REPUBLIC OF CYPRUS E P I T R O P O S No. Fax: 11.17.001.009.242 OFFICE OF THE COMMISSIONER FOR THE PROTECTION OF PERSONAL DATA DECISION Complaint for breach of personal data Mr. XXX at XXX General Hospital Facts I refer to the complaint submitted to my Office regarding the above matter and according to the information before me I find a violation by the complainant of the provisions of Regulation (EU) 2016/679 on the protection of natural persons against the processing of personal data and on the free movement of such data (hereinafter the "Regulation"). A. 2.1. A complaint was submitted to my Office on November 1, 2021, by Ms. XXX against the State Health Services Organization (hereinafter "OKypY"). However, in the context of the investigation of the complaint, it became clear that, with her actions, Ms. XXX made herself a separate data controller, a status which entails obligations in accordance with the provisions of the Regulation. Therefore, I issue this Decision against Ms. XXX (hereinafter "Mrs."). 2.2. The complaint states, among other things, the following: (a) The Defendant is XXX in the Medical Services of G.N. XXX. (b) The Lady claims that, while she was absent on sick leave, she was informed that Mr. XXX, who is XXX OKYPY in the same Department of the General Hospital. XXX, emptied Kathy's desk drawers, and then placed her documents and personal effects in cardboard boxes, without informing her first. (c) In addition, the Defendant states that Ms. XXX, who is XXX OKYPY in G.N. XXX, gave instructions to an Information Technology Officer, how to replace her computer tower with a computer tower belonging to another OKYpY employee. (d) Further, in her drawers, Kathy had the personal medical files of herself, her husband and her children. (e) Mr. XXX informed Ms. XXX, who in turn notified the Administrative Officer, Mr. XXX, and then the File Manager, Mr. XXX, and then the Secretarial Officer, Ms. XXX. The files in question were returned to the Archive, without any information and in the absence of the Court. Iasonos 1, 2nd floor, 1082 NICOSIA / PO Box 23378, 1682 NICOSIA. Tel: 22818456, Fax: 22304565 E-mail: commissioner@dataprotection.gov.cy, Website: http://www.dataprotection.gov.cy (f) The Professor claims that the personal medical files have always been kept in staff drawers within the hospital, for easy access as well as precaution, because the file archive does not have the appropriate conditions and conditions for their safe keeping. (g) In order to strengthen her position, she presented to my Office a relevant circular dated October 25, 2021 with no. lens 05.25.063, which the Patient Registry Manager communicated to the staff of G.N. XXX, after the incident, so as to "… justify their action, … thus showing that they knew that the staff held personal files and also that it was not prohibited." 2.3. On November 05, 2021, based on my duty to examine complaints, pursuant to Article 57(1)(f) of the Regulation, an electronic message was sent on my behalf to the Data Protection Officer (hereinafter the "DPO") of OKYpY, with which was informed of the complaint in question and was called

upon to, until November 25, 2021, inform me regarding the positions on the Defendant's allegations. More specifically, the OKYPY was requested, by the above date, to: (a) submit its positions, in relation to the incident in question, (b) inform my Office about the reasons why the personal belongings and the contents of the drawers of Ms.'s office were moved in her absence and without notification, (c) inform my Office of the reasons why the staff of G.N. XXX had in his possession the physical medical files of himself and their relatives and (d) informed my Office of the procedure followed, regarding the movement and/or clearing of the contents of the drawers of the staff offices. 2.4. On the same day, i.e. November 5, 2021, my Office sent an electronic message to the Client, informing her of the letter to OKYPY, as well as pointing out the fact that she had personal data in her possession, namely special categories, which automatically makes it responsible for data processing. Furthermore, the storage of original physical medical files and not copies constitutes a violation of the provisions of the Regulation. Therefore, the Lady was called upon to inform my Office by November 26, 2021, regarding: (a) the reasons why she had in her possession the physical medical files in question, (b) the reasons why the said medical records were kept in her workplace, (c) whether the drawers in which the said medical records were located were locked, and (d) whether third parties had access to her office. 2.5. On November 15, 2021, she sent another email, informing my Office that Mr. XXX, a nursing officer, who was appointed responsible for personal data at G.N. XXX, called Kathy to give a statement about the events. Furthermore, the Professor expressed her concern that, possibly, the investigation of G.N. XXX not to be impartial, as Mr. XXX was appointed by OKYpY. 2 2.6. In response to Ms email, on the same day my Office replied via email that, on the one hand, an organization's internal process does not affect my own independent investigation, on the other hand, its findings will be taken into account once they are confirmed. 2.7. On November 22, 2022, Ms. responded to the questions raised by my Office with an email dated November 15, 2021 in which, among other things, she states that: (a) Ms. is XXX in the Medical Services of G. N .XXX but until XXX he worked on secondment for a period of XXX years at OKYpY. He is housed in the same office where he has been for the last XXX years, that is in XXX of the Hospital. Since XXX she has been under the Medical Services, as her secondment has been terminated, but she continues to be housed in the same office until she is moved to another location, which will be indicated later. (b) Mr. XXX, XXX of OKYpY, with whom the Ms. is housed in the same office, had declared the previous day, in front of the other colleagues in the office, his intention to vacate the Ms.'s office. Kathy claims that, the next day, she signed the attendance register at 6:40 and by 7:30, when the rest of the employees arrive, she vacated her office. Mr. XXX admitted his act in question to the Defendant over the phone. (c) Further, according to the Plaintiff, Mr.

