Decision on appeal with registration № PPN-01-808 / 02.10.2018 DECISION» PPN-01-808 / 2018 Sofia, 10.09.2019 Commission for Personal Data Protection (CPDP, Commission) composed of, Chairman - Ventsislav Karadzhov and members: Tsanko Tsolov, Tsvetelin Sofroniev and Maria Mateva at a regular meeting held on 26.06.2019 and objectified in protocol № 27 / 26.06.2019, 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-01-808 / 02.10.2018, filed by N.R. against a health institution (ZZ). The administrative proceedings are by the order of art. 38 of the LPPD. The Commission for Personal Data Protection has been seised with a complaint with registration № PPN-01-808 / 02.10.2018, against Z.Z. In the complaint, Ms N.R. has indicated that on 01.10.2018 by Z.Z. have unilaterally terminated her employment. Informs that as a medical secretary - coder has an electronic signature, with her name and personal data, with which she works in the HADIS system of the National Health Insurance Fund (NHIF). He claims that after the termination of the legal relationship, Z.Z. has continued to use her electronic signature, and children have been discharged on October 2, 2018. The complaint also adds that in the period from September 3, 2018 to October 2, 2018 by Z.Z. have misused her personal data by using an electronic signature through the HADAIS system, during which time Ms N.R. has been on paid annual leave. He considers that this is a violation of the Personal Data Protection Act. Attached as evidence is a copy of the order for termination of employment and a certificate of electronic signature issued by Borika AD. Asks for an inspection by the commission. 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 the NHIF and the Health Insurance Act. opinions and relevant evidence have been requested. With a letter ex. № PPN-01-808 # 3 / 30.10.2018 ZZ, on the grounds of Art. 26 of the APC was notified of the initiated administrative proceedings, and was given the opportunity to express an opinion and relevant evidence. In response from Z.Z. an opinion was filed, with the following allegations: The opinion filed by N.R. Complaint with reg. According to Art. 30, para. 1 of the Rules of Procedure of the Commission for Personal Data Protection (CPDP) and its administration proceedings before the CPDP shall be initiated at the written request of the natural person, as in accordance with Art. 30, para. 1 of the same regulations, each request should contain data about the applicant: names, address, contact telephone number, nature of the request; other information or documents, when this is provided by law or in these regulations; date and signature. In the filed complaint with registration №

PPN-01-808 / 30.10.2018 there are no data for a specific violation of the rights of the complainant. In this sense, they consider that such an approach significantly complicates the procedural right to protection of ZZ, as the lack of a clear description of the request and specification leads to ambiguity on which issues he should focus his opinion and what should be the scope of his defense. They consider the filed complaint to be irregular, asking to be disregarded and the administrative proceedings to be terminated. Regarding the unfoundedness of the complaint, it is stated that the holder of all electronic statements made by employees of ZZ is ZZ. in connection with the fulfillment of its statutory obligations and a contract with the NHIF. According to Art. 4 of the Electronic Document and Electronic Certification Services Act, the author of the electronic statement is the natural person who is indicated in the statement as its perpetrator, and the holder is the person on whose behalf the electronic statement was made. According to the information presented on the website of the publisher - provider of electronic certification services, this type of electronic signature (marked as professional) is "issued to a natural person - author. Certifies his professional affiliation with a legal entity (company, organization, free profession). The natural person is the author and the legal entity is the holder of the signature. "Therefore, this special electronic signature represents a legal entity and electronic documents are signed on its behalf and on its behalf. In the present case, the applicant, N.R., had a professionally qualified electronic signature in order to ensure the fulfillment of her duties as an employee of the position of “medical secretary-coder” in the medical institution. The holder of each electronic statement made by this employee is Z.Z. In addition to the above, according to the policy of providing qualified certificates for qualified electronic signature, cloud qualified electronic signature and qualified electronic seal of "BORICA" JSC the identity of the holders of the signature and the connection of the holders with its public key in the certificate '. This indicates that the professional electronic signature is the property of the legal entity, which provides it to its employee in order to perform his duties. In this context, emphasis should be placed on the fact that the professional electronic signature with serial number *** and smart card number ****** is not a personal electronic signature of employees with which the person makes statements on his own behalf. As the holder of the electronic signature, Z.Z. is responsible for the electronic statements made with the respective electronic signature. According to Art. 7. of the Law on Electronic Document and Electronic Certification Services (EMSA), the holder bears the risk of error in transmitting an electronic statement. When making statements through the HADIS system, the personal data of employees holding a professional QES are processed only for the purpose of registering health insurance events (hospitalization and dehospitalization). In connection with the conclusions between Z.Z. and the National Health Insurance Fund contract for

