Sofia, but with a different PIN, thus the employee from the "Registry" sector has registered Ms. R.D. from the town of K. with the unique civil number of the applicant R.D. from Sofia. It is evident from the evidence provided in the administrative proceedings that the personal data of the complainant R.D. from Sofia with PIN 57 ********. From the submitted IZ, as evidence it is evident that a correction of the unified civil number was made on 31.07.2019. A reference was provided by the National Revenue Agency (NRA) dated 19.03.2018, which shows that it is reference was made to the health insurance status of Ms. R.D. from Sofia with PIN 57 ********, and not to the actually hospitalized Mrs. R.D. from the town of K. with PIN 53 ********. A reference from the National Revenue Agency dated 31.07.2019 for the health insurance status of Ms. R.D. from the town of K. Two epicrisis DK-07-0004

were provided as evidence, from which it is clear that only the unique civil number of the person to whom the epicrisis refers has been changed, the address and content of the epicrisis have not been changed. From the slip for immunohematological examination from 20.03.2018 it is again evident that the personal data of Mrs. R.D. from Sofia PIN 57 ********, as the unique civil number was corrected with the PIN of the actually hospitalized patient. The declaration of information and consent of the patient regarding the source of payment and the diagnosis and treatment of his illness again included the data of the complainant, Mrs. R.D. with PIN 57 ******** from Sofia. From the provided cardiograms it is evident that two names are written - R.D. At the reading of a record from Holter EGG dated March 19, 2018, the three names R.D. and age 61. The documents provided in the administrative file show that the applicant was born in 1957, ie at the date of reading the Holter EEG record she was 61 years old, as recorded in the survey, and the age of the actually hospitalized patient - R.D. of K. in view of the year of birth 1953 is 65 years, ie the reading was made for the applicant Mrs. R.D. from the city of Sofia, and not for the actually hospitalized Mrs. R.D. from the town of K. Results of laboratory tests are provided, which as indicators of hematological tests are identical, but some are for RD, with PIN 57 ********, and others of RD. with PIN 53 ********. In the same way, two outpatient foxes № *** from 19.03.2018 were provided, in which the difference is in the uniform civil number and the age of the registered patient. In view of the above, the allegations of Z.Z. EAD that “it is evident from the entire medical documentation that the actual hospital treatment (hospitalization) with the necessary tests was performed on R.D. from the town of K., and not to the applicant, did not correspond to the evidence provided in the administrative file. It should be noted that the allegations of the hospital that the data from the ID card of Ms. R.D. from the town of K. in the client part of the registration part of the registration system of the National Health Insurance Fund “Registration system of the events on hospitalization and dehospitalization” (HADIS). From the attached printout from the hospital information system for hospitalization and dehospitalization it is evident that the correct unique civil number of the patient R.D. from the town of K. with PIN 53 ********. From the provided receipt for payment of user fee - bed with № **** from 20.03.2018 it is evident that the personal data of the actually hospitalized Mrs. R.D. from the town of K. In the outpatient sheets № *** and ****, both from 19.03.2018, the names and the unique civil number of the actually hospitalized patient Mrs. R.D. from the town of K., however, the date of issue is 31.07.2019, ie more than a year after the hospitalization of the patient. From the evidence provided in the administrative file, it is evident that a violation was found "regarding the confusion of patient data" and the NHIF, a protocol was drawn up for unreasonably received amounts and for Z.Z. the obligation to recover an amount unduly received has arisen. In the opinion provided to the head of the Patient