XXX, Information Technology Officer stated that he was instructed by Ms. XXX, XXX, how to replace the Plaintiff's computer. (d) The Defendant admits that she had her family's medical files in her drawer and "as stated they are confidential and it is forbidden to move them outside the hospital". (e) In front of the rest of the staff, Mr. XXX alerted Ms. XXX by showing her the files he found in her drawer. (f) It is the position of the Accused that, the situation that prevails in the files of G.N. XXX is not good. More specifically, the kardex system has been full for years and now several folders are some on the floor, some in cardboard boxes, or many of those stored on shelves, have data that has either fallen on the floor or is exposed. In addition, it is common for patient files to be lost and a new one created. "Due to space and the need to protect the files and sometimes recommendations from the attending physicians, the staff were in possession of their personal file inside the hospital." (g) [ ]. (the) [ ]. (i) She adds that, in her office, the drawers cannot be locked. Furthermore, only those who work in that office (another 5 people in total) have access to her office. (j) The Professor notes that she returned to her office, following the intervention of the Associate Director of Medical Services, Ms. XXX, and her computer has also been reconnected. The Director of the Hospital, Mr. XXX, called the people involved to his office and informed them that Mr. XXX does not admit that he moved the Ms.'s personal belongings, in her absence and despite the orders of the Directorate of G.N. XXX. 2.8. On November 24, 2021, my Office received via e-mail a reply letter, from the DPA of OKYPY, in which, among other things, the following are mentioned: 3 2.8.1. The Directorate of G.N. XXX, through XXX, Mrs. XXX, had given an order for the transfer of the Ms. and her return to her duties at the Ministry of Health, after her sick leave. Kathy was aware of this particular move when she would return from her sick leave. 2.8.2. Despite the instructions to carry out the transfer in question, after Ms return, another employee of OKYPY, on his own initiative, vacated the office of the Defendant, during her absence and while she was on sick leave. Kathy was informed about the incident by other colleagues. 2.8.3. During the process of moving Kathy's personal belongings from her drawers, to which there was free access, it became apparent that she had in her possession original medical records of herself and her family members. The medical files in question were subsequently returned to the OKYpY file, where the relevant re-filing took place. 2.8.4. The DPO of the OKYpY adds that, even if there was a need for immediate movement of the Defendant's belongings and she could not be present, "the movement was poorly executed without first notifying the Defendant of this intention and be given the possibility to authorize another person to be present during the movement process'. 2.8.5. The Ministry of Foreign Affairs, in summary, admits that: (a) The staff of OKYpY are not sufficiently informed and aware of matters concerning personal data. (b) OKYPY recognizes that the absence of written procedures for