medical care in accordance with Art. 65 of the Health Insurance Act, the executors of medical care are obliged to provide the NHIF / RHIF with information about their activities under the conditions, order and volume specified in the National Framework Agreement (NDA). According to Art. 273, para. 6 of the NDA for medical activities for 2018, the medical institution - provider of hospital medical care (BMP) collects data from the identity document of the insured person - patient, as well as information about the date and time of admission and departure of the medical institution - BMP contractor in the client part of the information system of the National Health Insurance Fund "Registration system of events for hospitalization and discharge". According to para. 8 of the same provision, the information system of the National Health Insurance Fund generates an electronic document, which is signed by an authorized person through a valid certificate for qualified electronic signature. This certificate contains the UIC of the medical institution, name, PIN and three names of the authorized person. In fulfillment of its contractual relations with the NHIF ZZ registers each event of hospitalization and dehospitalization. The employment relationship of the applicant N.R. was terminated by Order № *****, as of 01.10.2018. As can be seen from Annex № 2 - reference from the Hadis system regarding the children discharged on 02.10.2018, on behalf of N.R., in the capacity of authorized by Z.Z. person, a document has been signed certifying the dehospitalization of a patient with IH № **** due to the need to register the health insurance event that occurred for this patient. The processing of the complainant's personal data was carried out lawfully and in accordance with Regulation (EU) 2016/679, for which according to item 4.9 of the applicant's job description in accordance with the Regulations for organizing patient care in the ZZ and in particular Section VPI Registration system for health insurance events: - hospitalization and dehospitalization at ZZ in the capacity of an employee of ZZ in the position of "medical secretary - coder", knows and works with the Registration system for health insurance events : - hospitalization: and dehospitalization "and registers patients whose admission is financed by the NHIF. In addition, according to item 4.9.4 of the job description, the medical secretary - coder, has and works with a qualified electronic signature QES (professional type), certifying his professional affiliation as a registrar with the legal entity he represents. The data collected from the registration of health insurance events: in the reception-consultation offices (PKK), as well as the information about the date and time of admission and discharge from Z.Z. in the client part of the information system of the NHIF are generated in an electronic document, which is signed with QES by an employee of the position "medical secretary - coder". According to item 4.9.7 and in accordance with the regulations, the signed document is sent immediately to the server part of the information system located in the Central Office of the NHIF. According to item 5 of Order № RD-043 / 21.04.2015 of the

manager of Z.Z. in case of need for hospitalization in another medical institution of a patient admitted to a clinical path in ZZ, the registration of the discharge should be done by selecting the option "official dehospitalization", and the patient's data that were recorded during hospitalization should be enter manually as follows: on working days within their regulated working hours - by medical secretary-coder, after working hours of the PKK and on weekends - by medical secretary - coder available through access to specialized mobile internet. It follows from the above that the need and urgency of the registration of health insurance events even requires these employees to be available on weekends and after working hours of the hospital. According to the regulations for the activity, the structure and the internal order of the Consultative-Diagnostic Unit of ZZ, the medical institution has four reception-consulting rooms, which work according to a certain schedule, which is made by the head nurse and approved by the manager of Z.Z. .3 .. PKK № 1, № 2, № 3 and № 4 are serviced according to a schedule, according to the order determined by doctors and medical secretaries - coders. According to item 2 of Section VIII. Registration system for health insurance events - hospitalization and dehospitalization at Z.Z. Registration of health insurance events (admission and discharge from the Health Insurance Act) is carried out in PKK № 1 and PKK № 2. On 02.10.2018, PKK № 1 and № 2 admitted and discharged patients according to the attached schedule. After the termination of NR's employment, as of October 1, 2018, only one employee remained in the medical institution as a "medical secretary - coder", who has a professional QES to perform his duties. From the attached schedules it is evident that in