Flight Raja Travels Singapore Pte. Ltd.

[2018] SGPDPC 16

Yeong Zee Kin, Deputy Commissioner — Case No DP-1705-B0730

Data Protection – Protection obligation – Disclosure of personal data – Insufficient security arrangements

11 June 2018.

1 This complaint concerns a user of Flight Raja Travels Singapore Pte. Ltd's (the "**Organisation**") online travel booking system (the "**Booking System**"). While using the Booking System, the user was able to access information of other users (the "**Incident**").

2 What happened was that after the user resumed his session after time-out, the Booking System showed him 45 sets of booking records. The booking records accessed by the user contained the personal data of 72 other individuals. This included name, passport number, booking ID, flight details (including the flight number, departing/ arrival date, time and airport), booking date, amount paid, and flight inclusions.

3 Investigations were commenced under section 50 of the Personal Data Protection Act 2012 (the "**PDPA**"). The material facts of the case are as follows.

4 Up to December 2016, the Booking System was accessed through browser login via the Organisation's website. The Organisation then introduced

a new application (the "**New Mobile App**"). The New Mobile App enabled access through mobile devices without login. It recognised the mobile device IDs of registered users stored as part of their account information.

5 Proper change management would have included full system integration testing of the New Mobile App with the Booking System to detect any unintended effects from the changes. However, two unintended effects went undetected. They affected non-registered users who had just completed a booking via the Booking System through a browser, and had been registered by the Booking System as new users ("**Newly Registered Users**").

6 The first unintended effect was to change the behaviour of the Booking System when Newly Registered Users resumed their sessions following a Time-out. A Time-out occurred if their sessions happened to be idle for 30 minutes. The System no longer redirected them to the homepage as it did before the changes. Instead, they stayed on the same page where they could access the "Dashboard".

7 The second unintended effect was when the timed-out Newly Registered Users accessed the Dashboard tabs. The Dashboard's "past" "upcoming" and "all" tabs disclosed the records of bookings by other individuals. Each tab could display a maximum 15 records thereby disclosing a total of 45 records.

Findings and Basis for Determination

8 The Complaint pertains to the protection obligation under section 24[1] of the PDPA. In the context of the present case, when an organisation makes changes to a system that processes personal data in its possession or control, the organisation has to make reasonable arrangements to prevent any compromise to personal data.

9 The Organisation omitted to test the effects of access through the New Mobile App with the existing access through browsers. Registered Users are identified by their mobile device IDs that are associated with their user account. However, newly Registered Users who completed bookings through browsers had no mobile device IDs stored in their accounts.

10 An integration test plan should have considered whether such newly registered users could be identified by other information in their accounts. However, in the absence of mobile device ID in a Newly Registered User's account, the browser retrieved and displayed other booking records in the Dashboard tabs as mentioned above.

11 Further, session time-out was a likely occurrence. This included time-out of browser sessions of Newly Registered Users. An integration test plan ought to have anticipated this scenario. The Organisation was therefore found in breach of section 24 of the PDPA.

[1] Section 24 of the PDPA requires an organisation to protection personal data in its possession or under its control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risk.

12 Having found that the Organisation is in breach of the PDPA, I am empowered under section 29 of the PDPA to issue the Organisation such directions as it deems fit to ensure compliance with the PDPA. In assessing the impact of the breach, I considered the fact that a specific set of circumstances was needed for the disclosure to have occurred, and such a coincidence is uncommon:

(a) The user had never registered on the Website previously;

(b) The user made a booking and made payment;

(c) The user did not log our or close the browser window but instead left the page idle for 30 minutes;

(d) The user returned to the same webpage after 30 minutes; and

(e) The user clicked on the dashboard hyperlink.

13 The disclosure occurred only if payment had been made for one or more travel tickets. This meant that disclosure would likely have been to bona fide customers rather than other persons. Additionally, the nature of the flaw made it less readily detectable by an attacker, compared with misconfigured firewalls or unpatched servers for instance.

14 Further, I considered that disclosure to the complainant was limited to 45 sets of booking records disclosed. At a maximum, the bug exposed a total of 72 personal data sets of booking information.

15 Accordingly, I hereby direct the Organisation to carry out the following within 60 days:

(a) Assess whether its application testing has been complete in order to discover and remedy any risk to personal data from the changes made to introduce the new mobile application function;

(b) Furnish a report of the assessment as well as action taken in response; and

(c) To put in place procedures and processes, to manage the risks to the personal data in its possession or control, when making changes to its applications, by implementing testing procedures and documenting the tests conducted

YEONG ZEE KIN
DEPUTY COMMISSIONER
FOR PERSONAL DATA PROTECTION