REPUBLIC OF CYPRUS OFFICE OF THE COMMISSIONER FOR PROTECTION OF PERSONAL DATA COMMISSIONER

No. Fac.: 11.17.001.009.224 DECISION Complaint against the State Health Services Organization regarding a breach of his personal data I refer to the complaint which was communicated to my Office, on October 04, 2021, through a letter addressed to the Ministry of Health, on behalf of of Mr. —H (hereinafter the "complainant"), an employee of the State Health Services Organization (hereinafter the "Organization"), from the law firm Elena Mala & Associates D.E.P.E., as well as in all the relevant with the above subject correspondence, which is part of the case file, based on which there is a violation, on the part of the Organization, of articles 5(1)(a), (c), (f), 6(1), and 9(1) of the General Data Protection Regulation, (EU) 2016/679 (hereinafter the "Regulation"). A. Circumstances of the case, among others, the Financial Officer of the Organization (hereinafter the "Financial 2.1. The complaint refers to, Director of the Directorate Director"), by letter dated 08/26/2021 to the attending physician of the complainant HHHHHHHI (hereinafter the "doctor"), asked for clarifications and justification of the issuance of a three-week sickness certificate, which he issued on the 26th. It should be noted that the complainant works in July 2021 B9; for the complaint 2.2. In the CFO's letter, which was shared with my Office, it appears that the CFO asked the doctor to provide him with copies of relevant evidence and diagnostic and other tests that may have been in the complainant's medical record. He also reported to the doctor details relating to the complainant's sick leaves and information contained in his leave register. 3.1. On October 22, 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 Organization, in which it was informed about the complaint in question and invited Iasonos 1, 2nd Floor, 1082 NICOSIA / P.O. 23378, 1682 NICOSIA-CYPRUS, Tel. +357 22818456, Fax +357 22304565 E-GP3II: ^™ini$5ioithG@a3i3rGlioIioin.9on.(:c, \L/th6$iin6: IIIIIr:/LL/nnnn.P3I3rGti6aiioni.9on.<:n as, until on November 05, 2021, informed me regarding the positions on the allegations of the complainant. More specifically, it was requested, by the above date, to inform my Office regarding: a. The legal basis on which the doctor was requested to provide documents from the complainant's medical file b. The manner in which the details of the complainant's license register had come into the possession of the Financial Director and whether they had been forwarded to his doctor c. The authority under which the investigation of the objectivity of the certificates was carried out illness of employees of 3.2. On November 05, 2021, my Office received an electronic letter, from the Organization, in which, among other things, the following are mentioned: a. The Financial Director with the intention of performing tasks that fall under his competence, as a Housekeeper Director and member of a three-member Management Team investigated the reasons why the doctor granted continuous sick leave to the

complainant, since there were suspicions of abuse of privileges and fraud of the Agency by the complainant. b. The Financial Director, in an attempt to manage the case confidentially, proceeded to investigate the incident himself instead of the appropriate procedure for employee disciplinary investigation matters, without following Internal Regulation 1 "Recording of Events" through which: - An authorized officer is designated for management of these issues. - In the event that potential disciplinary offenses are found, then the case is referred to the Organization's Disciplinary Council if it concerns staff of the Organization, or to the Public Service if it concerns a seconded civil servant in accordance with the Public Service Law of 1990 (Law 1/1990). - If the event is of a medical nature, an opinion is requested from the Medical Council. c. The data for the investigation and filing of the case (sick leave register, sick leave attachments, etc.) were collected by the Human Resources department of HHHH^HHHHHH and then the Financial Director, again for the purposes of investigating the case, communicated the above data to the physician to provide answers/clarifications. d. The Financial Director does not have medical knowledge, nor does he have the authority to evaluate the adequacy and correctness of medical procedures performed by doctors. His duties include inspecting and auditing the sick leave levels of existing staff, to confirm that the balance of meeting the personal needs of staff is maintained with the correct use and not abuse of the system. 2 3.3 In addition to the above, the following are mentioned in said electronic reply letter: a The Financial Director's request for access to the complainant's health data. lacks a legal basis and the disclosure of the complainant's license register to the doctor is not justified. b Despite the intentions of the Financial Director to perform his duties, it is clear that there is also a reduced understanding of the principles and provisions of the Regulation. c The Personal Data Officer of the Organization plans, among other actions, training on the subjects of the Regulation for all the managerial staff of the Organization, which the Financial Director will also propose to attend. In addition, it has already been pointed out to the Financial Director that in the future in similar cases the internal regulations / procedures of the Organization should be followed 4 On December 22, 2021, a prima facie decision was delivered to the Organization, after I found that there is a prima facie violation of Articles 5 (1) (a), (c), (f), 6(1) and 9(1) of the Regulation. The Organization, through a letter dated January 05, 2022, repeated everything it had stated to my Office through the reply letter dated November 05, 2021, additionally including the following clarifications / information: a The Financial Director does not have medical training, nor the authority to evaluate the adequacy and correctness of the medical procedures of doctors and did not do this b In the context of the Organization's action plan to strengthen the perception and knowledge of all its staff regarding the provisions of the relevant Regulation, training was implemented on the

