

REPUBLIC OF CYPRUS ΕΠΙΤΡΟΠΟΣ Νο. 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 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"), by the State Health Services Organization ( henceforth "OKYPY").

A. 2.1. A complaint was submitted to my Office on November 1, 2021, by Ms. XXX (hereinafter the "complainant") against OKYPY. 2.2. The complaint in question mentions, among other things, the following: (a) The complainant is XXX at the Medical Services of G.N. XXX. (b) The complainant 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 G.N. XXX, emptied the drawers of the complainant's desk, and then placed her documents and personal belongings in cardboard boxes, without informing her first. (c) In addition, the complainant 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, the complainant had the personal medical records 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 complainant. f) The complainant maintains that the personal medical files have always been kept in the staff drawers inside the hospital, for easy access as well as for protection, because the appropriate conditions and conditions for their safe storage do not prevail in the file archive. Iasonos 1, 2nd floor, 1082 NICOSIA / PO Box 23378, 1682 NICOSIA. Tel: 22818456, Fax: 22304565 E-mail: [commissioner@dataprotection.gov.cy](mailto:commissioner@dataprotection.gov.cy), Website: <http://www.dataprotection.gov.cy> (g) To strengthen her position, the complainant 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 inform me, until November 25, 2021, regarding the positions on the allegations of the complainant. 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 the complainant'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) inform my Office of the procedure followed, regarding the movement and/or clearing of the contents of the staff desk drawers.

2.4. 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:

2.4.1. The Directorate of G.N. XXX, through XXX, Mrs. XXX, had instructed the complainant to move and return to her duties at the Ministry of Health, after her sick leave. The complainant was aware of this particular move when she would return from her sick leave.

2.4.2. Despite the instructions to carry out the transfer in question, after the return of the complainant, another employee of OKYPY, on his own initiative, vacated the office of the complainant, in her absence and while she was on sick leave. The complainant was informed of the incident by other colleagues.

2.4.3. During the process of moving the complainant'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.

2.4.4. The DPO of OKYPY adds that, even if there was a need for immediate movement of the complainant's belongings and she could not be present, "the movement was poorly executed without first notifying the complainant of this intention and giving her the opportunity to authorize another person to be present during the moving process".

2.4.5. The Ministry of Internal Affairs, in summary, admits that:

2 (a) The staff of OKYPY is 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. In general, the practice followed is for the liquidation to take place in the presence of the subject or his authorized representative. However, in this particular case this practice was not followed. (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 complainant's possession of the physical medical files in question 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 records that he may have in his possession. (g) 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. (h) The absence of a process for managing the Medical File reveals the inability to properly process the medical files within (but also outside) the Organization, which however does not reduce the consequences of the illegal possession of the medical files by the complainant. (i) Regarding the movement of the complainant'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.

2.4.6. 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 concerning 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.).

2.5. On November 05, 2021, my Office sent an email to the complainant, raising questions about the custody of the originals 3 Legal framework medical files in the drawers of her office, as the fact that the possession of personal data, especially of special categories, automatically makes her responsible for data processing. Consequently, the responsibilities of the complainant, as a separate data controller, in the complaint in question are the subject of an independent violation on its part.

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, objectivity and transparency")". Also, in subsection (f) of the same 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. 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. 4 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, b) 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 law and social protection, if permitted by Union or Member State law or by a 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 data subject or other physical 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 legitimate activities of an institution, organization or other non-profit body with a political, philosophical, religious or trade union objective and under the condition that the processing concerns exclusively the members or former members of the organization or persons who have regular communication with it in relation to its purposes and that the personal data are not shared outside the specific organization without the consent of the data subjects, e) the processing concerns personal data that has been manifestly made public by the data subject, f) the processing is necessary for the establishment, exercise or support of legal claims or when the courts act in their jurisdictional capacity, 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 to data protection and provides for appropriate and specific measures to safeguard 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 professional in the field of health and subject to the conditions and guarantees referred to in paragraph 3, i) the processing 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 law or the law of a Member State, 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) based on Union or Member State law, which are proportionate to the objective pursued, respect the essence of right to data protection and provide for appropriate and specific measures to safeguard the fundamental rights and interests of the data subject.

