MDIS Corporation Pte Ltd

[2020] SGPDPC 11

Tan Kiat How, Commissioner — Case No DP-1905-B3832

Data Protection – Protection obligation – Unauthorised access to and disclosure of personal data – Insufficient security arrangements

17 March 2020

Introduction

1 On 2 May and 17 June 2019, the Personal Data Protection Commission (the "**Commission**") received two complaints from an individual (the "**Complainant**") in relation to a Microsoft Excel spreadsheet (the "**Spreadsheet**") containing personal data of individuals who had signed up for courses with MDIS Corporation Pte Ltd (the "**Organisation**"). The Complainant was able to access the Spreadsheet through a Google search of her NRIC number on 2 May and 17 June 2019 (the "**First Incident**" and "**Second Incident**" respectively).

Facts of the Case

2 The Organisation is a not-for-profit, professional institute for lifelong learning. The Organisation's server and webpage were maintained by a web

development vendor (the "**Vendor**"). In October 2017, the Organisation engaged the Vendor to develop its website (the "**Website**") to include a content management system ("**CMS**") for the Organisation to manage training and courses provided, and an online registration form (the "**Form**") for course participants to provide their personal data. The purpose of the Form was for the Organisation to use the personal data collected to identify course attendees, create certificates for individuals who had completed their courses and verify their details for the purposes of claiming SkillsFuture credits. The Vendor subsequently engaged a freelance developer based in India (the "**Developer**") to assist in developing the Website.

3 There were no written contracts between (i) the Organisation and the Vendor; and (ii) the Vendor and the Developer setting out the parties' respective scope of work and responsibilities with respect to the development of the Website. During development of the Website, the Organisation conveyed its instructions for the Website via telephone to the Vendor, and the Vendor acted as the middleman between the Organisation and the Developer. From time to time, the Organisation would also contact the Developer directly.

4 In December 2017, the Organisation and the Vendor carried out pre-launch testing on the Website (including the Form). In September 2018, the Organisation approved the Website for launch and the Website went "live"

shortly after. Between September 2018 and February 2019, the Vendor assisted to rectify various features on the Website that were not developed to the Organisation's expectations. The Organisation terminated the Vendor's engagement in or around February 2019 as it was not satisfied with the Vendor's service.

5 The First Incident occurred on 2 May 2019 when the Complainant entered her NRIC number into a Google search. The search result was a URL link displaying partial information about the Complainant, including NRIC number, email address and mobile phone number (the "**Spreadsheet Link**"). The Complainant clicked on the Spreadsheet Link which led to the Spreadsheet containing the following information of 304 individuals including the Complainant's (the "**Disclosed Data**"):

(a) Name;

(b) Designation;

(c) Citizenship;

(d) NRIC number / identification number (for foreigners);

(e) Email address;

(f) Name of Company name that the individual worked for;

(g) Registration type;

(h) Contact number;

(i) Billing address;

(j) Country;

(k) Contact person; and

(l) Course title, course code and date.

6 On the same day, the Complainant notified the Commission and the Organisation about the First Incident. The Organisation promptly took the following remedial actions:

(a) Blocked the CMS administrative backend;

(b) Inserted a "*robot.txt*" file to prevent search engines from crawling the Website; and

(c) Submitted a removal request to Google to ensure cached versions of Spreadsheet Link would be removed from search results.

7 In addition, as part of the Organisation's investigations, it periodically removed the blockage on the CMS administrative backend to test and replicate the First Incident.

8 The Second Incident occurred on 17 June 2019 when the Complainant entered her NRIC number into a Google search and was again able to access the Spreadsheet Link and Spreadsheet. According to the Organisation, the Second Incident occurred because the Complainant carried out the Google search of her NRIC number at the same time that the Organisation had removed the blockage on the CMS administrative backend to conduct tests on the First Incident.

9 As of 19 June 2019, the Organisation's newly appointed vendor deployed security patches on the Website and removed the codes that caused the First Incident and Second Incident. As part of the Organisation's remedial actions, a new backend system for the Website will also be deployed.

The Commissioner's Findings and Basis for Determination

10 As a preliminary point, the Organisation owned the Website and was in possession and control of the Disclosed Data (collected through the Form) at all material times. While the Vendor and the Developer were engaged to develop the Website, the Organisation confirmed that neither of them processed the Disclosed Data on the Organisation's behalf. Both the Vendor and Developer were accordingly not data intermediaries, and the responsibility to protect the Disclosed Data fell squarely and solely on the Organisation.

11 Section 24 of the PDPA requires an organisation to protect personal data in its possession or under its control by taking reasonable steps or arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks. The Organisation failed to put in place reasonable security arrangements to protect the Disclosed Data for the reasons explained below.

12 First, the Organisation failed to communicate any data protection requirements to the Vendor or the Developer.

(a) The Organisation conceded that it did not have a written contract with the Vendor in relation to the development of the Website. There was also no written contract between the Vendor and Developer. As emphasized in previous decisions and the Commission's Guide on Building Websites for SMEs (revised 10 July 2018) at [4.2.1], organisations that engage IT vendors to develop and/or maintain their websites should ensure that their IT vendors are aware of the need for personal data protection by making it part of their contractual terms.[1]

(b) According to the Organisation, it had verbally communicated data protection requirements to the Vendor and Developer. In contrast,

[1] See for example *Re EU Holidays Pte Ltd* [2019] SGPDPC 38 at [11].

the Vendor asserted that there was no such communication. As the data controller and customer, the Organisation ought to be clear about the scope of services that it is procuring from its service providers, and document the scope properly in contract and other project documentation.[2] In this case, the Organisation was not able to produce anything in writing to corroborate its assertions. In the circumstances, the Commissioner finds that the Organisation failed to communicate data protection requirements to the Vendor and Developer.

