EU Holidays Pte. Ltd.

[2019] SGPDPC 38

Tan Kiat How, Commissioner — Case No DP-1901-B3254

Data Protection – Protection obligation – Unauthorised disclosure of personal data

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

4 October 2019

Introduction

1 On 14 January 2019, the Personal Data Protection Commission (the "**Commission**") received a complaint that personal data of EU Holidays Pte. Ltd.'s (the "**Organisation**") customers was accessible through its website (the "**Incident**").

Facts of the Case

2 Pursuant to a Quotation of Services dated 16 May 2017 ("**Contract**"), the Organisation engaged an IT vendor (the "**Vendor**") to develop a new website with e-commerce capabilities (the "**Website**"). One of the purposes of the Website was to allow the Organisation's customers ("**Customers**") to make online reservations for tour packages either directly or through the Organisation's partner agents. Information relating to travel reservations received from Customers were stored in 2 web directories. For reservations made directly by Customers on the Website, the tax invoice generated would be stored in a web directory ("**Web Directory 1**"). As for reservations made through the Organisation's partner agents on the Website, the tax invoice generated would be stored in another web directory ("**Web Directory 2**").

3 The scope of work in the Contract did not specify any requirements with respect to the storage and protection of Customers' personal data which was collected through the Website. The Website was launched on 9 December 2017. Since its launch, the Organisation has been managing the Website, with the Vendor's role limited to maintenance and technical troubleshooting.

4 On or around 5 January 2019, a member of the public ("**Complainant**") discovered copies of tax invoices containing Customers' personal information while browsing for tour packages on the Website. The Complainant notified the Commission of the Incident on 14 January 2019.

5 Based on the Organisation's internal records, from 9 December 2017 to 14 January 2019, tax invoices containing information of 1,077 Customers were exposed to unauthorised access and disclosure through links to Web Directory 1 and Web Directory 2.[1] The information contained in the invoices include the following personal data (collectively, the "**Disclosed Personal Data**"):

(a) Name;

(b) Email address;

(c) Address;

(d) Contact number;

(e) Booking date;

(f) Travel destination;

(g) Departure date;

(h) Gender;

(i) Date of birth;

(j) Passport details (including number, date of issue and expiry);

(k) Rooming arrangement (i.e. whether travellers are adults / children and the type of beds required); and

(l) Amount payable.

[1] Specifically, the information of 336 Customers were stored in Directory 1 and the information of 741 Customers were stored in Directory 2.

6 Upon being notified of the Incident, the Organisation promptly carried out the following remedial actions:

(a) Deleted all tax invoices stored on Web Directory 1; and

(b) Disabled public access to Web Directory 2.

7 Separately, the Commission's investigations revealed that the Organisation had not developed or implemented any internal data protection policies that are necessary for it to meet its obligations under the Personal Data Protection Act 2012 (the "**PDPA**").

Findings and Basis for Determination

Whether the Organisation had contravened section 24 of the PDPA

8 As a preliminary point, the Organisation owned and managed the Website and had possession and control over the Disclosed Personal Data at all material times. While the Vendor had been engaged to develop the Website and subsequently provided maintenance and technical troubleshooting services, the Vendor had not processed the Disclosed Personal Data 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 Personal Data under the PDPA.

9 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. In the Commissioner's view, the Organisation failed to put in place reasonable security arrangements to protect the Disclosed Personal Data as explained below.

10 First, the Organisation failed to assess the risks to the Disclosed Personal Data collected through its Website and stored in Web Directory 1 and Web Directory 2. The investigations revealed that the Organisation had left it to the Vendor to put in place the appropriate security arrangements to protect the Disclosed Personal Data. Consequently, as mentioned at [3], the scope of work in the Contract did not include any requirements with respect to how the Disclosed Personal Data was to be stored or protected. The Organisation also did not review the standard of security of the Website and left it completely to the Vendor. In particular:

(a) In relation to Web Directory 1, prior to the Incident, since the Organisation did not provide any instructions to the Vendor on the storage of tax invoices generated from direct reservations on its Website, it was unaware that such tax invoices were stored in Web Directory 1 which was publicly accessible. In this regard, the Organisation's assertion was that it had intended for these tax invoices to be stored in a backend Content Management System which only authorised staff could log into and access. Its intention was not translated into action.

(b) In relation to Web Directory 2, the Organisation intended for tax invoices generated from reservations through its partner agents to be stored in Web Directory 2, and accessed by partner agents using their respective email addresses and password. The Organisation asserted that did not intend for Web Directory 2 to be publicly accessible. However, since the Organisation did not provide any instructions to the Vendor in relation to access controls for Web Directory 2, none was implemented.

11 What is expected from organisations contracting professional services to build their corporate websites or other online portals is explained in the Commission's Guide on Building Websites for SMEs (revised 10 July 2018). 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] Given that the development of the Website was for the purposes of e-commerce (including the collection of Customers' Disclosed Personal Data in relation to reservations for tour packages), the Organisation's failure to specify clear requirements with respect to the protection of personal data is particularly glaring in this case.

12 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, the Organisation could have instructed the Vendor to implement any of the following reasonable technical security measures to protect the Disclosed Personal Data:

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

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

(b) place documents containing the Disclosed Personal Data 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 Personal Data 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).

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

Whether the Organisation had contravened section 12 of the PDPA

14 Section 12 of the PDPA requires organisations to develop and implement policies and practices that are necessary for the organisation to meet its obligations under the PDPA and communicate information about such policies to its staff.

15 By the nature of its business as a travel agency, the Organisation regularly collects personal data of customers to fulfil reservations for tour packages. Notwithstanding this, the Organisation did not have any internal data protection policies to provide guidance to its employees on the handling of such personal data.

16 In the circumstances, the Commissioner found that the Organisation had contravened section 12 of the PDPA.

The Commissioner's Directions

17 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 took prompt remedial actions following the Incident;

(b) the Organisation was cooperative during the investigations; and

(c) Although the Disclosed Personal Data of 1,077 Customers was at risk of unauthorised access and disclosure, actual disclosure was only to the Complainant in respect of Customers' Disclosed Personal Data in 20 invoices albeit for a period of more than 1 year.

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

(a) 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;

(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 personal data in its possession and/or under its control;

(ii) Put in place a data protection policy, including written internal policies, to comply with the provisions of the PDPA; and

(iii) Develop a training programme for the Organisation's employees in respect of their obligations under the PDPA when handling personal data and require all employees to attend such training

YEONG ZEE KIN
DEPUTY COMMISSIONER
FOR COMMISSIONER FOR PERSONAL DATA PROTECTION