idpc.

Information and Data Protection Commissioner

CDP/COMP/910/2023

[redacted]

vs

[redacted]

COMPLAINT

1. On the 26th October 2023 [redacted] (the **"complainant"**) lodged a complaint against [redacted] (the **"controller"**) 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 the controller lost her personal data as a result of the lack of appropriate security measures, and therefore, considered this to be an infringement of the provisions of the Regulation.

2. The complainant outlined the following relevant facts in relation to her complaint:

   a. that, on the 2nd September 2023, the complainant underwent a surgery, which was performed at [redacted];

   b. that the complainant had provided the controller with an original copy of the MRI report and the CD with medical imaging which were carried out at another hospital;

[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.

c. that the controller was supposed to take a copy of the MRI report and the CD with medical imaging and return the original copies to the complainant, however, the controller mistakenly kept the original copies;

d. that the complainant was informed by the controller that the original copies were to be left at the reception and could be picked up by the complainant; and

e. that the complainant could only pick up the original copies on the 26th October 2023, when she was informed by the receptionist that they could not find the original copies of the MRI report and the CD with medical imaging.

INVESTIGATION

3. Pursuant to this Office's investigation procedure and in terms of article 58(1)(a) of the Regulation, on the 9th November 2023, the Commissioner requested the controller to provide information which is relevant to defend itself against the allegation raised by the complainant. In particular, the Commissioner requested the controller to provide the following information:

   a. to explain how manual records containing the patients' data are stored;

   b. to indicate which security measures are implemented by the controller to ensure that the data are stored in a secure manner;

   c. to indicate who has access to the manual records held by the controller;

   d. to provide, if any, copies of the policies and procedures in relation to the secure processing of manual records; and

   e. to indicate if any action has been taken to locate the data of the complainant.

4. On the 29th November 2023, the controller provided the following arguments for the Commissioner to consider during the legal analysis of this case:

a. that the controller maintains a secure Medical Records department where patient information is stored, however, the original copies were kept by the controller on a temporary basis as these did not fall within the controller's record storing process;

b. that the controller requested the complainant's data as a routine process carried out during a surgery for use of the medical imaging made for the surgical operation and the controller used the MRI CD to upload the images;

c. that the original copies of the records were retained by the controller in error as they were not handed back to the complainant when she was discharged, which is the normal procedure;

d. that upon the request of the complainant, the original copies were left at the reception for collection, however, the complainant was not able to collect the envelope containing these records for about a month, and in the meantime, the envelope was misplaced;

e. that, therefore, the controller treated the envelope as a belonging left behind by the complainant and kept at reception awaiting collection;

f. that the controller treats all personal data, especially medical data, that is an integral part of its operations with the utmost care, taking all the necessary technical and administrative measures in order to securely store data;

g. that even though the related personal data of the patient had been collected, processed and later stored by the controller, only the copy of the written medical report was retained and considered as a medical record;

h. that regardless of its content, the data were considered as a personal belonging of the complainant, and it was only meant to be kept for a temporary basis;

i. that the [redacted] department employs stringent security measures, including protection from fire and theft, and access is restricted to authorised personnel through RFID cards, and the area is monitored by CCTV surveillance;

j. that the only authorised people who have access to the manual records held by the controller are the personnel of the [redacted] department and further personnel that are providing medical services to the patients or processing payments;

k. that the internal investigation revealed that the complainant's belongings, in this case an envelope with her medical records, were inadvertently placed in a box folder at main reception, and a delay occurred in the patient retrieving her belongings;

l. that due to the fact that storing such records is not part of the responsibilities and capacity of the attendants of reception, it may not be expected from employees to treat any other belonging left in the reception nor to foresee the importance of the content of it as they are left at their owners' own risk;

m. that the controller acknowledges the importance of the data that the belongings contained, and remedial actions are being continuously implemented to prevent the recurrence of such incidents and that as a result, the controller is revising its process for storing records by incorporating lockable devices and maintaining a logbook to enhance accountability and traceability;

n. that the main reception assured the controller that the patient's record was not handed to another individual, however, a lapse was identified in the timely reporting of this incident, and the controller addressed this by raising awareness among receptionists and reprimanding the Head of Department for not escalating the issue and reporting it through the company's onlin[redacted] as stipulated in the [redacted][2]; and

o. that the controller is committed to continuous improvement, and corrective and preventive actions are consistently applied to prevent the recurrence of similar incidents, and guidelines for incidents management are readily available on the intranet, emphasising the importance of reporting such incidents promptly.