(c) Given that one of the purposes of developing the Website was to collect Disclosed Data through the Form, the Organisation's failure to specify clear requirements with respect to the protection of personal data is particularly glaring.

13 Second, prior to the launch of the Website, the Organisation failed to take reasonable steps to scope the pre-launch testing to discover risks to the Disclosed Data that was collected through the Form. As a result, the vulnerability in the CMS administrative backend of the Website (which allowed Google to crawl and index the Spreadsheet Link) remained undetected prior to the First Incident.

---

[2] *Re Royal Carribean Cruises (Asia) Pte Ltd* [2020] SGPDPC 5 at [12]

(a) Websites connected to the Internet are subject to a multitude of cyber threats that may compromise the website and expose any personal data collected. The Commissioner takes this opportunity to reiterate that organisations should ensure protection of personal data and the security of the website is a key design consideration at each stage of the website's life cycle, including requirements gathering, design and development, UAT, deployment and operations support.[3]

(b) The Commission's investigations revealed that the pre-launch testing conducted prior to launch of the Website focused on its functionality. According to the Organisation, it believed that the password protection to the administrative panel was "*secure enough*". In this regard, the Organisation admitted that it did not inform the Vendor of the requirement to secure personal data collected through the Form.

(c) The omission to include security testing prior to the launch of the Website is particularly concerning given that:

[3] See Commission's *Guide on Building Websites for SMEs* (revised 10 July 2018) at [3.2 – 3.3] and *Re Horizon Horizon Fast Ferry Pte. Ltd.* [2019] SGPDPC 27 at [26]

(i) The purpose of the Form was to collect Disclosed Data from individuals participating in the Organisation's courses; and

(ii) The Organisation knew that the administrative panel had an export function which collated the Disclosed Data (entered by course participants in the Form) into the Spreadsheet. The export function could be triggered either by clicking on the export button in the administrative panel or by clicking on the Spreadsheet Link. The Spreadsheet link was not intended to be publicly available and should have only been accessible with valid login credentials.

(d) In the circumstances, the Organisation should have scoped the pre-launch testing to verify that password protection measures on the administrative panel and the login credentials on the Spreadsheet Link operated as intended.

14 During the course of the Commission's investigations, the Organisation asserted that it was not an IT services provider, and therefore had relied on its Vendor to identify the risks and implement the appropriate security measures for the Website. This is not an acceptable explanation. It should be reiterated that while organisations may delegate work to vendors to comply with the PDPA, the organisation's responsibility for complying with statutory

obligations under the PDPA may not be delegated.[4] While an organisation may not have — or need to have — the requisite level of technical expertise, a responsible organisation would have engaged competent service providers and made genuine attempts to give proper instructions.[5] The Organisation is only expected to articulate its business requirements as owner of the system, which the service provider can translate into technical requirements. In addition, as the data controller, the Organisation is required to exercise reasonable oversight to ensure that its instructions are carried out.[6] In this case, and as mentioned at [12], the Organisation failed to provide any data protection instructions to either the Vendor or the Developer. The Commission's investigations also revealed that the Organisation did not exercise reasonable oversight in respect of the security arrangements for the Website.

15 For the reasons above, the Commissioner finds the Organisation in breach of section 24 of the PDPA.

---

[4] *Re WTS Automotive Services Pte. Ltd.* [2018] SGPDPC 26 at 23; *Re National Healthcare Group* [2019] SGPDPC 46 at [17]

[5] *Re WTS Automotive Services Pte Ltd* [2018] SGPDPC 26 at [24]; *Re DS Human Resource Pte. Ltd*. [2019] SGPDPC 16 at [15].

[6] *Re Smiling Orchid (S) Pte Ltd and others* [2016] SGPDPC 19 at [51]

The Commissioner's Directions

16 In determining the directions, if any, to be imposed on the Organisation under Section 29 of the PDPA, the Commissioner took into account the following mitigating factors:

(a) The Organisation was cooperative in the course of the Commission's investigations and provided prompt responses to the Commission's requests for information;

(b) The Organisation implemented prompt remedial actions; and

(c) The unauthorised disclosure of the Disclosed Data was only to the Complainant.

17 The Commissioner also took into account, as an aggravating factor, that the Disclosed Data was exposed to the risk of unauthorised disclosure for a period of approximately 6 months.[7]

18 Having considered all the relevant factors of this case, the Commissioner hereby directs the Organisation to pay a financial penalty of S$10,000 within 30 days from the date of this direction, failing which interest, at the rate

[7] The approximate period of 6 months was between November 2018 (when individuals started signing up for courses on the Website using the Form) and June 2019 (when security patches were deployed to fix the vulnerabilities on the Website).

specified in the Rules of Court in respect of judgment debts shall accrue and be payable on the outstanding amount of the financial penalty until it is paid in full.

19 The Commissioner has not set out any further directions given the remediation measures already put in place.