moving objects and/or electronic personnel data and clearing the contents of drawers entails risks. Generally, the practice followed is for the liquidation to take place in the presence of the subject or his authorized representative. However, this practice was not followed in this particular case. (c) The possession of original medical files by the staff is a violation of the Law on the Establishment of the State Health Services Organization (Law 73(I)/2017) and the Law on the Entitlement and Protection of Patients' Rights (Law 1(I) /2005), which provide that the competent health service provider (G.N. XXX) must keep medical records, which show the course of the patient's treatment. (d) It is the position of OKYpY that the withholding of the medical file by the patient himself "in addition to being illegal, creates a multitude of problems for the management of the Organization, but also in the management of incidents that may arise and concern the subject". Anyone wishing to obtain a copy of their medical record may do so through the appropriate process and upon request. (e) The Ministry of Internal Affairs emphasizes that the possession of said physical medical files by the Claimant is unjustified and violates the instructions of the OKYPY to the staff. (f) The Directorate of G.N. XXX, recognizing the problem, repeatedly called the staff, with internal circulars, to return to the Archives, medical files that he may have in his possession. (h) The inability to identify the absence of the medical files from the Archive reveals the Organization's inability to handle similar incidents, a fact which is recognized by the Directorate. (i) The absence of a medical file management process reveals the inability to properly process the medical files within (but also outside) the Organization, which 4 Legal framework, however, does not reduce the consequences of the illegal possession of the medical files by the Defendant. (j) As regards the movement of the Accused's belongings, the Ministry of Foreign Affairs states that it was done in the context of her own movement to her duties at the Ministry of Health. However, they were moved without reason and in her absence and without prior notification. 2.8.6. After the incident, the Ministry of Foreign Affairs, in collaboration with the management of OKYpY, plan, among other things, to take the following actions: (a) Training of all staff in matters related to the Regulation and the proper management of personal data. (b) Preparation of a procedure for managing and handling the Medical file inside and outside the hospitals, so as to prevent the recurrence of similar incidents, whether it concerns an employee or a patient visiting the health units / services of the OKYpY. (c) Preparation by OKYpY and adoption of personnel movement / transfer procedures, where clear reference will be made to the method of movement / departure of personnel, personal data and work equipment (computers, electronic devices, etc.). B. 3.1. Article 4(1) of the Regulation defines that "personal data" is "any information concerning an identified or identifiable natural person (data subject)". 3.2. In Article 4(2) of the Regulation, processing is defined as "any act or series of acts carried out with or

without the use of automated means, on personal data or sets of personal data, such as the collection, registration, organization, structure, storage, adaptation or alteration, retrieval, retrieval of information, use, disclosure by transmission, dissemination or any other form of disposal, association or combination, limitation, deletion or destruction”. 3.3. Furthermore, in Article 4(7) of the Regulation, a data controller is defined as anyone (the natural or legal person, public authority, agency or other entity) who, "alone or jointly with another, determine the purposes and manner of processing of personal data". 3.4. In Article 4(12) of the Regulation a personal data breach is defined as "a breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access of personal data transmitted, stored or otherwise submitted in processing". 3.5. The Principles governing the processing of personal data are defined in Article 5(1) of the Regulation. In subsection (a) of this Article it is provided that personal data must be "subject to legal and legitimate processing in a transparent manner in relation to the data subject ("legality, 5 objectivity and transparency")". Also, in subsection (b) of the same Article it is stated that personal data must be "collected for specified, explicit and lawful purposes and not further processed in a manner incompatible with these purposes ("purpose limitation")". Furthermore, in subsection (f) of this Article it is provided that, personal data must be "processed in a way that guarantees the appropriate security of personal data, including their protection from unauthorized or illegal processing and accidental loss, destruction or deterioration, using appropriate technical or organizational measures ("integrity and confidentiality")." 3.6. Article 6(1) of the Regulation, regarding the legality of the processing, provides that the processing is lawful, "only if and as long as at least one of the following conditions applies: a) the data subject has consented to the processing of personal data of its nature for one or more specific purposes, b) the processing is necessary for the performance of a contract to which the data subject is a party or to take measures at the request of the data subject prior to the conclusion of a contract, c) the processing is necessary for compliance with a legal obligation of the controller, d) the processing is necessary to safeguard a vital interest of the data subject or another natural person, e) the processing is necessary for the fulfillment of a task performed in the public interest or against the exercise of public authority assigned to the controller, f) the processing is a waived for the purposes of the legitimate interests pursued by the controller or a third party, unless these interests are overridden by the interest or the fundamental rights and freedoms of the data subject that require the protection of personal data, in particular if the data subject he is a child. Item f) of the first paragraph does not apply to the processing carried out by public authorities in the exercise of their duties." 3.7. In addition, Article 9 of the Regulation, which concerns the processing of special categories of personal data, states that:

