Society of Tourist Guides (Singapore)

[2019] SGPDPC 48

Tan Kiat How, Commissioner — Case No. DP-1903-B3445

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

Data Protection – Accountability obligation – Lack of data protection policies and practices

Data Protection – Accountability obligation –Failure to appoint data protection officer

26 December 2019

Introduction

1 On 3 March 2019, the Personal Data Protection Commission (the "**Commission**") received a complaint that personal data of individuals had apparently been exposed to unauthorised access and disclosure through links on the Society of Tourist Guides (Singapore)'s (the "**Organisation**") website.

Facts of the Case

2 The Organisation is a non-profit organisation that works with the Singapore Tourism Board ("**STB**") to promote the professionalism of tourist guides as tourism ambassadors of Singapore. Tourist guides registered with STB may sign up as members of the Organisation

("**Members**"). In May 2018, the Organisation engaged a Vietnam-based IT company (the "**Vendor**") to develop its website https://societyoftouristguides.org.sg (the "**Website**").

3 One of the Organisation's purposes for the Website was to collect personal data from its Members. Personal data was collected from Members through their respective user accounts on the Website and included their names, photographs, contact numbers, e-mail addresses and a write-up of themselves (for example, with the type of services they provided) ("**Profile Data**"). Members could also upload images of their identification documents (e.g. NRIC, employment pass, driving and vocational licences) which contained various personal data ("**ID Data**").

4 Members' Profile Data were published on their respective public profile pages on the Website. This enabled members of the public to find and engage a Member with the necessary experience and expertise to provide services that he or she required.

5 As regards the ID Data, these were used by the Organisation for a few purposes. These included (i) applying for SkillsFuture grants for training programmes conducted for Members; (ii) facilitating arrangements for Members to gain access to secure locations when required (e.g. transit areas in airports); and (iii) verifying that the Members were qualified to provide transport services based on his or her driving and vocational licences.

6 The Organisation did not specify any requirements to its Vendor with respect to the storage and protection of Members' personal data collected through the Website. The Website

was launched on 1 October 2018. Since its launch, the Organisation has been managing the Website, with the Vendor's role limited to ad-hoc technical assistance.

7 On 3 March 2019, the Commission received a complaint that there had been disclosure without consent of sensitive information of individuals, such as Singapore National Registration Identity Card ("**NRIC**"), Driving Licence and photographs, through links on the Website (the "**Incident**"). The Commission's investigations revealed that a total of 111 unique Members were affected by the Incident (the "**Affected Members**")[1]. In this regard, the publicly accessible directories on the Website ("**Web Directories**") were found to store images of identification documents set out below which contained ID Data of the Affected Members (the "**Disclosed Data**"):

S/N.	Type of Identification Document	Type of Personal Data in the Identification Document	Number of Members Affected
1.	Singapore National Registration Identity Card ("**NRIC**")	Name, NRIC number, photograph, thumbprint, address, date of birth, country of birth, race, gender and date of issue.	97
2.	Singapore Armed Forces Identity Card	Name, NRIC number/colour, photograph, address, date of birth, country of birth, race, gender, blood group, service status and military rank status.	1
3.	Vietnamese Identity Card	Name, card number, photograph, date of birth, place of birth, place of residence, fingerprints, ethnic group, religion and date of issue.	1

[1] A Member could have uploaded images of more than one type of identification document on the Website.

4.	Singapore Employment Pass	Name, photograph, occupation, Foreign Identification Number, date of application, date of issue, date of expiry and employer.	1
5.	Singapore Driving Licence	Name, licence number (same as NRIC number), photograph, date of birth, classes of vehicles the individual is licensed to drive and each pass date and date of issue.	47
6.	Singapore Vocational Licence	Name, licence number (same as NRIC number), photograph, date of issue and type and description of each vocational licence held, and their respective dates of issue.	16

8 It also emerged in the course of the Commission's investigations that the Organisation had not appointed any data protection officer ("**DPO**"), and had not developed and put in place any data protection policies that are necessary for it to meet its obligations under the Personal Data Protection Act 2012 (the "**PDPA**").

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

(a) Appointed two DPOs;

(b) With the assistance of its Vendor, disabled public access to the Web Directories and contacted Google to remove all cached images of the Disclosed Data; and

(c) Developed a data protection policy.

Findings and Basis for Determination

Whether the Organisation had contravened section 24 of the PDPA

10 As a preliminary point, the Organisation owned and managed the Website, and had possession and control over the Disclosed Data at all material times. While the Vendor had been engaged to develop the Website and subsequently provided technical assistance on an ad-hoc basis, 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 Organisation was solely responsible for the protection of the Disclosed Data under the PDPA.

11 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.

12 In this regard, the Commissioner found that the Organisation had failed to put in place reasonable security arrangements to protect the Disclosed Data for the following reasons. First, as mentioned at [6], the Organisation did not specify any requirements to its Vendor with respect to the storage and protection of personal data (including the ID Data) which was collected from Members through the Website. The Organisation had intended for the Website to have public profile pages for which Members' Profile Data were displayed for public access, but at the same time ID Data was collected and to be used for administrative purposes like applying for training grants, facilitating access to secure location and verifying driving qualifications. Clear requirements could and should have been communicated to its Vendor

that ID Data collected through the Website was not meant to be publicly accessible. This can be done by the Organisation from the perspective of the business owner of the Website, while relying on the Vendor to propose the technical implementation that will meet this business requirement.

