No. Fac.: 11.17.001.007.251 May 25, 2020 General Executive Director of OKYPY Prodromou 1 & Chilonos 17 Corner, (3rd floor) 1448, Agios Andreas, Nicosia (Under the authority of OKYPY's Data Protection Officer) DECISION OF THE DATA PROTECTION COMMISSIONER: PRIVATE ANNOUNCEMENT possible violation of the GDPR I refer to the complaint dated November 20, 2019, submitted to my Office for non-compliance with security measures in the processing of personal data of Ms. XXXXXXXXX (hereinafter the Complainant) by the State Health Services Organization (OKYpY), through the General Hospital Nicosia (hereinafter referred to as the complaint) and I inform you of the following. Facts: 2. Specifically, the Complainant's lawyer, in a letter dated 11/11/2019, states that around the end of November 2016, the Complainant received medical treatment at the Nicosia General Hospital and the Complainant did not take the appropriate measures security with the result that her medical file has been lost and additionally, the Complainant's personal data has been leaked to her employers. 2.1. In addition, she claims that, on 19/9/2019, the Complainant submitted a request for a medical certificate search to the Complainant. Subsequently, the Complainant's lawyer, on 1/11/2019, submitted a letter to the Defendant with the complaint dated 14/10/2019, where he requested the immediate granting of the medical certificate in question to his client, a request which until and the date the complaint was submitted to my Office, it had not been satisfied. 3. On 5/12/2019, an employee of my Office sent an electronic message to the Data Protection Officer (hereinafter DPO) of the Complainant, informing him of the content of the complaint, drawing his attention to the provisions of the General Regulation of Personal Data (hereafter GDPR 2016/679) asking for his positions and opinions until 17/1/2020, both with regard to the Complainant's claims for the loss of her medical file and leakage of personal data to employers of it, as well as for the procedures and security measures followed by the Complainant. He was also asked to send us/report anything relevant to this case. 3.1. On 17/1/2020, the Plaintiff requested and received an extension until 6/3/2020 to file his positions and opinions on the present case. Positions of the Plaintiff: 4. On 5/2/2020, the Plaintiff sent a letter with an attached document, the letter of the competent Doctor, in which it was stated that the Complainant was notified on 20/1/2020 to receive the Medical certificate he requested. The Complainant indicated that she would inform her lawyer. Medicine 4.1. On 11/2/2020, an Officer of my Office sent an email to the Complainant's Office of the DPA, reminding that no response was received on the matter raised by the Complainant regarding the leakage of her personal data, to her employers by of the Defendant's complaint, as well as for the procedures and security measures followed by the Defendant's complaint. Therefore, we expected an update on the case by 6/3/2020. 5. In a telephone conversation between my Office Officer, the OKYPY Officer and the Patient Rights Officer, the following was established: - when the patient leaves

the hospital, he only receives the discharge note, on which is written the date of admission and discharge from the hospital, as well as in summary the treatment provided, any medication and anything else relevant deemed by the doctor on duty, - he does not receive any other documents and/or analyses, - he can receive the X-rays as well as the results of the CT scan on a CD free of charge and MRI, - the patient has the right to request a detailed medical report for a fee of €62, after requesting it in writing. 5.1. In a related question from my Office Officer, if in 2016 the Complainant could receive the detailed medical report in question free of charge, the answer was that the detailed medical report is drawn up after the relevant request of the patient and not previously, who pays the amount of €62 to secure it. This is provided for in the Government Institutions and Services General (Amendment) Regulations of 2013. 5.2. As far as the present case is concerned, it is the claim of the DPA of the Complainant that the file of the Complainant has not been lost. 5.2.(a). The medical report was requested by the Complainant in September 2019 and later by her lawyer in a letter dated 14/10/2019. The medical report was not in the medical file to be granted as it had not previously been requested, therefore it was not lost. 5.2.(b). The reason why the Complainant was asked to pay the amount of €62 was not to draw up a new medical report, as she claims, but to draw up a medical report for the first time, since there was none, as mentioned above, in the medical file, since it had not been requested previously, i.e. in 2016 when he was discharged or later in any case before 19/9/2019. 6. With regard to the issue of the leakage of personal data, as raised by the Complainant's lawyer, that is to say, medical treatment information was leaked to the Complainant's employers without her being informed, the Complainant claims that as a competent health service provider as well as any employee thereof, did not provide any information to a third party. 7. On 12/3/2020, an Officer of my Office sent an electronic message to the lawyer of the Complainant, informing him of the allegations of the Complainant and asked for his positions and opinions until 13/4/2020. Positions of the Complainant represented by a lawyer: 8. It is an admitted fact that on and/or around the end of January 2020, the Complainant informed the Complainant to come and collect the medical report against payment of €62. 2 8.1. It is also admissible, that on 5/2/2020, an Officer of my Office contacted the office of the Complainant's lawyer, requesting to be informed whether the Complainant received the medical report. A lawyer from the Complainant's office informed the Officer of my Office that indeed the Complainant was informed to receive her medical report, but she did not do so because she was asked for the amount of €62. The Office Clerk informed me that the issue of payment of an administrative fee is not a matter that concerns our Office and she asked when and if the medical report is received to inform us. On 7/2/2020, an Officer of my Office sent a reminder email to the Complainant's lawyer. 8.2. On 12/2/2020, one of the Complainant's lawyers