"1. The processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or participation is prohibited in a trade union organization, as well as the processing of genetic data, biometric data for the purpose of indisputable identification of a person, data concerning health or data concerning a natural person's sexual life or sexual orientation. 2. Paragraph 1 shall not apply in the following cases: a) the data subject has provided express consent to the processing of such personal data for one or more specific purposes, unless Union or Member State law provides that the prohibition referred to in paragraph 1 cannot be removed by the data subject, 6b) the processing is necessary for the performance of the obligations and the exercise of specific rights of the controller or the data subject in the field of labor law and social security and social protection law, if permitted by Union or Member State law or by collective agreement in accordance with national law providing appropriate guarantees for the fundamental rights and interests of the data subject, c) the processing is necessary to protect the vital interests of the data subject or another natural person, if the data subject is physically or legally unable to consent, d) the processing is carried out, with appropriate guarantees, in the context of the legal activities of an institution, organization or other non-profit body with a political, philosophical, religious or trade union objective and on the condition that the processing concerns exclusively the members or former members of the body or persons who have regular communication with him in relation to his purposes and that the personal data are not shared outside the specific body without the consent of the data subjects, e) the processing concerns personal data that has been manifestly made public by the data subject, f) processing is necessary for the foundation, exercise or support of legal claims or when the courts act in their jurisdiction, g) the processing is necessary for reasons of substantial public interest, based on the law of the Union or a Member State, which is proportionate to the intended objective, respects the essence of the right in data protection and provides appropriate and specific measures to ensure the fundamental rights and interests of the data subject, h) the processing is necessary for the purposes of preventive or occupational medicine, assessment of the employee's ability to work, medical diagnosis, provision of health or social care or treatment or management of health and social systems and services based on Union law or the law of a Member State or pursuant to a contract with a health professional and subject to the conditions and guarantees referred to in paragraph 3, i) the processing she is necessary for reasons of public interest in the field of public health, such as protection against serious cross-border threats to health or ensuring high standards of quality and safety of healthcare and medicines or medical devices, based on Union or Member State law; which provides for appropriate and specific measures to protect the rights and freedoms of the data subject, in particular professional

confidentiality, or j) the processing is necessary for archiving purposes in the public interest, for the purposes of scientific or historical research or for statistical purposes in accordance with Article 89(1) on the basis of Union or Member State law, which are proportionate to the objective pursued, respect the essence of the right to data protection and provide for appropriate and specific measures to safeguard his fundamental rights and interests subject of data. 3. The personal data referred to in paragraph 1 may be processed for the purposes provided for in paragraph 2, point h), when such data is processed by or under the responsibility of a professional who is subject to the obligation to maintain professional secrecy based on of Union or Member State law or based on rules established by competent national 7 bodies or by another person who is also subject to an obligation of confidentiality under Union or Member State law or based on rules established by competent national bodies. 4. Member States may maintain or introduce further conditions, including restrictions, regarding the processing of genetic data, biometric data or health-related data.' 3.8. Based on Article 58(2) of the Regulation, the Commissioner has all the following corrective powers: "a) to issue warnings to the controller or processor that intended processing operations are likely to violate the provisions of this regulation, b) to direct reprimands to the controller or processor when processing operations have violated provisions of this regulation, c) instruct the controller or processor to comply with the requests of the data subject for the exercise of his rights in accordance with this regulation, d) to instruct the data controller or the processor to make the processing operations comply with the provisions of this regulation, if necessary, in a specific way and within a certain period, e) to instruct the data controller to announces the personal data breach of an optical nature to the data subject, f) to impose a temporary or definitive restriction, including the prohibition of processing, g) to order the correction or deletion of personal data or the restriction of processing pursuant to articles 16, 17 and 18 and an order to notify the actions of those to recipients to whom the personal data was disclosed pursuant to Article 17(2) and Article 19, h) to withdraw the certification or to order the certification body to withdraw a certificate issued in accordance with Articles 42 and 43 or to order the organization of certification not to issue certification, if the certification requirements are not met or no longer met, i) to impose an administrative fine pursuant to article 83, in addition to or instead of the measures referred to in this paragraph, depending on the circumstances of each individual case, j) to instructs to suspend data traffic to a recipient in a third party country or to an international organization." 3.9. Furthermore, Article 83 of the Regulation, which concerns the general conditions for imposing administrative fines, provides that: "1. Each supervisory authority shall ensure that the imposition of administrative fines in accordance with this article against violations of this regulation referred to in paragraphs 4, 5 and 6 is effective, proportionate