5. The Commissioner provided the complainant with the opportunity to rebut the arguments of the controller. By means of a letter dated the 17th December 2023, the complainant submitted the following facts in relation to her case:

[2] The controller provided a copy of [redacted].

a. that the complainant requested the original medical report and the MRI CD in person whilst visiting the hospital to remove the stitches, and she was guided by the receptionist to speak to the liaison officer in charge on the 14th September 2023;

b. that the liaison officer informed the complainant that she would need to check with the medical records department and call her later;

c. that after the complainant returned home, the liaison officer informed the complainant that the official medical reports and MRI CD were ready for her to pick up;

d. that due to limited mobility, the complainant could not pick up the data and therefore the liaison officer informed her that the normal procedure is to leave the papers at the reception and pick them up whenever possible; and

e. that the complainant informed the liaison officer that her next appointment was in a month's time and hence, the controller was aware that some time would pass before the complainant could pick up the data.

The complainant further made these submissions in relation to the present case:

f. that it is inherently incorrect that it is being argued that the medical data were considered to be a "*personal belonging of the complainant*";

g. that the complainant would like to seek a clarification as to how the hospital could confirm that the documents were not handed over to another individual and yet they could not track down what happened to these documents;

h. that if the receptionists and the [redacted] are handling personal data, with some documentation also including medical data, the controller should provide training to its personnel; and

i. that the incident was a clear breach of the Regulation, which although not malicious in nature, resulted from the lack of training and procedures, and left the complainant with little control or options over how to retrieve her own medical data, which were kept unlawfully and processed incorrectly by the controller.

6. On the 15th January 2024, the controller provided its final submissions in relation to this complaint:

   a. that the staff involved in this case received training in relation to data protection;

   b. that the medical records – a report and MRI CD – were not the property of the controller as these were prepared by another clinic and brought to the hospital by the complainant to be used by the surgeons before and during the procedure, which is indeed a common practice;

   c. that after the surgery, these records are returned to the patient, however, in this case, this did not happen, and the data were placed with the hospital's medical records until such time these were delivered to the patient;

   d. that the documents were misplaced after being removed from the secure medical records room and handed to reception for collection by the complainant;

   e. that the controller believes that the documents have been misplaced and not handed to the wrong person because if that was the case, that person would have returned them to the hospital and requested the proper report and CD as another person's data would be useless for their treatment;

   f. that the controller strongly denies that at any time held or processed the data unlawfully, and the data were only used for the patient's procedure and were not processed in any other way at any time other than to remove them from the Medical Records room and take them to reception for collection;

   g. that the controller takes handling of patient data very seriously and does its utmost to ensure confidentiality, integrity and availability of medical records at all times, however, human error is unavoidable and will happen from time to time irrespective of the number of controls implemented and training carried out; and

   h. that the controller assures the Commissioner and the complainant that it had learned from this mistake and will be revising its procedure for the handling of such cases to prevent repeating these unfortunate cases.

7. On the 17th January 2024, the Commissioner requested the controller to submit further clarifications in relation to its submissions:

   a. to indicate if the box file containing the personal data of the complainant, which was left in the reception, was kept under lock and key; and

   b. to provide evidence that the staff involved in this case received data protection training, including the dates of training.

8. On the 26th January 2024, the controller submitted the following clarifications:

   a. that the box file was not being kept under lock and key, however, it was placed in a cabinet at the back office of the reception, which is manned by the reception team 24/7; and

   b. that training on data protection was provided to the personnel involved in this case and this was supported by attendance sheets which demonstrate that training was provided in July 2023.

LEGAL ANALYSIS AND DECISION

9. During the course of the investigation, both parties confirmed that the medical records of the complainant, which included a medical report and MRI CD, were lost whilst being held by the controller. In its submissions, the controller argued that the data of the complainant were considered as "*a personal belonging of the complainant*", and therefore, the data did not fall within the record storing process of the hospital. The controller further explained that the personal data of the complainant "*were requested as a routine process carried out during a surgery for use of the medical imaging made for the surgical operation. During this process* [redacted] *uses the MRI CD to upload the images during the surgery. However ... originals of the records were retained by the hospital in error as they were not handed back to the patient when she was discharged*" [emphasis has been added]. This effectively demonstrates that the original copies of the data were requested by the controller and used for the purpose of performing the surgery and delivering its service to the patient. The fact that the original copies of the records were retained in error does not mean that the controller was not in fact storing the data of the complainant.