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 Union or Member State law or based on rules established by competent national 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.'

3.7. Article 24(1) of the Regulation states that it is the responsibility of the controller, so in this case of the GDPR, such as, "taking into account the nature, scope, context and purposes of the processing, as well as the risks of different probability of occurrence and seriousness for the rights and freedoms of natural persons, ... implements appropriate technical and organizational measures in order to ensure and be able to demonstrate that the processing is carried out in accordance with this regulation. These measures are reviewed and updated when deemed necessary."

3.8. Also, Article 32(1) of the Regulation concerning processing security provides that, "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 seriousness for

the rights and freedoms of natural persons, the controller and the processor implement appropriate technical and organizational measures in order to ensure the appropriate level of security against the risks...". 3.9. Based on Article 57(1) of the Regulation, the Commissioner has the following tasks: "a) monitor and enforce the implementation of this regulation, b) promote public awareness and understanding of risks, rules, guarantees and rights related to processing. Special attention is paid to activities specifically aimed at children, c) advises, in accordance with the law of the Member State, the national parliament, the government and other bodies and organizations on legislative and administrative measures related to the protection of the rights and freedoms of natural persons against processing, d) promote the awareness of controllers and processors regarding their obligations under this regulation, e) upon request, provide information to data subjects regarding the exercise of their rights under this Regulation and, where appropriate, cooperates for this purpose with supervisory authorities in other Member States, f) handles complaints submitted by the data subject or by an entity or organization or association in accordance with Article 80 and investigates, to the extent appropriate, the subject of the complaint and informs the complainant about the progress and the outcome of the investigation within a reasonable period of time, in particular if further investigation or coordination with another supervisory authority is required, g) cooperates, among others through the exchange of information, with other supervisory authorities and provide mutual assistance to other supervisory authorities, in order to ensure the consistency of the implementation and enforcement of this Regulation, h) carry out investigations related to the application of this Regulation, including based on information received by another supervisory authority or other public authority, i) monitors the relevant developments, to the extent of that have an impact on the protection of personal data, in particular the developments of information and communication technologies and commercial practices, j) establishes standard contractual clauses of article 28 paragraph 8 and article 46 paragraph 2 letter d), k) draws up and maintains a list in relation to the requirement to carry out a data protection impact assessment under Article 35(4), l) provides advice on processing operations under Article 36(2), m) encourages the development of codes of conduct in accordance with article 40 paragraph 1 and formulates an opinion and approves such codes of conduct that provide adequate guarantees, in accordance with article 40 paragraph 5, n) encourages the establishment of data protection certification mechanisms and data protection seals and marks under article 42 paragraph 1 and approves the certification criteria in accordance with Article 42(5); o) as the case may be, carry out a periodic review of the certifications issued in accordance with Article 42 paragraph 7, p) design and publish the accreditation criteria for a body for monitoring codes of conduct in accordance with Article 41 and a