and dissuasive in each individual case. 2. Administrative fines, depending on the circumstances of each individual case, are imposed in addition to or instead of the measures referred to in Article 58 paragraph 2 points a) to h) and Article 58 paragraph 2 point j). When making a decision 8 on the imposition of an administrative fine, as well as on the amount of the administrative fine for each individual case, the following shall be duly taken into account: a) the nature, gravity and duration of the infringement, taking into account the nature, the extent or purpose of the relevant processing, as well as the number of data subjects affected by the breach and the degree of damage they suffered, b) the fraud or negligence that caused the breach, c) any actions taken by the controller or the processor to mitigate the damage suffered by the data subjects, d) the degree of responsibility of the controller or the processor, taking into account the technical and organizational measures they apply pursuant to articles 25 and 32, e) any relevant previous violations of the controller or processor, f) the degree of cooperation with the control authority to remedy the violation infringement and the limitation of its possible adverse effects, g) the categories of personal data affected by the breach, h) the way in which the supervisory authority was informed of the breach, in particular if and to what extent the data controller or processor notified the violation, i) in the event that the measures referred to in Article 58 paragraph 2 were previously ordered to be taken against the controller involved or the processor in relation to the same object, the compliance with said measures, j) the observance of approved codes of conduct in accordance with article 40 or approved certification mechanisms in accordance with article 42 and k) any other aggravating or mitigating factor resulting from the circumstances of the specific case, such as the financial benefits obtained or losses avoided, directly or indirectly, from the violation. 3. In the event that the controller or processor, for the same or related processing operations, violates several provisions of this regulation, the total amount of the administrative fine does not exceed the amount set for the most serious violation. 4. Violations of the following provisions shall attract, in accordance with paragraph 2, administrative fines of up to EUR 10 000 000 or, in the case of undertakings, up to 2 % of the total worldwide annual turnover of the previous financial year, whichever is higher: a) the obligations of the controller and processor in accordance with Articles 8, 11, 25 to 39 and 42 and 43, b) the obligations of the certification body in accordance with Articles 42 and 43, c) the obligations of the monitoring body in accordance with article 41 paragraph 4. 5. Violations of the following provisions attract, in accordance with paragraph 2, administrative fines of up to EUR 20 000 000 or, in the case of businesses, up to 4 % oftotal worldwide annual turnover of the previous financial year,

whichever is higher:

a) the basic principles for the processing, including the terms that apply to

the approval, in accordance with articles 5, 6, 7 and 9,

b) the rights of data subjects in accordance with Articles 12 to 22;

9

c) the transmission of personal data to a recipient in a third country or internationally

organization in accordance with Articles 44 to 49,

d) any obligations under the law of the Member State which

enacted under Chapter IX,

e) non-compliance with an order or with a temporary or permanent restriction thereof

processing or to suspend the circulation of data imposed by the supervisory authority

authority under section 58(2) or failure to provide access in breach thereof

Article 58 paragraph 1.

6. Failure to comply with an order of the supervisory authority as referred to in article 58

paragraph 2 attracts, according to paragraph 2 of this article, administratively

fines of up to EUR 20 000 000 or, in the case of undertakings, up to 4 % of the total

of global annual turnover of the previous financial year, depending on

whichever is higher.

7. Subject to the remedial powers of the supervisory authorities under

Article 58(2), each Member State may determine the rules on whether

and to what extent administrative fines may be imposed on public authorities and

bodies established in that Member State.

8. The exercise by a supervisory authority of its powers pursuant to this article

subject to due process guarantees in accordance with Union law and the

law of the Member State, including the exercise of actual jurisdiction

appeal and due process.