10. Accordingly, the Commissioner examined article 4(2) of the Regulation, which defines 'processing' as "*any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as* ***collection****, recording, organisation, structuring,* ***storage****, adaptation or alteration, retrieval, consultation,* ***use****, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction*" [emphasis has been added]. The collection, use and storage of the data are considered to be processing operations within the meaning of article 4(2) of the Regulation. Despite the fact that the data were not generated, prepared or owned by the hospital, the controller processed that data for its own purposes and used its own means to process that data. This leads the Commissioner to establish that the hospital acted in the capacity of a controller pursuant to article 4(7) of the Regulation, and therefore, the hospital shall be responsible for the processing of the data and be able to demonstrate compliance with the provisions of the Regulation pursuant to the principle of accountability as set forth in article 5(2) of the Regulation.

11. The Commissioner strongly emphasises that personal data, in particular, data in relation to health, which is considered to be a special category of personal data pursuant to article 9(1) of the Regulation deserve heightened protection due to the level of sensitivity of the data processed. Given that the core activities of the controller consist of processing operations, which, by virtue of their nature and purposes, require processing of special categories of personal data on a large scale, the controller is obliged to ensure that the data are safeguarded against risks at all times regardless of the place where the data are stored.

12. For the purpose of this legal analysis, the Commissioner sought to establish whether the controller had the appropriate security measures in place to ensure the ongoing availability and confidentiality of the personal data. Whereas the controller is arguing that this is not a confidentiality breach, the Commissioner was not presented with any sufficient evidence to completely exclude the possibility that this case is not also a confidentiality breach. The controller is assuming that if an individual received incorrect data pertaining to a third party, that individual would supposedly return the data or inform the controller. However, this is a mere assumption of the controller, which is not supported by any evidence. Given that the controller did not manage to locate the data of the complainant by the time of the issuance of this decision, the Commissioner could not ascertain that this incident did not effectively materialise in a confidentiality breach.

13. Pursuant to article 32(1)(b) of the Regulation, the controller shall implement the appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including *inter alia* the ability to ensure the ongoing availability and confidentiality of the data. Article 32(2) of the Regulation further provides that the controller shall in assessing the appropriate level of security, take into account the risks that are presented by the processing of a special category of personal data, in particular from loss.

14. The internal investigation conducted by the controller revealed that the data were misplaced after being removed from the medical records room and handed to reception for collection. The envelope with the medical records of the complainant were inadvertently placed in a box folder. Furthermore, the controller stated that the data were handed to the reception attendants despite the fact that "*storing such records is not part of the responsibilities and capacity of the attendants of reception*".

15. The controller recognised its shortcomings in the manner how it handled the personal data of the complainant, particularly, that the data were not kept in a secure manner and it had no proper access control when the data were moved from the medical records room. As stated by the controller in its submissions, it is not the task of the reception attendant to store health data of patients. Given the nature and sensitivity of the data that is processed by the controller on a daily basis, the Commissioner strongly emphasises that health data should not be handled by reception attendants or left in the reception area. Whereas it has been noted that it is the normal procedure of the controller to hand over the data to the patients upon their discharge, there may be instances where this does not happen, such as in the present case. In this regard, the controller should have in place the appropriate procedure to handle these situations where data may need to be collected by the data subjects at a later time. The Commissioner recommends that the health data should be kept secure in the medical records room and only moved when the patient calls in at the reception to collect the data. An employee from the department of the medical records should personally hand over the data to the patient in order to ensure that the data is safeguarded against risks at all times.

On the basis of the foregoing considerations, the Commissioner is deciding that the controller did not implement the appropriate security measures in order to ensure a level of security appropriate to the risk at the time of the incident, which consequently led to an infringement of article 32(1)(b) of the Regulation.

By virtue of article 58(2)(b) of the Regulation, the controller is served with a reprimand and warned that in the event of similar infringement, the appropriate enforcement action shall be taken accordingly.

Pursuant to article 58(2)(d) of the Regulation, the controller is hereby being ordered to implement the appropriate measures to prevent the reoccurrence of a similar incident. The controller shall comply with this order within a period of one (1) month from receipt of this decision and inform the Commissioner immediately thereafter of the action taken, supported by evidence to demonstrate compliance.

Furthermore, the controller shall ensure that personal data are strictly handled by individuals who are aware of the risks resulting from the processing operations of the hospital. The controller is also reminded that employees who are responsible for handling personal data should be provided with ongoing data protection training.

Ian DEGUARA (Authentication)

Digitally signed by Ian DEGUARA (Authentication)
Date: 2024.02.02 10:00:17 +01'00'

Ian Deguara
Information and Data Protection Commissioner

Right of Appeal

The parties are hereby being informed that 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 to the Information and Data Protection Appeals Tribunal within twenty (20) days from the service of the said decision as provided in article 23 thereof.

An appeal to the Tribunal shall be made in writing and addressed to The Secretary, Information and Data Protection Appeals Tribunal, 158, Merchants Street, Valletta.