PERSONAL DATA PROTECTION COMMISSION

[2024] SGPDPCS 5

Case No. DP-2405-C2321

In the matter of an investigation under section 50(1) of the Personal Data Protection Act 2012

And

HMI Institute of Health Science Pte. Ltd.

… Organisation

DECISION

Data Protection *– Protection obligation – Unauthorised disclosure of personal data – Insufficient administrative security arrangements – Failure to exercise reasonable oversight over vendor*

SUMMARY OF THE DECISION

1 HMI Institute of Health Science Pte. Ltd. (the "**Organisation**") is a healthcare training provider in Singapore. On 2 May 2024, the Organisation notified the Personal Data Protection Commission (the "**Commission**") of a personal data breach incident after it received a complaint from an affected individual who found an Excel file containing the personal data of 761 individuals which the Organisation had inadvertently made publicly available on the Internet (the "**Incident**").

2 The personal data disclosed included a combination of the name, address, email address, telephone number, NRIC number, date of birth, nationality, race, gender and educational qualification.

3 The Organisation requested, and the Commission agreed, for the investigation to proceed under the Expedited Decision Procedure. To this end, the Organisation voluntarily and unequivocally admitted to the facts set out in this decision. It also admitted to a breach of the Protection Obligation under Section 24 of the Personal Data Protection Act 2012 ("**PDPA**").

Facts of the Case

4 Investigations revealed that the affected individuals had provided their personal data to the Organisation via the Students' Career Portal (the "**Portal**"), which was previously part of the Organisation's website from 2017 to 2019. In December 2019,

the Organisation decided to decommission the Portal. Investigations revealed that the Organisation did not follow up with the vendor to ensure that the Portal had been properly decommissioned, other than checking and confirming that the Portal was no longer accessible at its original URL address.

5 The Excel file continued to reside in the web directory of the Organisation's website with no access control to prevent indexing by online search engines. This led to the Excel file being indexed and made publicly accessible via an online search using relevant keywords.

Remedial Action

6 Following the Incident, the Organisation promptly took the following remedial actions:

(a) Removed the Excel file in its web directory;

(b) Liaised with internet search engines to ensure that all web links to the Excel file had been removed;

(c) Implemented an internal checklist for all future commissioning, onboarding and decommissioning of IT solutions; and

(d) Established additional protocols to monitor its website content.

Findings and Basis for Determination

Whether the Organisation had contravened the Protection Obligation

7 Under section 24(a) of the PDPA, organisations must protect personal data in its possession or under its control by making reasonable security arrangements to

prevent unauthorised access, collection, use, disclosure, copying, modification or disposal, or similar risks.

8 The Organisation admitted to a breach of section 24 of the PDPA as it did not have adequate policies and processes to exercise reasonable oversight over the vendor tasked with decommissioning the Portal. While the Organisation alluded to its own lack of technical expertise and reliance on the vendor to decommission the Portal, the Organisation's lack of technical expertise is not an adequate defence to the Organisation's failure to take the necessary steps in order to comply with its obligation under section 24 of the PDPA.

9 The Commission noted that in this case, the exercise of reasonable vendor oversight did not require technical expertise. The Organisation could have exercised reasonable oversight by verifying with its vendor that the personal data previously collected by the Organisation via the Portal had been properly deleted and was no longer accessible following the decommissioning of the Portal. However, the Organisation did not have the policies and processes in place to allow it to adequately supervise the work carried out by its vendor.

10 For the above reasons, the Organisation was determined to have breached the Protection Obligation.

The Deputy Commissioner's Decision

Financial Penalty

11 In determining whether the Organisation should be required to pay a financial penalty under Section 48J of the PDPA, the Commission considered all relevant factors listed at Section 48J(6) of the PDPA, in particular, the impact of the personal data breach on the individuals affected, the duration of and the nature of the Organisation's non-compliance with the PDPA.

12 The Commission also considered the fact this is the second contravention of the PDPA by the Organisation.

13 The Commission considered the following mitigating factors:

(a) The Organisation was cooperative during the course of our investigations; and

(b) The Organisation voluntarily admitted to breach of the Protection Obligation under the Commission's Expedited Decision Procedure.

14 For the reasons above, the Commission hereby requires the Organisation to pay a financial penalty of $10,000 within 30 days from the date of the relevant notices accompanying this decision, failing which interest at the rate specified in the Rules of Court in respect of judgment debts shall accrue and be payable on the outstanding amount of such financial penalty until the financial penalty is paid in full.

Directions

15 In addition, to ensure the Organisation's compliance with the Protection Obligation, the Organisation is directed to report to the Commission on the completion of the following remedial actions:

(a) Create and maintain a personal data asset inventory for tracking of its personal data assets;

(b) Put in place a well-documented vendor management policy and relevant processes for effective management and supervision of its IT vendors;

(c) Conduct a vulnerability assessment and/or penetration testing of its existing IT systems and to resolve any identified vulnerabilities; and

(d) Prepare and submit to the Commission a written report of the completion of the remediation actions directed above within 60 days from the date of the relevant notices accompanying this decision.

WONG HUIWEN DENISE
DEPUTY COMMISSIONER
FOR PERSONAL DATA PROTECTION

The following section(s) of the Personal Data Protection Act 2012 had been cited in the above summary:

Protection of personal data

24. An organisation shall protect personal data in its possession or under its control by making reasonable security arrangements to prevent –

(a) unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks; and

(b) the loss of any storage medium or device on which personal data is stored.