the office of PKK № 2 on October 2, 2018 there were two employees on duty with working hours from 07:30 - 15:00, namely - N.R. and nurse (MS) M.F. In view of the termination of the applicant's employment, as of 1 November 2018, MF remained on duty in the office, who at that time did not have a professional QES with which to register health insurance events. The attached copy of her employment contract shows that the person started working as a "medical secretary coder" on March 13, 2018, but due to lack of experience and proven skills in registering such events, the employee was trained to for an extended period, as a result of which no electronic signature was issued to her as of that date. From the register of electronic signatures maintained by Borika AD pursuant to Art. 28, para. 1 of ZEDEUU, the certificate of the employee M.F. was issued on October 3, 2018. It is further clarified that the hospitalization performed in PKK № 1 was registered at 9:22 am - four minutes after the hospitalization of a patient in PKK № 2. The two offices are located in two adjacent buildings of the hospital (base № 1 and base №2), accepting children in different stages of physical development (early and late neurorehabilitation). In the Regulations for organizing patient care on the territory of Z.Z. It is stated that PKK-1 refers patients for treatment in the Early Rehabilitation Unit (ORNR) and PKK-2 refers

patients for treatment in the Late Rehabilitation Unit (LRR). In this case, the professional electronic signature was used to ensure compliance the established obligations of ZZ, as well as the obligations of the medical institution according to the contract concluded with the NHIF regarding the specific patient in the reception-consultation office of the hospital. The processing of the complainant's personal data is justified by the need to protect the immediate legitimate interest of the administrator Z.Z. aims to provide health services to its patients. In accordance with the guidance and clarifications provided by the UK Data Protection Authority (ICO) on the assessment of legitimate interests, the controller considers that the specific processing of the complainant's personal data is based on personal data processed on a daily basis in connection with enforcement. of the obligations assigned to her in connection with the employment and legal relationship, which in no way adversely affects her personal and personal sphere. The fulfillment of the medical institution's obligation to provide information to the NHIF has not data has suffered any damage from the specific processing. When assessing the existence of a violation of the LPPD, please take into account the specific and urgent activities of the personal data controller, who provides medical services to its patients in strict compliance with applicable regulations. Please note that the electronic signature certificate N.R. has been terminated as of October 3, 2018. The termination was made on the basis of a request for management of a certificate, filed by Z.Z. on 03.10.2018 and upon reference in the register of electronic signatures with the B-Trust mark, maintained by Borika AD, it is established that the signature has been terminated. The processing of the applicant's personal data was suspended, except for personal data, resp. the documents containing personal data, which the principal is obliged to keep in accordance with his normative obligations. In case the Commission accepts that Z.Z. has infringed the LPPD, please take into account the insignificance of the infringement and take into account all other elements related to it (according to recital 148 of Regulation (EU) 2016/679): lack of gravity of the infringement, its short duration, lack of of harmful result and negative consequences for the data subject, the measures taken for its termination, etc. In the light of all the above, they emphasize that the complainant, a personal data subject, did not securely store the professional electronic signature provided to her, leaving not only the electronic device of the QES but also the PIN code accessible to others. , mediating and allowing its use and signing electronic statements on behalf of the medical institution. According to the general conditions of Borika AD, as well as the instructions set out on the website of the certification service provider, the author is obliged to keep / keep his key throughout the validity of the certificate in a way that protects it from compromise, loss, disclosure , modification and unauthorized use. The use of the professional electronic signature by another person would be possible only if the complainant

had voluntarily provided the device and its personal PIN code, or had shown obvious negligence regarding its storage. The following are attached as evidence: Power of attorney; Excerpt from the HADIS system of the discharged children on October 2, 2018; Reference from the public register of electronic signatures with the mark B-Trust, which certifies that the electronic signature of N.R. is terminated; Request for management of a certificate from 03.10.2018; Certificate issued by BORICA AD regarding the termination of the electronic signature with serial № **** on 03.10.2018; Job description of N.R. - employee in the position of "medical secretary-coder"; Schedule of the reception and consultation offices for the month of October 2018 - 3; Reference from the public register of electronic signatures with the B-Trust mark, from which