responded by email with the following: "Regarding our client's medical certificate, which following a relevant oral and written request from our client as well as a letter from her lawyers to the General Nicosia Hospital was found to be lost and could not be found, I inform you that the Nicosia General Hospital has recently informed our client that a new medical report has been drawn up which costs €62 to receive from the patient concerned. As we have been informed by our client, on the one hand, the medical report in question has been received by her against the payment of the amount in question, and on the other hand, she has informed us that it is complete and there are no deficiencies as she believes." 9. In a recent electronic message dated 30/3/2020 sent by the Complainant's lawyers, the following are mentioned: 9.1. He clarifies that the Complainant's claim concerns the loss of the medical certificate, which certifies that the Complainant has undergone surgery, and not the entire medical file. This fact, as he states, violates the patient's right to information and access to information concerning him included in the medical records and, on the one hand, the right to protection of personal data. 9.2. It is his position that it is the obligation of the Complainant to observe all the appropriate technical and organizational security measures for the processing of personal data, in order to ensure the appropriate level of security against risks. 9.3. In addition, it considers that the claim for loss of the medical certificate is further strengthened: (a) due to the repeated verbal requests as well as the written request for a medical certificate search by the Complainant on 9/19/2019, the submission of which, as claims, the complaint was made at the instigation of the Defendant's officials due to the non-finding of the said medical certificate by the competent officials and (b) due to his own letter dated 10/14/2019, in which he invited the Defendant to file the complaint to issue the said medical certificate as required. 9.4. It is the claim of the Complainant's lawyer that the medical certificate it was drawn up again by the competent doctor at the urging of my Office, since there was no relevant response to the Complainant's application and his own letter. In his opinion, this clearly indicates the previous loss of the medical certificate. 9.5. It is his position that the claim of the Complainant, regarding the delay in the granting of a medical certificate due to workload, is not true and cannot be accepted, due to the fact that the medical treatment took place around the end of November 2016 3 and they had efforts were made by the Complainant and by themselves to immediately grant the medical certificate, as early as the end of September and mid-October 2019. 9.6. The compliance of the Plaintiff in the granting of the Medical certificate, occurred after excessive delay and inaction of the Plaintiff at the end of January 2020 and was carried out at the urging of my Office. 9.7. He does not accept the position of the Defendant, the complaint that the leakage of personal data on his part to the employers of the Complainant is not true and it is his strong position that information about the medical treatment, which the Complainant

