Information and Data Protection Commissioner

CDP/COMP/700/2024

[redacted]

vs

[redacted]

COMPLAINT

1. On the 12th October 2024, [redacted] (the **"complainant"**) lodged a complaint with the Information and Data Protection Commissioner (the **"Commissioner"**) pursuant to article 77(1) of the General Data Protection Regulation[1] (the **"Regulation"**), alleging that an employee of [redacted] (the **"controller"**) accessed his personal data while he was a patient of the controller.

INVESTIGATION

Request for submissions

2. Pursuant to the internal investigation procedure of this Office, the Commissioner sent a copy of the complaint to the controller and provided the controller with the opportunity to make any submissions which it deemed relevant and necessary to defend itself against the allegation raised by the complainant.

3. On the 20th November 2024, the controller confirmed that the employee in question had accessed the complainant's profile in violation of established procedures and had been dismissed on the 8th October 2024 for breaching access protocols and that the complainant had

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[2] [redacted] (C [redacted]) having its registered address at [redacted], (according to the Malta Business Registry records accessed on 30th April 2025).

been informed accordingly. The controller explained that the employee had exceeded their authorised access rights and that corrective action was taken. Additionally, on the 26th November 2024, the controller submitted a copy of its Data Protection Policy, specifically referencing Section 5.1, which clearly states that employees should only access records of patients with whom they are directly involved. The controller also noted that its employees are required to sign a Non-Disclosure Agreement (NDA).

LEGAL ANALYSIS AND DECISION

4. During the course of the investigation, the Commissioner established that an employee accessed the complainant's personal data while he was a patient of the controller. The controller confirmed in its submissions that the access occurred without authorisation and in breach of its internal policy. After confirming that unauthorised access had occurred, the Commissioner sought to determine whether such access could be justified as reasonably necessary for the provision or facilitation of healthcare or for another lawful purpose. In this regard, the controller stated that the employee accessed the data for personal reasons and had no role in the complainant's care. Accordingly, the Commissioner concluded that the processing of the complainant's personal data by the employee lacked a lawful basis under the Regulation and thus, this access constituted a violation of the controller's Data Protection Policy.

5. In view of the above, the Commissioner examined the technical and organisational measures implemented by the controller at the time of the incident to assess whether these were appropriate under article 32(1) of the Regulation. Article 5(1)(f) of the Regulation lays down the principle of integrity and confidentiality, which establishes that processing shall be carried out in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. By virtue of the principle of accountability held under article 5(2) of the Regulation, the controller is responsible for and must be able to demonstrate compliance with the principles of data processing.

6. The principle of integrity and confidentiality is further specified in article 32(1) of the Regulation, which is more prescriptive and sets out the obligations to which the controller is subject in terms of data security. According to article 32(1) of the Regulation, the controller is required to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of

varying likelihood and severity for the rights and freedoms of natural persons. This indicates that the controller should identify the specific risks and assess the potential impact having regard to the particular circumstances of the processing and implement appropriate measures to mitigate those risks which are likely to materialise. Article 32(1) of the Regulation provides a non-exhaustive list of measures which are deemed effective to ensure compliance with the data protection legislative framework.

7. In its submissions, the controller provided a copy of the Data Protection Policy which was already in place at the time of the incident and included various access provisions. In particular, section 5.1 of the Data Protection Policy clearly stipulates that *"[s]taff should only have access to personal data and / or sensitive personal data in the following circumstances: 5.1.1 Where they are involved in that person's healthcare; 5.1.2 For personnel / HR issues, where the employee is authorised to access personnel files;"*. Additionally, section 5.2.7 of the same policy makes an important qualification regarding the risk of misuse of personal connections, stating that *"[s]taff must not access records of people they know (whether a relative or not) without a legitimate clinical reason for doing so or unless they obtain written consent from the patient"*.

8. The Commissioner acknowledges that the controller had data protection measures in place, including internal policies limiting access to data on a need-to-know basis, role-based access controls and prohibition of the unauthorised use of patient information, reinforced by the requirement to sign Non-Disclosure Agreements (NDAs).

9. In the circumstances of this case, the employee's conduct constituted an unauthorised act in direct violation of the controller's established policies. The controller responded promptly by investigating the incident, taking disciplinary action and informing the complainant. During its investigation, it was established that the employee's actions were for personal reasons, thereby the employee's actions fall outside the lawful access scenarios outlined in section 5.1 and directly disregarded the restrictions in section 5.2.7 of the Data Protection Policy.

In light of the foregoing, the Commissioner concludes that the employee accessed personal data without authorisation and in clear breach of the controller's Data Protection Policy. However, the Commissioner is satisfied that the controller had implemented all the reasonable and proportionate technical and organisational measures, in line with article 24 and article 32 of the Regulation, to protect personal data and prevent unauthorised access. The controller also responded promptly and appropriately upon becoming aware of the incident, including taking

disciplinary action against the employee and notifying the data subject. Accordingly, the Commissioner considers the case closed.

Ian DEGUARA (Signature)
Digitally signed by Ian DEGUARA (Signature)
Date: 2025.04.30 10:01:21 +02'00'

Ian Deguara
Information and Data Protection Commissioner

Right of Appeal

In terms of article 26 (1) of the Data Protection Act (Cap 586 of the Laws of Malta), *"**any person to** whom a legally binding decision of the Commissioner is addressed, shall have the right to appeal in writing to the Tribunal within twenty days from the service of the said decision as provided in article 23".*

An appeal to the Information and Data Protection Appeals Tribunal shall be made in writing and addressed to:

The Secretary
Information and Data Protection Appeals Tribunal
158, Merchants Street
Valletta.