it is established that the electronic signature of M.F. was issued and valid from 03.10.2018; Order № RD-043 / 21.04.2015 of the manager of Z.Z. ; Employment contract № *** of M.F. ; Employment contract № *** of M.D. ; Staffing of positions and starting basic salaries as of 30.09.2018 of Z.Z. ; Rules for the activity, structure and internal order of the Consultative - diagnostic unit of Z.Z. ; Regulations for organizing patient care on the territory of Z.Z. The NHIF has submitted an opinion stating that detailed information on how to work with the registration system is available on the official website of the NHIF in the section "Services for contractual partners", hyperlink "registration system of events in hospitalization and hospitalization" (http : //hadis.nhif.bg), button "guides and instructions). The information about the registration system for hospitalization and dehospitalization is intended to process and store information about the identity of the health insured persons, collected by automatic retrieval of data from a machine-readable personal document upon receipt and discharge of the health insured persons from the medical institution. NHIF, respectively with RHIF. With a letter ex. № PPN-01-808 (18) # 11 / 16.04.2-19. The Commission has requested from Z.Z. additional information about the period during which Ms. N.R. has been on paid annual leave, certified by the relevant order and screen printouts of the system used by Z.Z. for hospitalization and dehospitalization of patients, for the period from 03.09.3018 to 02.10.2018, inclusive. The information was provided by letter Reg. № PPN-01-808 # 12 (18) / April 18, 2019. The complaint of N.R. is fully compliant with the requirements for regularity, according to Art. 30, 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. 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 capacity 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 24.04.2019 the complaint was accepted as procedurally admissible and as parties in the administrative proceedings were constituted: complainant N.R., respondent Z.Z. in the capacity of personal data controller and interested party - NHIF. The parties are regularly notified of the meeting of the Commission for consideration of the complaint on the merits scheduled for June 26, 2019. 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. The complaint is directed against the illegal use of NR's personal data. 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. According to the administrative file, it is not disputed that Z.Z. it was requested to issue the electronic signature of the natural person - N.R. The electronic signature was used by Z.Z. for hospitalization and dehospitalization of persons, in a period in which Ms. N.R. was on paid annual leave, as well as one day after the termination of employment between Z.Z. and the applicant. Attached to the file is order № ***, signed by the manager of ZZ, which shows that it is allowed to Mrs. N.R. leave for the period from 03.09.2018 to 30.09.2018 incl. Screen printouts from the system used by ZZ are also attached. ZZ, from which it is evident that for the period from 03.09.2018 to 02.10.2018, in the column registrar, there is only the name of Mrs. N.R. From ZZ> not specified that for some reason the leave of Ms. N.R. was interrupted. At the open meeting held on June 26, 2019 before the commission, the procedural representative of Z.Z. has stated that as of the date of filing the complaint no procedure has been introduced in ZZ for deleting professional electronic signatures when leaving the relevant persons who have such an official electronic signature, but days later this omission has been overcome and to currently there is such a procedure and on the day of termination of employment immediately the manager of Z.Z. sends an application requesting the termination of that person's qualified professional electronic signature. It is not disputed in the file that between Z.Z. and the NHIF have a contractual relationship. However, the allegations of lawful

processing of Ms. N.R.'s personal data. on the grounds of "legitimate interest" of Z.Z. should not be credited. In order to have this ground for personal data processing, namely Art. 6, para. 1, p. "E" of Regulation (EU) 679/2016, according to the guidelines given by Working Group 29, the controller should test the required balance between his legitimate interests and the interests or rights and freedoms of data subjects, and the balance test is done before data processing begins. It must also be demonstrated that the legitimate interest takes precedence over the interests and rights and freedoms of the data subject. In the present case, the legitimate interest did not take precedence over the rights and interests of the applicant, and no evidence was provided to show that Z.Z. the balance of interests test was carried out, ie this ground for processing the complainant's personal data could not be substantiated. The allegations of negligent storage by the complainant of the electronic device of QES and the PIN code are not credited. On the one hand, it should be pointed out that from the provided regulations for the activity, the structure and the internal order of the Consultative-diagnostic block of Z.Z. and regulations for organizing patient care on the territory of Z.Z. there are no written rules, which can be seen in the absence of an employee who has QES, where and in what way the QES is stored. On the other hand, no