subjects of the Regulation, initially at the local Contact Points of Personal Data in all Directorates / Hospitals, and subsequently to all the management staff of the Organization, in which the Financial Director also participated. The said training was implemented after the above incident. c. In addition, as a corrective measure, the gradual implementation of multiple trainings for all the staff of the Organization on the subjects of the Regulation is planned, as my instructions in a previous letter. The Organization has a staff of more than 7,000 people. It is planned, in consultation with the Ministry of Foreign Affairs and the local Personal Data Contact Points of the Organization, lifelong training that will be attended by all the staff d The Organization's concern is compliance with the provisions of Regulation 3 B. Legal Framework 5.1 Article 4 of the Regulation defines as: a "personal data"? any information concerning an identified or identifiable natural person ("data subject") the identifiable natural person is one whose identity can be ascertained, directly or indirectly, in particular by reference to an identification element such as a name, an identification number, a location data, an online identifier or one or more factors that characterize the physical, physiological, genetic, psychological, economic, cultural or social identity of that natural person'. b "processing", any operation or series of operations carried out with or without the use of automated means, on personal data or sets of personal data, such as collection, registration, organization or structuring, storage, adaptation or alteration, retrieval, retrieval of information, use, disclosure by transmission, dissemination or any other form of disposal, association or combination, restriction, deletion or destruction', c "controller", the physical or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and manner of processing personal data when the purposes and manner of such processing are determined by Union law or of a Member State, the controller or the specific criteria for his appointment may be provided for by Union law or the law of a Member State', d "data relating to health" personal data ha which are related to the physical or mental health of a natural person, including the provision of health care services, and which disclose information about the state of his health", with "personal data breach" the breach of security that leads to accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access of personal data transmitted, stored or otherwise processed" 5.2 With reference to health-related data, recital 35 of the Regulation clarifies that "The data personal health-related data should include all data relating to the data subject's state of health and which disclose information about the data subject's past, current or future state of physical or mental health. This includes information about with the natural person they collect when registering for health services and when providing them as referred to in Directive 2011/24/EU of the European Parliament and of the Council to the said natural person a number, a symbol or an identity characteristic assigned to

a natural person for the purpose of full identification of the natural person for health purposes information resulting from examinations or analyzes of a part or substance of the body, including genetic 4 data and biological samples and any information for example. about disease, disability, risk of disease, medical history, clinical treatment or the physiological or biomedical condition of the data subject, regardless of source, for example. by a doctor or other health care professional, hospital, medical device or in vitro diagnostic test' 5.3. Pursuant to article 5, paragraph 1 of the Regulation concerning the Principles governing the processing of personal data, these data, among others, as referred to in subsection (a), are processed lawfully and legitimately in a transparent manner in relation to the subject of the data ("legality, objectivity and transparency") 5.4 Also in the same paragraph of Article 5, point (c) it is provided that personal data "are appropriate, relevant and limited to what is necessary for the purposes for which they are processed ("data minimization")" Furthermore, point (f) states that personal data "are processed in a manner that guarantees the appropriate security of personal data, including its protection against unauthorized or unlawful processing and accidental loss , destruction or deterioration, using appropriate technical or organizational measures ("integrity and e confidentiality')'. 5 5 According to paragraph 1 of article 6 of the Regulation, 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 his personal data 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 before entering into a contract, c the processing is necessary to comply 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 in the exercise of public authority assigned to the controller, f. h processing is necessary for the purposes of the legal 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 subject of the data 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." 5 6. Based on paragraph 1 of article 9 of the Regulation, the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or membership in a trade union is prohibited, as well as the processing of genetic data, biometric data for the purpose of unambiguously identifying a person 5 data concerning health or data concerning a natural person's sexual life or sexual orientation 5 7. In the same article, i.e. article 9. in paragraph 2. it is clarified that the previous paragraph does not apply in specific cases. Specifically in point (h) it

