SCAL Academy Pte. Ltd.

[2020] SGPDPC 2

Tan Kiat How, Commissioner — Case No. DP-1811-B3061

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

8 January 2020

Introduction

1 SCAL Academy Pte. Ltd. (the **"Organisation**") provides courses, seminars and workshops for individuals (the "**Participants**") and collects personal data of Participants through its website, http://www.scal-academy.com.sg (the "**Website**"), for registration purposes. The Website was developed and maintained by a freelance vendor (the **"Vendor"**).

2 On 29 November 2018, the Personal Data Protection Commission (the "**Commission**") received a complaint that the results of an online search of the names of Participants displayed links to scanned copies of registration documents (the "**Documents**") on the Website (the "**Incident**"). The Documents were accessible by clicking on the listed links.

3 The Documents contained various personal data of 3,628 Participants including their name, race, nationality, date of birth, gender, country of birth, NRIC or work permit number, address, occupation and the name of the company the Participants were employed by (the "**Compromised Personal Data**").

4 The cause of the Incident was traced to an enhancement to the Website (the "**Enhancement**") which allowed Participants to upload the Documents directly onto a folder (the "**Folder**") on the Website. The Vendor had been tasked with developing the Enhancement on 7 February 2018 and, in the course of doing so, the Vendor omitted to programme the Enhancement to verify that only authorised employees can access the Folder. The Documents were thus accessible without the need for login credentials. Additionally, the Vendor had also, through an oversight, omitted to implement another requirement, which is to implement Google's recommendations to prevent bot crawlers from searching and indexing website content.

5 Following the Incident, the Organisation took the following remedial actions:

(a) Implemented measures to prevent Google trawling and indexing, such as deploying 'noindex' tags and scripts to ignore search bots;

(b) Requested Google to remove search engine records of the production environment and the links to the Documents;

(c) Removed the Documents from the Website;

(d) Disabled the upload function for Documents for online registration on the Website; and

(e) Assessed the harm and impact of the Incident on the affected individuals and notified approximately 27 of them who the Organisation believed would likely suffer significant harm or impact.

Findings and Basis for Determination

Whether the Organisation had contravened section 24 of the Personal Data Protection Act 2012 ("PDPA")

6 As a preliminary point, the Organisation owned and managed the Website, and had possession and control over the Compromised Personal Data at all material times. While the Vendor had been engaged to develop and maintain the Website and

subsequently assisted in the development of the Enhancement, the Vendor had not processed any personal data collected via the Website on the Organisation's behalf. The Vendor was therefore not a data intermediary of the Organisation, and the obligations under the PDPA did not apply to the Vendor in respect of its engagement by the Organisation.

7 Section 24 of the PDPA requires an organisation to protect personal data in its possession or under its control by taking reasonable security steps or arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks.

8 In this regard, while the Organisation had instructed the Vendor to prevent the Documents from being 'leaked' online, it did not check with the Vendor what security arrangements had been put in place to ensure this. It is essential that, having identified a data protection risk, the Organisation and the Vendor agree on the measures to be implemented. These can then be followed through to the testing stage and scenarios can also be devised for user acceptance testing. Since this was not done, it therefore follows that the Organisation did not conduct any tests, or verify whether the Vendor had conducted any tests, to ensure that the security arrangements were effective in protecting the Documents from unauthorised disclosure.

9 As observed in *WTS Automotive Services Pte Ltd* [2018] SGPDPC 26 at [24], the responsibilities of an organisation over the personal data in its control and/or possession does not require technical expertise. The examples of actions that the Organisation ought to have undertaken as set out at paragraph 8 above do not require deep technical expertise. Instead, it requires that organisations articulate their business requirements, work with their vendors on a set of agreed technical measures, and to follow through with proper testing based on risk scenarios derived from the business requirements.

10 In view of the above, the Commissioner found that the Organisation had not put in place reasonable security arrangements to protect the personal data in the Documents and, accordingly, was in breach of section 24 of the PDPA.

The Organisation's Representations

11 In the course of settling this Decision, the Organisation submitted its representations to the Commission on various aspects of the preliminary Decision. The representations, in part, covered matters which have already been addressed in this Decision or which were not relevant to this Decision. The relevant matters raised in the representations which are not addressed elsewhere in this Decision were:

(a) The Organisation warned the Vendor that the Incident was a breach of the PDPA;

(b) While not justifying the data breach, the Organisation took the position that the Incident neither impacted nor caused significant harm to the affected individuals;

(c) The Organisation has since taken steps to prevent a recurrence of a similar incident such as strengthening and improving communication with suppliers and vendors especially where personal data is concerned and educating members on compliance with the PDPA; and

(d) The Organisation counselled the Vendor and obtained an undertaking requiring the Vendor to implement additional safeguards, such as, disabling all UAT websites from being searchable by search engines, educating staff members on the PDPA and communicating and collaborating with the Organisation to ensure that work done complies with the PDPA.

12 With respect to the matter raised at [11(a)], as stated at [6], the Vendor was not a data intermediary for the purpose of its engagement by the Organisation. Nevertheless, informing the Vendor of the Incident and that the PDPA had been breached is a legitimate remedial action. This has already been taken into consideration in determining the directions to be issued to the Organisation, as set out below at [15(b)].

13 With respect to [11(b)], this should be seen in light of the Organisation having, as part of its remedial efforts, notified affected individuals who it believed would likely suffer significant harm or impact. Looking at the Organisation's assertions, it is the Organisation's own view that 27 individuals were likely to have suffered significant harm or impact and mitigated this harm or impact by notifying these individuals. Again, this remedial action had already been taken into consideration when determining the appropriate directions to be issued.

14 With respect to the additional matters raised and as set out at [11(c) and (d)], the Commissioner accepts these points and the financial penalty imposed has been reduced to the amount stated below.

The Commissioner's Directions

15 In determining the directions 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 investigations and provided information promptly; and

(b) Upon being notified of the Incident, the Organisation swiftly took remedial actions.

16 Having considered all the relevant factors of this case, the Commissioner hereby directs the Organisation to pay a financial penalty of $15,000 within 30 days from the date of the directions, 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.

17 In light of the remedial actions taken by the Organisation, the Commissioner has decided not to issue any further directions.