data from the Health Insurance Fund were provided, which show that a person on leave has access to the Hadis system, as well as the possibility to perform hospitalization and discharging operations during this period. On the contrary, in the opinion of Z.Z. it states that "the need and urgency of registering health insurance events even requires these staff to be available". With regard to the allegations in the written statement filed by Z.Z. with registration № PPN-01-808 # 6 / 09.11.2018, should be specified. It is not disputed that the holder of the electronic statements is Z.Z. According to the provision of art. 4 of the Electronic Document and Electronic Certification Services Act, the “author” of the electronic statement is the natural person who is indicated in the statement as its perpetrator. The "holder" of the electronic statement is the person on whose behalf the electronic statement was made. Given that the "author" of the electronic statement is the person who actually makes it, the "author" can only be a natural person. The legal entity does not have its own mental activity and cannot form a will. The "holder" of the statement is bound by the legal consequences, because the statement is made on his behalf. The legal relationship between the "author" and the "holder" may be based on different legal grounds. Unlike the "author", the "holder" can be both a natural person and a legal entity. It is he - the "holder", not the "author" who derives rights and assumes obligations under it, ie in his legal sphere the legal consequences occur. It follows from the above that an electronic signature cannot be used, be it an official one, once it has been personified, by another person who replaces the holder. In view of the above, it follows that on behalf of Z.Z. the personal data of the applicant

were processed in violation of the principle set out in the provision of Art. 5, para. 1, p. "A" of the Regulation, namely the personal data to be processed lawfully, without the presence of any of the conditions for lawful processing of personal data specified in the provision of Art. 6, § 1, letters "a" - "e" of Regulation (EU) 2016/679. With regard to the stated reasons for the merits of the complaint, a special opinion was expressed by Mr. Sofroniev, Member of the Commission. It has been argued that there is no violation of either the General Regulation or the Personal Data Protection Act. It considers that the respondent has four reasons to use this electronic signature one day after the applicant's departure. And they are in Art. 6, § 1, letters "c", "d", "e" and "e", namely that the processing is necessary to comply with a legal obligation that applies to the administrator. In this case, the child was discharged and must be discharged, regardless of whether or not the applicant had left the previous day. Next, the treatment is necessary in order to protect the vital interests of another individual - in this case a child who is discharged with the relevant diagnosis from Z.Z. Next, the processing is necessary for the performance of a task of public interest or in the exercise of official powers - in this case the latter, which are provided to the administrator, ie. Z.Z. And fourthly, the processing is necessary for the purposes of the legitimate interests of the administrator. Even more so for public authorities in carrying out their tasks. This personal electronic signature was issued to the person in the scope of his official duties and was used in the performance of these official duties in the same position, albeit by another person who replaced the departed person only a few days before, so he does not consider that for a child's hospitalization so much of the applicant's personal data was protected, which in the end were only three names. In determining the most appropriate corrective measure for the violation committed by the administrator Z.Z., the following should be taken into account: There is no data on damages suffered by Ms. N.R. H., the violation is the first for the administrator, the data from the Hadis system have been provided to another state body - the NHIF, which already has them. In view of the above and according to the provision of Art. 9, para. 3 of LPPD in the circumstances thus presented, it is more expedient to impose the corrective power, specified in Art. 58, para. 2, p. "D" of the Regulation. 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 with the following DECISION: 1. Announces a complaint with registration № PPN-01-808 / 02.10.2018, filed by N.R. against a health institution, as well-founded for violation of the provision of Art. 5, para. 1, p. "A" of Regulation (EU) 2016/679. 2. In connection with item 1 and on the grounds of art. 58, § 2, letter “d” of Regulation (EU) 2016/679 orders the healthcare institution to comply with the processing of personal data with the provisions of the Regulation by organizing the access and use of QES by each employee

in a way that does not allow the use of QES and a password from a person other than that to whom the latter belongs, within one month of the entry into force of the decision, after which the administrator shall notify the Commission of the provision of the relevant evidence. 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. CHAIRMAN: MEMBERS: Ventsislav Karadjov / n / Tsanko Tsolov / n / O.M. Tsvetelin Sofroniev / p / Maria Mateva / p / Files for download Decision on appeal with registration № PPN-01-808 / 02.10.2018 print