certification body in accordance with Article 43, q) carries out the accreditation of a body for monitoring codes of conduct in accordance with article 41 and a certification body in accordance with article 43, j) allows contractual clauses and provisions of article 46 paragraph 3, s) approves binding corporate rules pursuant to article 47, k) contributes in the activities of the Data Protection Board, k) keep internal records of violations of this regulation and measures taken in accordance with article 58 paragraph 2, and kb) fulfill any other duty related to the protection of personal data." 3.10. 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, 7 e) to instruct the data controller to announce the data breach pr of a personal 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 thirds the country or to an international organization." 3.11. 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 deciding 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, 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 as well as 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 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 data controller involved or the processor in relation to the same object, the compliance with said measures, j) the observance 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 preceding financial year, whichever is higher: a ) the obligations of the controller and the 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 shall attract, in accordance with paragraph 2, administrative fines of up to EUR 20 000 000 or, in the case of undertakings, up to 4 % of the total worldwide annual turnover of the previous financial year, whichever is higher: a) the basic principles for the processing, including the conditions applicable to the authorization, in accordance with articles 5, 6, 7 and 9, b) the rights of data subjects in accordance with articles 12 to 22, c) the transmission of personal data to a recipient in a third country or an international organization in accordance with Articles 44 to 49, d) any obligations under the law of the Member State which are established pursuant to Chapter IX, e) non-compliance with an order or with a temporary or permanent restriction of processing or to suspend the circulation of data imposed by the supervisory authority pursuant to Article 58 paragraph 2 or failure to provide access in violation of Article 58 paragraph 1.

6. The non-compliance The mandate of the supervisory authority as referred to in Article 58



paragraph 2 entails, in accordance with paragraph 2 of this article, administrative fines of up to EUR 20 000 000 or, in the case of undertakings, up to 4 % of the total worldwide annual turnover of the previous financial year, whichever is higher. 7. Without prejudice to the corrective powers of the supervisory authorities in accordance with 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 under this Article shall be subject to due process safeguards in accordance with Union law and Member State 9 Reasonable law, including effective judicial review and due process. 9. Where the legal system of the Member State does not provide for the imposition of administrative fines, this article may be applied in such a way that the enforcement procedure is initiated by the competent supervisory authority and enforced by the competent national courts, while ensuring that the because legal remedies are effective and have an equivalent effect to the administrative fines imposed by the supervisory authorities. In any event, the fines imposed are effective, proportionate and dissuasive. Those Member States shall notify to the Commission the provisions of their laws which they adopt in accordance with this paragraph by 25 May 2018 and, without delay, any subsequent amending law or amendment thereof.'

C. 4.1.1. In the present case, the complainant claims that, while she was absent on sick leave, she was informed that another employee of OKYPY emptied her office drawers and then placed her documents and personal items in paper boxes, without informing her first. Among other things, the original medical files of herself, her husband and her children were found in the drawers. The files in question were returned to the Archive of G.N. XXX, without any information and in the absence of the complainant. 4.1.2. The above allegations of the complainant have also been verified by a relevant letter from the OKYpY dated November 24, 2021. More specifically, the letter in question states that the Directorate of G.N. XXX, had given an order for the complainant to move and return to her duties at the Ministry of Health, after her sick leave. The complainant was aware of this particular move when she would return from her sick leave. However, another employee of OKYpY, on his own initiative, ignoring the instructions of the Directorate, vacated the complainant's office, during her absence. Therefore, there is the admission that the complainant's belongings were moved in her absence, unjustifiably and without her having previously been informed that the movement of her personal belongings will take place, during the essential time. OKYpY, in the same letter, notes that there are no written procedures in case of moving staff items, clearing office drawers and/or the electronic content on the computers handled by the staff. 4.2.1. I consider it appropriate to remind that personal medical files and, in general, health-related data, fall under the special categories of personal data that are processed, in

