No. Fax: 11.17.001.006.016 June 12, 2019 Director General of the Ministry of Health Corner of Prodromou 1 & Chilonos 17 1448 Nicosia, Cyprus PERSONAL DATA PROTECTION COMMISSIONER DECISION SUBJECT: Complaint for possible violation of the GDPR – AP 249/2018 Complaint dated 12 December, 2018 submitted to my Office for non-observance of security measures in the processing of personal data of M.M. on behalf of the Ministry of Health, I am informing you of the following. 2. Specifically, the complainant was informed by a family friend that on and/or around June 27, 2018, a Ministry of Health usher, during the transfer of files, did not take the appropriate security measures, resulting in his personal data being in public view. In particular, a folder on the outside was written, M.M. INTIMIDATION OF EMPLOYEES, as a result of which it was read by a third person, who also informed him of this fact. 2.1. In addition, the complainant claims that the reason he did not submit the complaint to my Office earlier is because he did not realize the seriousness of the General Data Protection Regulation (EU) 2016/679 (hereinafter the "GDPR"). 3. My Office, by letter dated 19/12/2018, informed the Data Protection Officer (hereinafter "DPO") of the Complainant about the allegations of the complainant and asked for their own opinions and positions on the subject until 12/1/2019. 4. The response of the DPO of the Ministry of Health was sent to my Office on 21/5/2019 and states the following: - According to information received from the head of the file of the Ministry of Health, on the circulation card of the file named "M. M. - Intimidation of an Employee" states that the specific file was debited, for a period of 23 months, in the name of Nursing Officer A.F., who worked in the Nursing Services Directorate, - The file was returned to the file on 6/25/2018, - The file is classified in the Classification category "Confidential" and is being handled by the relevant officers handling the matter, as a classified file, - The officer handling the file reported that the file was debited to his name for a long time due to the continuous handling of of various ongoing disciplinary proceedings involving the complainant, - The file was locked in the office of the officer handling the case and he excludes the possibility that there was any violation during the time he was there, - When the file was returned to the file , the officer reports that the appropriate procedures followed for all confidants were followed files, ie the file was placed by the Secretary of the Nursing Services Department in another file and sent to the file by hand. 4.1. In the same letter dated 5/21/2019, the DPO of the Ministry of Health states that both in the case of classified documents and personal data, the Ministry of Health takes all appropriate technical and organizational measures to secure the data. 4.2. Specifically, in the cases of classified documents, these are handled on the basis of the Security Regulations of Classified Information, Documents and Material and Related Matters Law of 2002 (216(I)/2002), such as handling of the files by an authorized officer, movement of the file in a closed folder by writing the name of the operator who

will handle it in order to move the folder from/to the file/competent operator for handling, locking the folders in a cabinet located in the file area, etc. 4.3. Regarding the protection of personal data, as reported by the Ministry of Health's Office of the Ministry of Health, a lecture was held on 4/4/2018 for information by the Commissioner for Personal Data Protection, a circular was sent by the Director General of the Ministry of Health on 5/4/2018 to all Directors/Associates Directors of the Departments of the Ministry of Health for compliance with the GDPR and on 19/4/2018 a circular was sent again that specified both the competent DPO of the Ministry and the officials designated as contact points for each department and sector of the Ministry of Health. 4.4. As part of the investigation of this complaint, a reminder circular was sent to all staff on the implementation of the GDPR and in particular on maintaining security and avoiding processing in violation of the GDPR. 4.5. The Department of Health management takes the protection of personal data and classified documents handled within the Department of Health very seriously. As mentioned, meetings have been held with all relevant departments of the Ministry of Health administration (such as the subsidized patient sector, the health monitoring unit, the archive, etc.) both to confirm that all the necessary security measures are being followed and in the context of the regular checks carried out by the Ministry itself. 4.6. The security measures taken by the Ministry of Health concern, among other things, the encryption of information where required, safe storage of files in locked boxes, safe storage of data with access codes on the computers of operators who keep sensitive personal data, pseudonymization and encryption, etc. 5. The provisions of article 32 of the GDPR explicitly define the following: "1. Taking into account the latest developments, the cost of implementation and the nature, scope, context and purposes of the processing, as well as the risks of different probability of occurrence and severity for the rights and freedoms of natural persons, the controller and the executor the processing implement appropriate technical and organizational measures in order to ensure the appropriate level of security against risks, including, among others, as appropriate: a) the pseudonymization and encryption of personal data, b) the ability to ensure confidentiality, integrity, availability and reliability of processing systems and services on an ongoing basis, c) the possibility of restoring the availability and access to personal data in a timely manner in the event of a physical or technical event, 2 ensuring the security of organizational measures for d) process for the tical testing, assessment and evaluation of the effectiveness of techniques and processing……. 4. The controller and the processor shall take measures to ensure that any natural person acting under the supervision of the controller or the processor who has access to personal data processes it only on the instructions of the controller, unless required to do so by Union or Member State law'. 5.1. In addition, References 74 and 83 of the Preamble of the GDPR state,

inter alia, that the controller should be required to implement appropriate and effective measures and be able to demonstrate the compliance of the processing activities with the GDPR, including the effectiveness of the measures . 5.2. Such measures should take into account the nature, context, scope and purposes of the processing and the risk to the rights and freedoms of natural persons. To maintain security and avoid processing in breach of this Regulation, the controller or processor should assess the risks involved in the processing and implement measures to mitigate those risks, such as through encryption. Such measures should ensure an appropriate level of security, which includes confidentiality, taking into account the latest developments and the cost of implementation in relation to the risks and the nature of the personal data to be protected. 6. In this case, the Complainant took measures and proceeded with procedures, prepared a plan for information and monitoring and took measures to observe the security of personal data processing. 6.1. According to the evidence before me, the incident reported to my Office is likely to have occurred but this cannot be definitively confirmed. 6.2. On the one hand, there is the claim by the Complainant that the transfer of the file took place on 25/6/2018 and after all the necessary measures were taken, on the other hand, the complainant of the file was carried out on 27/6/2018, a date on which the complainant's family friend was at the Ministry of Health. According to the complaint form, the complainant's family friend was in the elevator with another person, who he assumed was the usher, and who was holding and carrying the file in question. 6.3. The incident occurred in June 2018, the complaint to my Office was submitted six (6) months later, i.e. December 2018.complicates the investigation process.

7. Article 58 par. 2(a) of GDPR 2016/679 gives me the authority as Commissioner
Personal Data Protection, among others, to address
warnings to the controller or processor that
intended processing operations are likely to violate provisions herein
regulation.

8. Bearing in mind the above facts, the legal aspect on which the
this decision and the analysis as explained above, below
powers granted to me by article 58 par. 2(a) of GDPR 2016/679, addressed
warning to the Ministry of Health as, in the future, when a transfer is made
claims that the transfer date

files, observes the appropriate security measures in such a way that there is no suspicion,

in any way, revealing the identity of the person.

Irini Loizidou Nikolaidou

Data Protection Commissioner

Personal Character