PERSONAL DATA PROTECTION COMMISSION

[2020] SGPDPC 17

Case No DP-1909-B4731

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

[2020] SGPDPC 17

Lew Chuen Hong, Commissioner — Case No DP-1909-B4731

14 August 2020

Introduction

1 On 6 September 2019, COURTS (Singapore) Pte Ltd (the "**Organisation**") notified the Personal Data Protection Commission (the "**Commission**") that an individual in its membership programme who had received an Electronic Direct Mail ("**eDM**") from the Organisation, was able to access, without authentication, data in another individual's account after clicking on a link (the "**New eDM Link**") in the eDM (the "**Incident**").

Facts of the Case

2 The Organisation is a well-known consumer electronics and furniture retailer, with a number of stores in Singapore. Its membership programme, known as "homeclub by COURTS" ("**Homeclub**") gives its members ("**Members**") exclusive access to, among other things, events and discounts. The Organisation regularly sends eDMs to Members with links to specific products on the Organisation's website (the "**Website**").

3 The Organisation used a platform called Salesforce to create and send eDMs (the "**Platform**") and the Website ran on the Magento system[1] (the "**System**"), an e-commerce platform. The System generated a dynamic session identifier ("**SID**") for each login to Homeclub on the Website. This SID would be used for all subsequent activities within the session.

4 On 31 August 2019, the Organisation sent an eDM to 76,844 Members (the "**Affected Members**"). This eDM, included for the first time, the New eDM Link, which was meant to direct Members to the Homeclub login page. The purpose of the New eDM Link was for Members to log in to their respective Homeclub accounts to update their membership identifier – Members were required to provide their mobile numbers to replace NRIC numbers that were previously used as the membership identifier.

5 The New eDM Link did not operate as intended, resulting in the Incident. The Commission's investigations revealed the following:

(a) Notwithstanding that the eDM sent on 31 August 2019 included for the first time the New eDM Link, the Organisation continued to use the System in its default setting. The default setting comprised (i) the SID embedded in the URL of the New eDM Link;[2] and (ii) cookie settings to be refreshed after 60 minutes.

(b) The default setting had not caused any issues when it was used by the Organisation to send marketing eDMs with eDM links directing Members to specific products on the Website. As Members were not

[1] The Organisation acquired a license to operate the System from 6 March 2017.

[2] This was due to the default setting "Use SID on Storefront" being set to "Yes"

required to log in to their accounts in order to view the specific products, the SID embedded in the URL and cookie settings did not affect the functioning of the Website.

(c) However, the default setting should not have been used for the New eDM Link – it led to the System assuming that every use of the New eDM Link within 60 minutes of a Member's login was part of the same session. This meant that:

(i) If Member X clicks on the New eDM Link and logs into his Homeclub account without logging out within 60 minutes, all other Members who subsequently clicked on the New eDM Link within 60 minutes of Member X's login would automatically be directed to Member X's account, without having to authenticate their credentials; and

(ii) If Member X logged out while other Members were still logged into Member X's account, the other Members would only be logged out of Member X's account if they refreshed a page or navigated to other pages within Member X's account.

6 According to the Organisation, 128 of the Affected Members clicked on the New eDM Link between approximately 8am on 31 August 2019 and 12.25am on 1 September 2019.[3] The Incident led to the risk of unauthorised access and modification of personal data in the Affected Members' respective Homeclub accounts. In this regard, each Member's Homeclub account

[3] The eDM containing the New eDM Link was sent to Members at approximately 8am on 31 August 2019. The Organisation rectified the error causing the Incident at approximately 12.25am on 1 September 2019.

comprised (i) account information; and (ii) address book, which collectively contained the following data ("**Personal Data Set**"):

(a) Name;

(b) Email address:

(c) Mobile Number;

(d) Date of Birth ("**DOB**");

(e) Address;

(f) Password; and

(g) Transactional information i.e. products previously purchased by a Member.