underwent, was leaked to her employers, who in their conversation with the Complainant it appeared that they knew about the treatment in question without ever being informed by her. 9.8. The aforementioned knowledge of the data of the treatment by the Complainant's employers, and by extension the leakage of her personal data, was a factor causing damage to the Complainant, because her employers, due to this fact, stopped working with each other for a period of time . 9.9. Finally, they repeat and emphasize that the loss of the medical certificate and the unauthorized disclosure of personal data by the Complainant to a third party constitute a serious violation of Articles 17 and 18 of the Law on the Entitlement and Protection of Patients' Rights Law of 2004, Law 1(I)/2005 (hereinafter Law 1(I)/2005), of Article 2(1) on the Protection of Natural Persons Against the Processing of Personal Data and the Free Movement of Given these Law of 2018 (hereinafter L. 125(I)/2018) to the point that assigns the meaning of "breach of personal data" and Articles 15 and 32 par. 1 (b) and (d) and par. 4 of the GDPR. Legal Basis: 10. According to the provisions of Article 15 of Law 1(I)/2005) "(1) (a) Subject to the provisions of subsection (2), all information on the patient's medical condition, diagnosis, prognosis and treatment, as well as any other personal information are kept confidential even after his death and are not disclosed to any person or authority. (b) The competent health service provider or any employee in a medical institution shall not disclose any information concerning a patient that comes to his knowledge in the course of his duties or work. (c) The management of the medical institution or the relevant health care provider shall make appropriate arrangements to ensure that employees under its direction do not disclose such information. (2) The medical institution or the competent health service provider may disclose medical information to a third party if - (a) the patient gives written consent. The patient's consent may be assumed when the information is given to a person involved in the patient's treatment; (b) the disclosure is made for the purposes of treating the patient by another competent health care provider; (c) the information is disclosed to the medical institution that provides health care to the patient or a member of its staff for the purpose of processing, or archiving them, or for the purposes of their disclosure, which is required by law; (d) the disclosure of the information is for the purposes of publishing it in medical journals or for research or teaching purposes, provided that patient-identifiable information is not disclosed; 4 (e) there is a legal obligation to do so. (f) the Council of the Medical Body of the Pancypriot Medical Association has decided, after the doctor and the patient have been given an opportunity to express their opinion, that the concealment of this information may entail a serious risk to the health or physical integrity of other persons or have a serious impact on society as a whole: Provided that, any information is disclosed to the extent necessary in each case and every measure is taken for the purpose of safeguarding

the identity of the patient: Provided further that, any person receiving any information under this subsection shall complies with the provisions of subsection (1) of this article. (3) All information and data that may reveal the identity of the patient must be protected". 10.1. According to Article 17 of Law 1(I)/2005, the competent health service provider must keep medical records, showing the course of the patient's treatment. These records include detailed information identifying the patient and the relevant health care provider, as well as medical information regarding the patient's treatment, past medical history, diagnosis of the patient's current medical condition, and treatment options. treatment provided. 10.2. Based on Article 18 of Law 1(I)/2005, the patient has the right to information, access and objection in relation to information concerning him and which is included in the medical records. 11. In Article 15 of the GDPR it is defined that "1. The data subject has the right to receive from the controller confirmation as to whether or not the personal data concerning him is being processed and, if this is the case, the right to access the personal data and the following information: a) the purposes of the processing, b) the relevant categories of personal data, c) the recipients or categories of recipients to whom the personal data have been disclosed or are to be disclosed, in particular recipients in third countries or international organizations, d) if possible, the period for which the personal data will be stored or, when this is impossible, the criteria that determine the period in question, e) the existence of the right to submit a request to the data controller for the correction or deletion of personal data or to limit the processing of the data of a personal nature concerning the subject of d data or the right to object to said processing, f) the right to submit a complaint to a supervisory authority, g) when personal data are not collected from the data subject, any available information about their origin, h) the existence of automated decision-making , including profiling, provided for in Article 22 paragraphs 1 and 4 and, at least in these cases, important information about the logic followed, as well as the importance and foreseen consequences of said processing for the data subject. …… 3. The controller provides a copy of the personal data being processed. For additional copies that may be requested by the data subject, the controller may charge a reasonable fee for administrative costs. If the data subject submits the request by electronic means, and unless the data subject requests otherwise, the information shall be provided in a commonly used electronic format. 4. The right to receive a copy referred to in paragraph 3 does not adversely affect the rights and freedoms of others.' 11.1 In Recital 63 of the Preamble of the GDPR, it is stated among other things that this includes the right of data subjects to have access to data concerning their health, for example the data of their medical records which 5 ensuring the security of organizational measures for contain information such as diagnoses, test results, evaluations by treating physicians and any treatment or procedure provided. 12. The