is stated that paragraph 1 does not apply when "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 Member State law or under a contract with a healthcare professional and subject to the conditions and guarantees referred to in paragraph 3". 5 8 With reference to the processing of special categories of personal data, recital 51 of the Regulation states that "Personal data which are inherently particularly sensitive in relation to fundamental rights and freedoms need special protection, as the context of their processing will could create significant risks to fundamental rights and freedoms." 5 9 Pursuant to paragraph 2 of article 58 of the Regulation "each control authority has all the following corrective powers a to send warnings to the controller or "tto the processor that intended processing operations are likely to violate the provisions of this regulation, b to send 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. instruct the data controller or 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 notify the personal data breach to the data subject, f to impose a temporary or definitive restriction, including the prohibition of processing, g to instruct the correction or deletion of personal data or restriction of processing pursuant to of articles 16, 17 and 18 and order notification of these actions to recipients to whom the personal data was disclosed pursuant to article 17 paragraph 2 and article 19, or to withdraw the certification or order the certification body to withdraw a certificate issued in accordance with Articles 42 and 43 or to order the certification body not to issue certification if the certification requirements are not met or are no longer met, i to impose an administrative fine under Article 83. in addition to or instead of the measures referred to in this paragraph, depending on the boundaries of each individual approx , 6 i to give an order to suspend the circulation of data to a recipient in a third country or an international organization" 5 10 Additionally, article 83 of the Regulation, which concerns the general conditions for imposing administrative fines, provides that: "1 Each supervisory authority ensures so 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 for each individual case effective, proportionate and dissuasive 2 Administrative fines, depending on the circumstances of each individual case, are additionally imposed or instead of the measures referred to in article 58 paragraph 2 points a) to h) and in article 58 paragraph 2 point j) When making a decision on the imposition of an administrative fine, as well as on the amount of

the administrative fine for each individual case , due consideration shall be given to the following a the nature, gravity and duration of the infringement, taking into account the nature, t 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, with any relevant previous violations of controller or processor, f the degree of cooperation with the supervisory authority to remedy the breach and limit its possible adverse effects, g the categories of personal data affected by the breach, or the way in which the supervisory authority was informed of the violation, in particular if and to what extent the data controller or the processor gasia notified the violation, i in case 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, i the observance of approved codes of conduct in accordance with article 40 or approved certification mechanisms in accordance with article 42 and 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, by 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 7 4. Violations of the following provisions incur, in accordance with paragraph 2, administrative fines of up to 10 000 000 EIIP or, in the case of enterprises, up to 2% of the total global annual turnover of the previous financial year, depending on which 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 c the obligations of the monitoring body in accordance with article 41 paragraph 4 5 Violations of the following provisions entail, in accordance with paragraph 2,administrative fines of up to 20 000 000 EIIP or, in the case of enterprises, 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 established under Chapter IX.

non-compliance with an order or temporary or permanent restriction of processing or suspension of data circulation imposed by the supervisory authority pursuant to Article 58 paragraph 2 or failure to provide access in violation of Article 58 paragraph 1

6 Failure to comply with an order 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 20 000 000 EuF or. in case of businesses, up to 4% of the total worldwide annual turnover of the previous financial year, whichever is higher. (...)»

C. Rationale

6 1 The data included in the license register constitute "personal data" Data relating to the health and/or medical history of a natural person and specific disease certificates, "evidence and diagnostic and other tests" contained in a medical file , fall under the "special categories of personal data", according to article 9 of the Regulation.