9. When the legal system of the member state does not provide for administrative enforcement

fines, this article may be applied in such a way that the procedure

enforcement to be initiated by the competent supervisory authority and to be enforced by the competent authorities

national courts, while ensuring that those remedies are

effective and have an equivalent effect to the administrative fines which

imposed by the supervisory authorities. In any case, the fines imposed

they are effective, proportionate and dissuasive. The Member States in question shall notify the

Commission the provisions of their laws which they adopt in accordance with this

paragraph, until 25 May 2018 and, without delay, every time thereafter

amending law or their amendment."

C.

4.1.1. In the present case, the Defendant claims that, while she was absent on leave

illness, he was informed that another employee of OKYpY emptied his drawers

office and then placed her documents and personal belongings

in paper boxes, without informing her first. In the drawers, among other things,

the original medical files of herself, her husband and the children were also located

her. The files in question were returned to the Archive of G.N. XXX, without any

information even in the absence of Ms.

4.1.2. The above allegations of Ms. have been verified by his relevant letter

OKYpY dated November 24, 2021. More specifically, the letter in question states

that, the Directorate of G.N. XXX, had given an order for Kathy's movement and return

in her duties at the Ministry of Health, after her sick leave. It was Kathy

Thinking

aware of this particular move, as soon as she would return from sick leave

her. However, another employee of OKYpY, on his own initiative, overlooked

the instructions of the Directorate, vacated the office of the Professor, during her absence.

Therefore, on the part of the OKYpY, there was an admission that the objects of the Defendant

they moved in her absence, unjustifiably and without prior notice

be informed that the movement of her personal belongings will take place according to

substantial time.

4.2.1. I consider it appropriate to remind that, personal medical files and in general

data relating to health fall under the special categories of data

of a personal nature that are processed, in accordance with Article 9 thereof

Regulation.

4.2.2. The fact that she had personal data in her possession,

and especially of special categories, makes it a separate data controller, with

all the obligations arising from the Regulation.

4.2.3. Even if the claim is accepted that the Defendant retained the

due to original medical files in order to [ ], however I consider that, o

her purpose could be achieved, having in her possession, a copy of

said medical records, and not the original version.

4.2.4. Furthermore, Kathy was in possession of the original medical records

of herself, her husband and her children in violation of the Organization Establishment

of State Health Services Law (L. 73(I)/2017) and the On Entitlement and

Protection of the Rights of Patients Law (Law 1(I)/2005), an act which, in addition to

of that, made her a separate controller with all the implications

obligations pursuant to the Regulation, violates Article 6(1) of the Regulation, as well

the act in question does not meet any of the conditions to be legal

processing.

4.3. As regards the complaint against OKYpY, regarding the movement of

personal belongings of the accused in her absence, the case was investigated

separately and on the basis of the data placed before me, I decided exercising

my remedial powers to give an Order to OKYpY, as within one and a half (1.5)

month:

(a) prepare written procedures regarding personnel transfer and movement

of his personal items and if deemed necessary, update and/or

strengthen existing written procedures, and

(b) take strict action to enforce the written procedures, on behalf of

of the employees of OKYpY.

D. Conclusion – Conclusion

5.1. Bearing in mind the above and based on the powers granted to me by

Articles 58 and 83 of Regulation (EU) 2016/679 and article 24(b) of the Law

125(I)/2018, my conclusion is that there is a violation, on the part of the Defendant, of

Article 6(1) of the Regulation, since the retention of the original medical files

of herself, her wife and children had no valid legal basis.

11

5.2. Having considered and considered –

(a) The applicable legislative basis regarding the prescribed administrative sanctions in

provisions of Article 58(2) and Article 83 of the Regulation.

(b) All the circumstances and factors put forward by the Plaintiff and OKYpY

me based on all existing correspondence,

I consider that, under the circumstances, the imposition of an administrative fine is not justified.

5.3. Nevertheless, bearing in mind the above facts, the legal aspect on which

based on this Decision and the analysis as explained above,

exercising the powers granted to me by Article 58(2)(b) of the Regulation,

I decided

at my discretion and in compliance with the above provisions, to address to Ms

Reprimand for the violation of Article 6 of the Regulation.

Irini Loizidou Nikolaidou

Data Protection Commissioner

Personal Character

Nicosia, 4 May 2022

12