accordance with Article 9 of the Regulation. 4.2.2. I consider the fact that OKYpY is unable to detect the absence and/or loss of medical files to be of essential importance, as at least one employee, namely the complainant, had in her possession original medical files not only of herself, but also of her husband and children . The fact that, it is known to the Directorate of the Health Care Agency that the staff of the Organization withholds medical files in violation of the Law on the Establishment of the State Health Services Organization (L. 10 73(I)/2017) and the Law on the Entitlement and Protection of Rights of the Patients Law (Law 1(I)/2005), demonstrates that it is something that happens systematically, but without substantial actions being taken to deal with the phenomenon. In addition, the internal circular dated 25 October 21 with no. lens 05.25.063 reinforces the claim of the complainant that the address of G.N. XXX was aware of the act in question, which appears to be a common practice on the part of the employees. 4.2.3. Although the Directorate of G.N. XXX issued internal circulars asking staff such as those in possession of medical files to hand them over to the Patient File Archive for safekeeping, although it did not strictly and consistently enforce this. 4.3. Even if I take into account that actions are being taken to create written procedures, in order to avoid future incidents of a similar nature, as mentioned in the letter of the OKYPY dated November 24, 2021, however I consider it necessary to take strict measures, so that the due to written procedures to be implemented by OKYpY staff. 4.4. Based on the above and taking into account the admission of the OKYPY that the staff of the Organization is not sufficiently informed and aware of matters concerning personal data, I consider that the omission of further organizational and technical measures to avoid such violations constitutes on its part OKYpY, violation of the provisions of Articles 5(1)(f), 24(1) and 32(1) of the Regulation. 4.5. Regarding the fact that the complainant had in her possession the original medical files of herself, her husband and her children in violation of the Law on the Establishment of a State Health Services Organization (Law 73(I)/2017) and the Law on the Entitlement and Protection of the Rights of Patients Law (Law 1(I)/2005), this act makes it a separate controller with all the consequent obligations under the Regulation and the said act was investigated separately. 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 Law 125(I)/2018, my conclusion is that there is a violation, part of OKYpY, Articles 5(1)(f), 24(1) and 32(1) of the Regulation, since the absence of the appropriate organizational and technical measures to avoid personal data breaches, as well as the inability to detect incidents of absence and/or loss of medical files. 5.2. Based on the provisions of Article 83 of the Regulation, insofar as they are applied in this particular case, I take into account the following aggravating (1-4) and mitigating (5-8) factors: (1) the fact that the staff of OKYpY did not is sufficiently informed about

issues concerning personal data, (2) the absence of written procedures for moving objects and/or electronic personnel data and/or clearing drawers, 11 (3) the absence of a medical file management procedure, (4) the impossibility of locating absence of the medical files from the OKYpY Archive, (5) the promotion of internal circulars by the Directorate of G.N. XXX, with which he repeatedly calls on the staff to return to the Archives medical files that he may have in his possession, (6) the fact that an employee of OKYpY acted arbitrarily, despite the orders of the Directorate of the Organization, (7) the examination for taking more effective organizational and technical measures to comply with the provisions of the Regulation, and (8) cooperation with my Office.

5.3. Having taken into account and taken into account – (a) The applicable legislative basis regarding the prescribed administrative sanctions in the provisions of Article 58(2) and Article 83 of the Regulation. (b) All the circumstances and factors that OKYpY put before me based on all existing correspondence. (c) The above mitigating and aggravating factors. I consider that, under the circumstances, the imposition of an administrative fine is not justified, since the employee in question acted arbitrarily, despite the orders of the Directorate of the Organization and at the same time measuring the responsibility of the complainant herself, who was in possession of original physical medical files.

5.4. Nevertheless, bearing in mind the above facts, the legal aspect on which this Decision is based and the analysis as explained above, exercising the powers granted to me by Article 58(2)(d) of the Regulation, I issue an Order to OKYPY such as: (a) prepare written procedures regarding the transfer of personnel and the movement of their personal belongings and if deemed necessary, update and/or strengthen the existing written procedures, and (b) take strict measures, in order to implement the written procedures , on behalf of the employees of OKYpY, within one and a half (1.5) months from the receipt of this Decision.

5.5. In the event that the above deadline has passed and OKYPY has not informed me of its compliance with the above within the set date, providing relevant evidence, I will consider whether it is appropriate for me to take further corrective measures, including the administrative sanction offline.

5.6. It is further provided that, in the event of future submission to my Office complaint of a similar nature, the complaint will be examined, among others, for potential violation of the Order, which, according to article 33(1)(b) of the Law 125(I)/2018, constitutes a criminal offence.

Irini Loizidou Nikolaidou

Data Protection Commissioner

Personal Character

Nicosia, 4 May 2022