PERSONAL DATA PROTECTION COMMISSION

[2019] SGPDPC 4

Case No DP-1707-B0917

In the matter of an investigation under section 50(1)
of the Personal Data Protection Act 2012

And

COURTS (Singapore) Pte Ltd

… *Organisation*

DECISION

COURTS (Singapore) Pte Ltd

[2019] SGPDPC 4

Tan Kiat How, Commissioner — Case No DP-1707-B0917

22 January 2019

Background

1 On 9 July 2017, the Personal Data Protection Commission (the "**Commission**") received a complaint from a customer ("**Complainant**") of COURTS (Singapore) Pte Ltd ("**COURTS**") stating that the http://www.courts.com.sg website ("**Website**") was "*unsafe for customers*". The Complainant discovered that by entering his name and e-mail address on COURTS' Guest Login ("**Guest Login Page**") for the purpose of making a purchase, the Website would automatically open another webpage ("**Guest Checkout Page**") disclosing the Complainant's contact number and address (the "**Incident**").

2 Following an investigation into the matter, the Commissioner found COURTS in breach of section 24 of the Personal Data Protection Act 2012 ("**PDPA**").

Material Facts

3 The Website is owned and managed by COURTS, a leading consumer electronics and furniture retailer in Singapore with a network of 80 stores nationwide. Ebee Global Solutions Pvt Ltd ("**Ebee**") was an IT vendor engaged by COURTS to develop and maintain the Guest Login Page and Guest Checkout Page ("**Guest Checkout System**") that was part of the Website. At the material

time, the process flow when a customer wished to make a purchase through the Guest Login Page was as follows:

(a) The customer accesses the Website and selects an item to "Add to cart" before selecting "Proceed to checkout";

(b) The customer may choose to log into his COURTS' HomeClub account or he may choose to "Checkout as guest user";

(c) If the customer chooses to check out as a guest user, he enters his name and email address and selects "Login as guest"; and

(d) Assuming that the customer has previously made a purchase through the Website using the same email address, the customer's contact number and residential address (collectively, the "**Personal Data Set**") will be displayed on the Guest Checkout Page.

4 Investigations revealed that in relation to (c) above, the Personal Data Set would be displayed upon an exact match with the Email Address the customer had used previously even if the name entered does not match the name the customer used initially. In the circumstances, the customer's email address was the sole login credential as the "Name" field did not serve any security purpose; access to the Guest Checkout System was not conditional on linking the input entered into the "Name" field with the customer's email address.

5 The Guest Checkout System was launched on 21 April 2014. Data collected from the Guest Checkout System was stored in COURTS' database hosted on the Amazon Web Services server ("**AWS Server**"). The database contained customers' email addresses, contact numbers and residential addresses.

6 As at 9 July 2017, COURTS confirmed that a total of 14,104 Personal Data Sets were stored in COURTS' database hosted on the AWS Server. The Personal Data Sets belonged to either COURTS' HomeClub customers or to customers who had made a purchase using the Guest Checkout System since 21 April 2014.

7 COURTS took the following remedial actions after it was notified of the Incident:

(a) On 30 August 2017, COURTS launched a new Website with a new Guest Checkout System in place. No data is stored for future use during the new guest checkout process. Customers using the new Guest Checkout System are required to key in their personal data each time a purchase is made. The Guest Checkout Page would not populate the Personal Data Set even if the same customer had previously made a purchase.

(b) On 30 September 2017, COURTS' database containing the Personal Data Sets hosted on the AWS Server was decommissioned;

(c) COURTS engaged a PDPA consultant to conduct PDPA trainings for its support centre and operation groups, and scheduled a full audit on COURTS' processes; and

(d) COURTS put in place additional security measures, such as adopting a policy for penetration tests to be performed at least once every 6 months on the new Website.

The Commissioner's Findings and Basis for Determination

8 It is not disputed that the Personal Data Set is "personal data" as defined in section 2(1) of the PDPA. There is also no dispute that the PDPA applies to COURTS as it falls within PDPA's definition of "organisation". The issue to be determined by the Commissioner in this case is whether COURTS had complied with its obligations under section 24 of the PDPA.

Whether COURTS complied with its obligations under section 24 of the PDPA

9 Section 24 of the PDPA provides that an organisation shall protect 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 risks. It is not disputed that COURTS had possession and/or control of the Personal Data Sets stored in COURTS' database, and hosted on the AWS Server. In this regard, COURTS confirmed that Ebee did not have the login credentials to COURTS' database. Its arrangement with Ebee was in the nature of a software development relationship. While the scope of the contract with Ebee covered the maintenance of the Guest Checkout System, in reality, maintenance was not carried out. COURTS did not engage Ebee to operate the database or perform any form of processing activities on the Personal Data Sets and as such, Ebee was not a data intermediary.