Admission Department, Z.Z. EAD stated that "it is quite possible in such a situation fraught with health problems when registering patients with three absolutely identical names and PINs starting with the same number, to make such a mistake mechanically and unintentionally", and in the opinion of KTM sector stated that due to a technical error led to the exchange of personal data of patients. On March 19, 2018, due to a power supply problem, the switch responsible for connecting patients was restarted, which led to a broken client-server connection and as a result to confusion in the personal data of two patients. From the evidence gathered in the administrative file it was indisputably established that the data of the applicant R.D. from the city of Sofia were illegally processed by the hospital as a result of a technical error, which the respondent did not dispute. In the provision of art. 32, § 4 EU Regulation 2016/679 states that the controller and the processor shall take steps against any natural person acting under the direction of the controller or processor who has access to personal data to process such data only on the instructions of the controller. administrator. Insofar as the hospital has illegally processed the data of Ms. R.D. from Sofia, apparently from Z.Z. no appropriate technical and organizational measures have been taken, which is a violation of the provision of Art. 32, § 4 of Regulation (EU) 2016/679. In view of the distribution of the burden of proof in the administrative process and the evidence gathered from the file, it must be concluded that the personal data of the applicant R.D. from Sofia are processed by ZZ EAD, in violation of Art. 32, § 4 of the Regulation. It should be noted that in the course of the administrative proceedings no evidence is involved to show that the controller has taken steps, individuals who have access to personal data and act under his direction, process the data on his instructions, not Evidence is provided of the rules for the processing of data by the hospital, as well as instructions or training for the individuals who process personal data. The Commission has the operational independence and, in accordance with the functions assigned to it, assesses which of the corrective powers under Art. 58, § 2 of Regulation 679/2016 to exercise. The assessment is based on the appropriateness and effectiveness of the decision, taking into account the specifics of each case and the degree of affecting the interests of a particular individual - data subject, as well as the public interest. The powers under Art. 58, § 2, without it under letter "i", have the character of coercive administrative measures, the purpose of which is to prevent or stop the infringement, thus achieving the due behavior in the field of personal data protection. The administrative penalty "property sanction" has a sanction nature. When applying the appropriate corrective measure under Art. 58, § 2 of the Regulation shall take into account the nature, gravity and consequences of the infringement, as well as any mitigating and aggravating circumstances. The assessment of what measures are effective, proportionate and dissuasive in each case reflects the goal pursued by the chosen corrective

measure - prevention or cessation of the violation, sanctioning of illegal behavior or both, as provided in Art. 58, § 2, letter “i”.

In the specific case the corrective measures under letters “a” - “h” and letter “j” of Art. 58, § 2 of the Regulation are applicable in view of the fact that it concerns the failure to take appropriate technical and organizational measures. The Commission also takes into account the fact that the applicant is a patient of the hospital Z.Z. EAD and her personal data appear in the hospital system. The fact was also taken into account that despite the fact that incorrect information was submitted to the NHIF, the institution has the personal data of the complainant R.D. from Sofia. With the submitted order № RD-18-162 / 01.08.2019 of the executive director of Z.Z. EAD, the Commission considers that technical measures for data protection have been taken by the hospital, but these technical measures have been taken after the violation was established by the hospital. Order № RD-18-162 / 01.08.2019 of the Executive Director of Z.Z. The SAD was issued only after the infringement of the present dispute had been established, and should have been issued at an earlier stage, as the hospital had not processed data since the time of the complaint. The order itself, which states that the Registry staff strictly comply with the requirement to enter a patient's PIN in the hospital information system, is not sufficient. the action of each employee who is on shift, as well as the workload in the hospital, which can lead to errors in the introduction into the system.The hospital should adopt administrative and technical measures. The technical measure must be such as to introduce the principle of default data protection, to adjust the system used so as not to automatically load this data in cases where data is entered manually, and to prevent automatic loading of data. personal data without being entered by an employee of the hospital registry, but to be entered entirely by the person on the basis of the information from the ID card, in order to avoid the subjective factor, which cannot be avoided with a specific order.

This technical measure is also in fulfillment of the obligations of the controller to apply the principle of personal data protection by default, which is in force since May 25, 2018. Therefore, the controller should take appropriate action and notify the Commission of the action taken in time within one month of the entry into force of the decision.

According to the above and given the nature and type of the violation found and the fact that it has been completed, the Commission considers it appropriate, proportionate and dissuasive to impose a corrective measure under Art. 58, § 2, letter “i” of the Regulation, namely the imposition of a property sanction on the administrator Z.Z. EAD for violation of Art. 32, § 4 of the Regulation, as the CPDP considers that it will have a warning and deterrent effect and will contribute to the observance by the administrator of the established legal order.

In accordance with Art. 83, § 2, letter “i”, the reasons are the following:

Letter "a" - The processing affected the rights of a data subject and did not reveal any damage to the complainant.