13 The Commission's investigations also revealed that security testing had never been conducted since the launch of the Website in October 2018. In this regard, the Organisation admitted that it failed to take into consideration the security arrangements of the Website due to its lack of experience. As observed in *WTS Automotive Services Pte Ltd* [2018] SGPDPC 26 at [24], while an organisation may not have the requisite level of technical expertise, a responsible organisation would have made genuine attempts to give proper instructions to its service providers. The gravamen in the present case was the Organisation's failure to do so.

14 The Commission's Guide on Building Websites for SMEs (revised 10 July 2018) provides guidance on what is expected from organisations contracting professional services to build their corporate websites or other online portals. In particular, organisations that engage IT vendors to develop and/or maintain their websites should emphasize the need for personal data protection to their IT vendors, by making it part of their contractual terms.[2]

15 Secondly, and as observed in *Re Tutor City* [2019] SGPDPC 5 at [21] to [23], where documents containing personal data have to reside on web servers, folder or directory permissions are common and direct methods of controlling access and preventing unauthorised access by public users and web crawlers. Depending on its business needs and circumstances,

[2] Guide on Building Websites for SMEs (revised 10 July 2018) at [4.2.1]

the Organisation could have instructed the Vendor to implement any of the following reasonable technical security measures to protect the Disclosed ID Images:

(a) place documents containing the Disclosed ID Images in a non-public folder/directory.

(b) place documents containing the Disclosed ID Images in a non-public folder or directory, with access to these documents controlled through web applications on the server.

(c) place documents containing the Disclosed ID Images in a sub-folder within the Public Directory but control access to files by creating a .htaccess file within that sub-folder. This .htaccess file may specify the access restrictions (*e.g.* implement a password requirement or an IP address restriction).

16 In view of the above, the Commissioner found that the Organisation had contravened section 24 of the PDPA.

Whether the Organisation was in breach of sections 11(3) and 12 of the PDPA

17 In relation to the Organisation's failure to appoint a DPO and develop and implement any data protection policy, these are required under sections 11(3) and 12 respectively of the PDPA. In particular, section 11(3) requires organisations to designate one or more individuals (typically referred to as a DPO) to be responsible for ensuring that they comply with the PDPA. Section 12 of the PDPA requires organisations to (among other things):

(a) develop and implement policies and practices that are necessary for the organisation to meet the obligations of the organisation under the PDPA; and

(b) communicate information about such policies to its staff.

18 The importance of these requirements have been emphasised multiple times in previous decisions. For example, it is important for an organisation to documents its data protection policies and practices in writing as they serve to increase awareness and ensure accountability of the organisation's obligations under the PDPA (*Re Aviva Ltd* [2017] SGPDPC 14 at [32]). Similarly, appointing a DPO is important in ensuring the proper implementation of an organisation's data protection policies and practices, as well as compliance with the PDPA (see *e.g. Re M Stars Movers & Logistics Specialist Pte Ltd* [2017] SGPDPC 15 at [31] to [37]).

19 In the circumstances, the Organisation was clearly in breach of sections 11(3) and 12 of the PDPA. While it has since appointed DPOs, it has not yet developed written policies and practices necessary to ensure its compliance with the PDPA.

Representations by the Organisation

20 In the course of settling this decision, the Organisation made representations on the amount of financial penalty which the Commissioner intended to impose, and requested that the financial penalty be paid in instalments. The Organisation raised the following factors for the Commissioner's consideration:

(a) The Organisation had limited funds in its bank account and does not have any tangible assets which may be sold to raise funds to pay the financial penalty;

(b) The Organisation had been making losses in the preceding 3 months; and

(c) The Organisation has been seeking funding assistance from the Singapore Tourism Board.

21 Having carefully considered the representations, the Commissioner has decided to maintain the financial penalty set out in [23(a)]. The matters raised by the Organisation in [20] are not additional mitigating factors that justify a reduction in the financial penalty. However, the Commissioner is agreeable to the Organisation's request that the financial penalty be paid in instalments.

The Commissioner's Directions

22 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 investigations and provided information promptly;

(b) Upon being notified of the Incident, the Organisation took action to disable public access to the Web Directories, and notified its Members of the Incident; and

(c) There was limited unauthorised access and disclosure of the Disclosed ID Images as the Web Directories had only been accessed a total of 6 times.

23 Having considered all the relevant factors of this case, the Commissioner hereby directs the Organisation to:

(a) Pay a financial penalty of $20,000 in 8 instalments by the due dates as set out below, failing which, the full outstanding amount shall become due and payable

immediately and 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:

(i) 1st instalment of $2,500 on 1 February 2020;

(ii) 2nd instalment of $2,500 on 1 March 2020;

(iii) 3rd instalment of $2,500 on 1 April 2020;

(iv) 4th instalment of $2,500 on 1 May 2020;

(v) 5th instalment of $2,500 on 1 June 2020;

(vi) 6th instalment of $2,500 on 1 July 2020;

(vii) 7th instalment of $2,500 on 1 August 2020; and

(viii) 8th instalment of $2,500 on 1 September 2020.

(b) Complete the following within 60 days from the date of this direction:

(i) Review the security of the Website and implement appropriate security arrangements to protect the personal data in its possession or control;

(ii) Put in place written internal policies and practices as required under section 12 of the PDPA;

(iii) Develop and implement a training policy for employees of the Organisation handling personal data to be trained to be aware of, and to comply with the requirements of, the PDPA when handling personal data; and

(iv) Require all existing employees to attend such training.