provisions of article 32 of the GDPR explicitly define the following: "1. Taking into account the latest developments, the cost of implementation and the nature, scope, context and purposes of the processing, as well as the risks of different probability of occurrence and severity for the rights and freedoms of natural persons, the controller and the executor the processing implement appropriate technical and organizational measures in order to ensure an appropriate level of security against risks, including, among others, as appropriate: a) the pseudonymization and encryption of personal data, b) the ability to ensure the confidentiality, integrity, availability and reliability of processing systems and services on an ongoing basis, c) the ability to restore the availability and access to personal data character in due time in the event of a physical or technical event, d) procedure for the regular testing, assessment and evaluation of the effectiveness of the techniques and processing……. 4. The controller and the processor shall take measures to ensure that any natural person acting under the supervision of the controller or the processor who has access to personal data processes it only on the instructions of the controller, unless required to do so by Union or Member State law'. 12.1. In addition, Recitals 74 and 83 of the Preamble of the GDPR state, among other things, that the controller should be required to implement appropriate and effective measures and be able to demonstrate the compliance of the processing activities with the GDPR, including the effectiveness of meters. 13. In the Official Gazette of the Republic of Cyprus, Appendix Three, Part I, Regulatory Administrative Acts, in relation to the K.D.P. 143/2013, Number 4666, Dated April 30, 2013, referred to on page 1042 in PART XVIII, entitled MISCELLANEOUS, at point. 4e) that the detailed medical report costs €62. Reasoning: 14. For the purposes of this decision, a reference to a medical certificate and a detailed medical report and/or medical report shall be understood to mean the same. 15. In this case, it is examined whether the Complainant (a) lost the Complainant's detailed medical report and (b) leaked the Complainant's personal data to her employers. 15.1. On the one hand, there is the claim by the Complainant that the medical report concerning her hospitalization in November 2016 was lost, hence the payment of the amount of €62 to have the said medical report prepared again and on the other hand the Defendant filed the complaint claims that the said medical report was not lost. In order for it to be drawn up and/or drawn up, a written request had to be submitted and if it was drawn up, the amount of €62 had to be paid for its receipt. Any delay in granting it was due to the workload of the Complainant, exclusively. 15.2. The Defendant of the complaint must prove that he took security and personal data protection measures to ensure that the Complainant's personal data is not leaked to her employers on his part, as alleged. 6 16. On the official website of the Ministry of Health, https://www.moh.gov.cy, under the title Medical Care since 1/8/2013, there are posted the General (Amendment)

Regulations of 2013, as published in the Official Gazette of the Government, dated April 30, 2013, Part I, Number 4666 there is a table with the charges of the various services provided. 16.1. In Part XVIII of the said table, under the heading Miscellaneous, 4. Health and Sickness Certificates, e) Detailed Medical Report, cost €62. 17. As mentioned above, the standing policy/procedure followed by the Complainant is to draw up a medical report when a written request is submitted and upon delivery the amount of €62 is paid. Therefore, the Defendant was under no obligation to prepare a medical report, either from November 2016 when the Complainant was discharged, or before September 19, 2019, the date on which the Complainant submitted the written request. 17.1. It was clarified by the Complainant's lawyer that the medical report and not the medical file was lost. From the facts, it does not appear that the medical report in question has been lost, since the Complaining Defendant had no obligation to prepare it prior to the submission of a written request by the Complainant, which was submitted in writing for the first time in September 2019. 17.2. What is apparent, from the evidence before me, is the delay in the preparation/drafting and issuing of the medical report. The Complainant submitted a written request for the medical report in September 2019 and the Defendant informed her to receive it in January 2020, i.e. approximately 4 months after the initial written request. 18. It should be noted that my Office carries out ex officio audits and monitors developments in various organizations and services, public and private. 18.1 Bearing in mind the above, I note that a visit was made by me, at an earlier stage and time, to the premises of the Complainant, in order to be informed about the progress of the computerized system and about the security and protection measures of the medical files of patients. 18.2. During my visit, I was informed, among other things, that: - the Nicosia General Hospital partially keeps an electronic patient file in which the tests performed by the patient are electronically registered, but not even the doctor's reports for each patient, - access to the electronic file of the patient is done only by the attending physician and always with a code, - no one can secure access to the patient's electronic file without a code, unless the patient is present and consents to this action, - the personal files of the patients are kept in various areas even in the basement, without providing access to a person who does not work in the archive, since the entrance to the central archive is controlled electronically while the entrance to the basement is supervised by a responsible person who is at the entrance and in the event of his absence, the entrance remains closed and locked, - the communication between the basement and ground floor is by telephone anyway ensure that the area is not abandoned or left unattended under any circumstances, 7 processing (Ministries/Departments/Services), - when files are found upon request from the basement area, a specific employee is notified, who is charged with the responsibility of transporting the file from the basement