Letter "b" - In this case, according to the guidelines of Working Group 29, adopted on 03.10.2017, it concerns negligence on the part of Z.Z. EAD, given the fact that companies should be responsible for providing adequate structures and resources depending on the nature and complexity of their activities.

Letter "c" - the administrative body found that measures have been taken by the administrator to prevent such violations, issued an order № RD-18-162 / 01.08.2019 of the Executive Director of Z.Z. EAD for strict introduction of patients' PINs in the hospital information system by the employees of the Registry, after the violation has been established. In the meantime, at the time the violation was identified, the hospital took timely action to prevent the violation from continuing or spreading to a stage where it would have a much more serious impact.

Letter "d" - the violation refers to the adoption of appropriate technical and organizational measures, in the administrative proceedings were not involved any evidence as far as procedures, methods, "good practices" applied by the hospital in the field of personal data protection .

Letter "e" - The violation, according to the provision of Art. 32, § 4 of the Regulation is first for the administrator.

Letter "e" - removal of the violation is not possible. According to the guidance given by Working Group 29 on this criterion, it is taken into account that, as a result of the administrator's intervention, the negative effects on the applicant's rights were greater than they could have been without those interventions.

Letter "g" - the three names, PIN and address of the complainant are processed, data that identify and allow direct identification of the person.

Letter "h" - after referral to the Commission by the data subject. Interpretation by Working Group 29 for this criterion states that compliance with this obligation cannot be interpreted as a mitigating factor, and the lack of notification or non - compliance with the deadline due to inadequate assessment of the extent of the violation may lead to a more serious sanction.

Letter "i" - the controller is not sanctioned for taking appropriate technical and organizational measures in the context of current legislation on personal data protection.

Letter "j" - no approved codes of conduct have been provided at the time of the infringement.

Letter "k" - taking into account the extent of the violation, take into account the mitigating circumstance that the hospital in any

way cooperated to clarify the violation, including the correction of data in the health file of the complainant.

In assessing the circumstances of the case, the Commission finds that Z.Z. EAD, an administrative penalty "property sanction" should be imposed in a small amount. Administrators are obliged to know the law and to comply with its requirements, moreover, they owe the necessary care provided by law and arising from its subject of activity, human and economic resources. The Commission considers that the sanction imposed should amount to BGN 500 (five hundred levs), well below the average minimum provided for in the Regulation, for such a violation.

In view of the above and on the grounds of Art. 57, § 1, b. "E" of the Regulation, respectively Art. 10, para. 1, in connection with art. 38, para. 3 of the Personal Data Protection Act, the Commission ruled as follows

ANSWER:

1. Announces a complaint with registration № PPN-01-499 / 27.05.2019, filed by R.D. against health institution EAD, as well-founded, for violation of the provision of Art. 32, § 4 of Regulation (EU) 2016/679.

2. In connection with item 1 and ground of art. 58, § 2, b. "D" of Regulation (EU) 2016/679 issues an order to the administrator of the health institution EAD to take appropriate technical measures to set up the system in a way that does not allow automatic loading of personal data without being entered by a hospital receptionist, in fulfillment of the obligations of the controller to apply the principle of personal data protection by default, which is in force since May 25, 2018.

3. Deadline for implementation of the order - one month from the entry into force of the decision, after which the administrator shall notify the Commission of the implementation, presenting the relevant evidence.

4. In connection with item 1, on the grounds of art. 83, § 4, letter “a”, in connection with Art. 58, § 2, letter “i” of Regulation 679/2016, imposes on the personal data controller - health institution EAD, UIC ******, with registered office and address of management *****, property sanction and the amount of BGN 500 (five hundred leva)

The decision is subject to appeal within 14 days of its service, through the Commission for Personal Data Protection, before the Administrative Court - Sofia - city.

After the entry into force of the decision, the amount of the imposed penalty to be transferred by bank transfer:

Bank of the BNB - Central Office

IBAN: BG18BNBG96613000158601 BIC BNBGBGSD

Commission for Personal Data Protection, BULSTAT 130961721

If the sanctions are not paid after the entry into force of the decision, enforcement actions will be taken.

THE CHAIRMAN:

MEMBERS:

Ventsislav Karadzhov

Tsanko Tsolov

Maria Mateva / p /

Downloads

Decision on the appeal with registration № PPN-01-499 / 27.05.2019

print