62 The collection, storage, search of information, use, disclosure by transmission, dissemination or any other form of disposal, etc. constitute processing of personal data, within the meaning of article 4(2) of the Regulation

6 3 As stated in the Organization's letters dated 05 November 2021 and 05 January 2022. the Financial Director with the intention of executing the

8

of his duties, he investigated the incident related to the granting of sick leave to the complainant. but not through "the appropriate procedure for matters of disciplinary investigation of employees and without following the Internal Regulation".

6 4 For personal data to be lawfully processed, the conditions for compliance with the principles governing the processing of personal data, which are determined by Article 5 of the Regulation, must be cumulatively met. The existence of a legal basis is also necessary, based on Article 6(1) of the Regulation

6 5 During the investigation, which was carried out in violation of his duties, the Financial Director proceeded to collect data from the license register and the complainant's health certificates, as well as forwarding/notifying them to the doctor. The actions taken. were not done lawfully and legitimately ("lawfulness"), as provided for in Article 5(1)(a), resulted in the data not being limited to what is necessary for the purposes for which they are processed ("minimization"), as provided for in Article 5(1)(c) and neither is confidentiality satisfied based on Article 5(1)(f), since they were communicated to an unauthorized person, i.e. the doctor

6 6 Regarding the legality of the processing of the complainant's data. none of the conditions of article 6(1) of the Regulation

are met, since this was not done legally. I also note that the Organization admitted that there is a request by the Financial Director for access to health data, which lacks a legal basis and that the publication of a license register of the patient to the physician is not justified

6 7 Additionally, and taking into account that the appropriate procedure was not followed, it follows that there is a violation of Article 9(1) of the Regulation, since the data of the complainant that were processed, belong to the special categories of data, as data related to health. It is noted that, in this particular case, the exception referred to in subsection (h) of Article 9(2) of the Regulation does not exist,

6 8 I consider essential, as recognition of the violation, the Organization's admission that there is a reduced understanding of the principles and provisions of the Regulation and that it has been pointed out to the Financial Director that in future similar cases, the internal regulations / procedures of the

Organization.

6 9 Regarding staff training, based on the Orders I gave to the Organization, with my Decision issued on November 04, 2021, the Organization

informed me

a. with a letter dated December 09, 2021 that the training of the management teams has been completed,

b by letter dated November 23, 2021 that the training of 17 officials, who are responsible for observing, supervising and implementing issues related to the protection of personal data, has been completed, and

V regarding the implementation plan for the training of all staff, for which I had set a deadline of November 04, 2022

6 10 Along with the attendance record for the training of the managerial staff, as it is referred to in point 6 9 a hereof, I confirm that the Financial Director attended said training.

6 11 Irrespective of the above, in the event that issues of employee behavior and/or labor relations issues arise based on the specific incident, I point out that these are not matters that fall within my responsibilities. and therefore I have not examined them.

D. Conclusion

7 Having taken into account all the facts concerning the present case, as well as the factors below

7.1 Mitigating Factors:

- the incident resulted from the effort of the Financial Director to manage the case confidentially and with the intention of performing the tasks falling within his competence, due to the existence of suspicions of abuse of privileges and deception of the Organization by the complainant,

* the Organization's admission that the Financial Director's request for access to the complainant's health data. lacks a legal basis and the disclosure of the complainant's license register to the doctor is not justified.

- the Organization's admission that there is a reduced understanding of the principles and provisions of the Regulation, in relation to the implementation of training.

- the implementation of training on the subjects of the Regulation to the management staff of the Organization, in which the Financial Director also participated, as well as the planned training plan for all staff.

7 2 Aggravating Factors

- the fact that while there is a recorded Sick Leave Management procedure as mentioned, it was not followed,

and exercising the corrective powers conferred on me by Article 58(2)(b) of the Regulation, pursuant to which. "Each supervisory authority has all of the following corrective powers (b) to address reprimands to the controller or processor when processing operations have breached provisions of this Regulation."

8 I decided

at my discretion and subject to the above provisions, to address to the Organization

Reprimand for violation of articles 5(1)(a), (c).(f). 6(1) and 9(1) of the Regulation.

Irene LoH

Irini Loizidou Nikolaidou Commissioner for Personal Data Protection

Nicosia. May 4, 2022