7 In addition to unauthorised access, the following types of personal data in the Affected Members' Personal Data Sets were at risk of unauthorised modification as a result of the Incident:

(a) The Affected Member's name, DOB, mobile number and residential address from his/her account information; and

(b) The Affected Member's name, mobile number and residential address from his/her address book.

8 The risk of unauthorised modification in [7(a)] and [7(b)] was possible because password verification was not required to make these changes. Conversely, an Affected Members' username (which was his/her email address) and password could not be modified without password verification. An Affected Member's Personal Data Sets also could not be downloaded by another Member

who had accessed his/her account because there was no download function on the Website.

9 There was no risk of financial loss to Affected Members through the Incident. While it was possible for another Member (who was given access to Member X's account) to make a purchase through Member X's account, he/she would have to provide credit card details to complete the purchase. This was because financial information (i.e. credit card details) was not stored in the System, and there was no reward system in Homeclub for the redemption of products or benefits.

10 Based on the Organisation's investigations into the Incident, there was no evidence of any unauthorised modification to the Affected Members' Personal Data Sets. Other than the Affected Member who had notified the Organisation of the Incident, the Organisation did not receive any further complaints or feedback.

11 Upon being notified of the Incident on the same day, the Organisation promptly took the following remedial actions:

(a) Fixed the error that caused the Incident at approximately 12:25am on 1 September 2019 by changing the setting for "*Use SID on Storefront*" to "*No*";

(b) Implemented password verification for any changes to Members' account information and address book;[4]

[4] This came into effect on 6 January 2020.

(c) Put in place a standard operating procedure ("**SOP**") to ensure correct link insertion into eDMs to protect personal data. For eDM links that are supposed to lead to a login page, checks will be conducted to ensure that there will be multiple concurrent user testing;

(d) Took steps to engage an external vendor to work on security matters (including data protection security), and disseminate this information to its employees; and

(e) Emailed the 128 Affected Members who had clicked on the New eDM Link to inform them of the Incident.

The Commissioner's Findings and Basis for Determination

Whether the Organisation had contravened section 24 of the PDPA

12 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 or similar risks (the "**Protection Obligation**"). It is not disputed that the Organisation had possession and control of the Personal Data Sets at the material time. The Commission's investigations revealed that the Organisation failed to put in place reasonable security arrangements to protect the Personal Data Sets for the reasons explained below.

13 First, the Organisation failed to conduct adequate testing before implementation. As mentioned at [4], this was the first time the Organisation included in its eDM, the New eDM Link to direct Members to the Homeclub login page. There was only 1 employee in the Organisation's digital marketing team that was in charge of creating the New eDM Link and testing it prior to its

launch. The employee conducted a limited test of sending the eDM containing the New eDM Link to himself – the New eDM Link operated as intended, directing the employee to the Homeclub login page. This limited test was clearly inadequate. As emphasized in the Commission's previous decisions, an organisation should ensure that testing scenarios are properly scoped. In particular, pre-launch testing of processes or systems needs to mimic expected real world usage, including foreseeable scenarios in a normal operating environment when the changes are introduced.[5] In the present case, the Organisation intended to send the eDM to a very large number of Members. It is therefore foreseeable that testing scenarios should include multiple sequential logins or even concurrent logins to the Homeclub login page at peak usage. If the Organisation had tested the New eDM Link to approximate this real world scenario, the Incident would have likely come to light at that stage.

14 Second, the Organisation failed to assess the appropriateness of the default settings in the System for the New eDM Link.