10 The investigations found that COURTS failed to put in place reasonable security arrangements to protect the Personal Data Sets for the following reasons:

(a) Email addresses are readily shared by individuals and searchable on various public platforms. The use of an email address as the sole login

credential on the Guest Login Page resulting in disclosure of the Personal Data Set on the Guest Checkout Page fell short of the standard of protection required to prevent unauthorised access. As has been held in *Re ABR Holdings Ltd [2016] SGPDPC 16*, it is not acceptable to use commonly used identifiers to retrieve personal data. The intention to make the user experience smooth for returning guest shoppers without a HomeClub account was laudable but quite unacceptable as it poses a risk to customers. The entry of an email address was sufficient to retrieve the associated contact number and address that had been stored in the database. This amounted to a failure to protect personal data of returning customers that falls below the standard expected under the PDPA.

(b) There was a glaring failure by COURTS to adequately consider data protection with respect to the Guest Checkout System of the Website. Although the Website and Guest Checkout Page were launched before the PDPA came into force, COURTS failed to review their system design or process flow, or implement any internal security policies in relation to data protection for the Website after the PDPA came into force for the purpose of ensuring compliance. Additionally,

(i) No penetration tests were conducted since the launch of the Website and the Guest Checkout Page on 21 April 2014;

(ii) No security scans were performed on the Website for a period of 12 months prior to the Incident; and

(iii) No maintenance of the Guest Checkout System had been carried out since its launch on 21 April 2014.

11 COURTS represented that it had scheduled training programmes in place for all employees with respect to data protection obligations under the PDPA.

(a) New employees are required to go through tailored PDPA training specific to their job scopes during on-boarding; and

(b) PDPA refresher training is conducted for all employees, with the most recent one being in February 2017.

12 While data protection training has an impact on the proper implementation of an organisation's data protection policies and practices, these training measures are ineffective to deal with the system design and process flow deficiencies in the Website and cannot therefore amount to sufficient security arrangement to protect against the unauthorised disclosure of the Personal Data Sets. Admittedly, COURTS conceded that the disclosure of the Personal Data Set on the Guest Checkout Page once an email address matched an existing customers' record in COURTS' database was "…*an oversight on a design flaw that we were serving data unauthenticated".* It is inexcusable for an established organisation like COURTS to neglect its obligations to put in place reasonable security arrangements to protect the Personal Data Sets. This resulted in the Personal Data Sets being exposed to risk of unauthorised disclosure for more than 3 years[1].

13 For the reasons above, the Commissioner finds COURTS in breach of section 24 of the PDPA.

---

[1] 21 April 2014 to 30 August 2017.

The Commissioner's Directions

14 Given the Commissioner's findings that COURTS is in breach of section 24 of the PDPA, the Commissioner is empowered under section 29 of the PDPA to issue COURTS such directions as it deems fit to ensure compliance with the PDPA. This may include directing COURTS to pay a financial penalty of such amount not exceeding S$1 million.

15 In assessing the breach and determining the directions, if any, to be imposed on COURTS in this case, the Commissioner took into account the following aggravating factors:

(a) Given that email addresses are widely shared, use of an email address as the sole login credential to protect against unauthorised disclosure of the Personal Data Set was clearly not a reasonable security arrangement;

(b) COURTS subjected the Personal Data Sets to risk of unauthorised disclosure for a substantial period of about 3 years; and

(c) COURTS displayed a lack of urgency and absence of initiative to obtain information in relation to the Incident.

16 The Commissioner also took into account the following mitigating factors:

(a) There was limited risk of unauthorised disclosure because the Personal Data Set would only be disclosed upon entry of a matching email address used by COURTS' HomeClub customers or previous customers who had made a purchase through the Guest Check Out System;

(b) There was no evidence to suggest any actual loss or damage resulting from the Incident; and

(c) COURTS effected remedial actions upon being informed to implement measures to prevent recurrences of the Incident and to increase employee's awareness of the PDPA.

17 Having considered all the relevant factors of this case, the Commissioner hereby directs COURTS to pay a financial penalty of S$15,000.00 within 30 days from the date of the Commissioner's direction, failing which, interest at the rate specified in the Rules of Court[2] in respect of judgment debts, shall accrue and be payable on the outstanding amount of the financial penalty until the financial penalty is paid in full.

YEONG ZEE KIN
DEPUTY COMMISSIONER
FOR COMMISSIONER FOR PERSONAL DATA PROTECTION

---

[2] Cap 322, R5, 2014 Rev Ed.