to the ground floor and in any case to a specific recipient, - the question of installing a biometric data collection system was raised, for the purpose of checking the attendance of employees, in place of the electronic card and a meeting with the guilds is expected to discuss it, - procedures were activated regarding the handling of medical files and the operation of a file handling recording system began, - the electronic storage of x-rays began, - the recording of lost files in the computerized system was planned, - measures and levels of accessibility to the medical file were defined, - no one can have remote access access to the system (from computers outside the hospital) and - signs were placed stating that patients themselves are not allowed to hold files. 18.3. For this purpose, I also issued a relevant Directive dated 11/10/2017, with number 4/2017, which is posted on the website of my Office, with instructions to the managers of the Public Sector and Organizations of the wider Public Sector for the exercise of right of access by employees or job candidates and which is still in force today. 18.4. By analogy, what is mentioned in Directive 4/2017 also applies to every citizen who exercises the right of access to the public sector, both public and private. 18.5. In this particular case, according to the data before me, the Complainant did not exercise a right of access in accordance with the provisions of GDPR 2016/679. What the Complainant did was to submit a request, initially orally and later in writing, for the preparation of a detailed medical report, the granting of which is provided for by special procedures resulting from Law 1(I)/2005 as well as the On Government Medicines Institutions and Services General (Amendment) Regulations of 2013. Therefore, the Complainant's request does not fall within the provisions of Article 15 of GDPR 2016/679. 18.6. In a written letter from the IT Services Department of the Ministry of Health, dated July 22, 2019, I have been informed that the project of digitizing the patients' physical medical records following a decision of the Electronic Governance Council dated 29/6/2018, will include the digitization of all State Hospitals and Health Centers throughout Cyprus and not just the digitization of the Nicosia General Hospital as was the initial approach. Conclusion/Ending: 19. According to the facts before me and during the investigation of the complaint, it does not appear that any medical report has been lost, since the medical report referred tothe Complainant is drawn up only upon written request and after being drawn up, the amount of €62 is paid as consideration, as provided for in the On Government Medicines Institutions and Services General (Amendment) Regulations of 2013. The Complainant, not had made before September 19, 2019, at least in writing, an application for preparation/drafting of a detailed medical report. Therefore, the claim that there was in medical file and it was lost, it does not seem to be correct.

19.1. As I mentioned above, there was a delay in training/writing and awarding

of the medical report, almost 4 months after the initial written request. The lack of training

and tradition of the medical exhibition is something that should concern Kat'ou her

complaint, since the Complainant's request related to the preparation of the medical report

pursuant to Law 1(I)/2005 and not in the exercise of the right of access pursuant to Article

15 of the GDPR.

19.2. The Complainant's allegation of leakage of her personal data by

As for the complaint against her employer, it is considered unfounded, since it has not been proven

according to the facts before me.

19.2.(a) I have not been presented with any evidence that proves/supports,

even the slightest allegation that there was any leakage or that the alleged

leakage of personal data was a factor causing damage to the Complainant

and because of this incident, their cooperation was interrupted for a time

space. Furthermore, the issue of any damage is not considered by my Office.

19.3. In any case, it seems that the Defendant, after the complaint, took measures and proceeded to

procedures for the protection of personal data, prepared a plan for

information and monitoring. In addition, the measures to comply with processing security

of personal data, appear to be such as to constitute a potential breach,

remote event, without this implying that these measures should not occur

control and revision, when and where this is deemed necessary.

20. Having regard to the facts, the analysis as explained above, I do not have

found a violation under the provisions of GDPR 2016/679 by the Defendant on

complaint and therefore I will not proceed with any further action.

Irini Loizidou Nikolaidou

Data Protection Commissioner