(a) The Organisation used the default setting in the System for the New eDM Link without any assessment on its implications. As mentioned in the Commission's Guide to Securing Personal Data in Electronic Medium at [17.5] and previous decisions,[6] when using ready-made software, organisations are required to obtain a clear understanding of the intended purpose of the software, how the software

[5] See *Re Option Gift Pte Ltd* [2019] SGPCPC 10 at [15]; *Re AIA Singapore Pte Limited* [2019] SGPDPC 20 at [15] and *L'Oreal Singapore Pte. Ltd.* Case No. DP 1812-B3091, Summary of the Decision at [3]

[6] See for example *Re DS Human Resource Pte Ltd* [2019] SGPDPC 16 at [9]

functions and how to configure the software correctly. The Organisation failed to do so in the present case;

(b) There was an option in the Platform to automatically generate eDM links without any SID in the URL. The Organisation did not fully appreciate the differences in using this option to create links that are embedded within an eDM, as compared with the effects of embedding SIDs as part of the URL for the New eDM Link. Due to the lack of understanding the differences between these out-of-the-box features of the commercial off-the-shelf product that he was using, the employee in charge of creating the New eDM Link was not aware that the appropriate method was to use the option in the Platform that generated eDM links without SID in the URL. Instead, the employee manually copied the New eDM Link (which contained the SID) from the internet browser for insertion into the eDM; and

(c) While the Organisation had in place a process for a second-level check on the content and layout of the eDM, the nature of this type of checks would not have been effective in picking up the more technical issues relating to embedded SID in the New eDM Link. Understanding fully the features of the commercial off-the-shelf product in use and properly scoping the testing scenarios during user acceptance testing would have been the more appropriate and effective way to avoid and catch such errors.

15 For the reasons above, the Commissioner found the Organisation in breach of section 24 of the PDPA.

Representations by the Organisation

16 In the course of settling this decision, the Organisation made representations on the amount of financial penalty that the Commissioner intended to impose. The Organisation raised the following factors for the Commissioner's consideration:

(a) The Organisation takes a serious view of its obligations under the PDPA, and has taken the necessary remedial actions to prevent future data protection incidents from occurring. Personal data protection remains a priority for the Organisation even during these uncertain and turbulent times amidst the COVID-19 pandemic; and

(b) The COVID-19 pandemic has had an adverse impact on the business of the Organisation, resulting in a significant loss of revenue. Specifically, due to "circuit breaker" measures imposed by the government, the Organisation closed all 14 of its retail outlets in Singapore from 7 April 2020 to 19 June 2020. Further, its operating overheads remained largely unchanged as labour accounted for significant portion of its costs, and the Organisation has maintained a commitment to retaining employees so as to protect their livelihoods. Even with the recent reopening of its physical stores, the Organisation continues to have a negative outlook of its business due to the impact of COVID-19 on the economy and a challenging retail landscape.

17 Having carefully considered the representations, the Commissioner has decided to reduce the financial penalty to the amount set out at [19]. The quantum of financial penalty has been calibrated after due consideration of the Organisation's financial circumstances due to the unprecedented challenges faced by businesses amid the current Covid-19 pandemic, bearing in mind that

financial penalties imposed should not be crushing or cause undue hardship on organisations. Although a lower financial penalty has been imposed in this case, the quantum of financial penalty should be treated as exceptional and should not be taken as setting any precedent for future cases.

The Commissioner's Directions

18 In determining the directions, if any, to be imposed on the Organisation under Section 29 of the PDPA, the Commissioner took into account as an aggravating factor that this is the second time the Organisation has been found in breach of the Protection Obligation.[7] The Commissioner also took into account the following mitigating factors:

(a) The Organisation cooperated with the investigations and provided prompt responses to the Commission's requests for information;

(b) The Organisation implemented remedial actions swiftly to address the Incident; and

(c) The Members' Personal Data Sets was exposed to the risk of unauthorised access and/or modification for a limited period of less than one day.

19 Having considered all the relevant factors of this case, the Commissioner hereby directs the Organisation to pay a financial penalty of S$9,000 within 30 days from the date of this direction, failing which interest, at the rate specified in the Rules of Court in respect of judgment debts, shall accrue and be payable

[7] See *Re Courts (Singapore) Pte Ltd* [2019] SGPDPC 4

on the outstanding amount of the financial penalty until it is paid in full. The Commissioner has not set out any further directions given the remediation measures already put in place.

YEONG ZEE KIN
DEPUTY COMMISSIONER
FOR COMMISSIONER FOR PERSONAL DATA PROTECTION