Option Gift Pte Ltd

[2019] SGPDPC 10

Tan Kiat How, Commissioner — Case No DP-1806-B2242, DP-1806-B2243 and DP-1806-B2244

Data protection – Protection obligation – Disclosure of personal data – Insufficient security arrangement

6 June 2019.

Background

1 On 12 June 2018, the Personal Data Protection Commission (the "**Commission**") was notified by the Organisation of the unintended disclosure of up to 426 individuals' personal data due to a coding error in its system. The Commission subsequently received complaints from 2 of the affected individuals on 12 and 13 June 2018 respectively.

2 Following an investigation into the matter, the Commissioner found the Organisation in breach of section 24 of Personal Data Protection Act 2012 ("**PDPA**") and sets out below his findings and grounds of decision based on the investigations carried out in this matter.

Material Facts

The Portal

3 The Organisation maintains Uniqrewards (the "Portal"), an online portal through which national servicemen ("NSmen") may redeem credits and gifts given by the Ministry of Defence ("MINDEF") and the Ministry of Home Affairs ("MHA") in recognition of their good performance during in-camp training or courses, or to celebrate certain events, such as the birth of a child. An NSman may log into the Portal and submit his redemption request, following which he would instantly receive a confirmation email that his order(s) are being processed ("Confirmation Emails"). Besides the NSman concerned, the customer service team of the Organisation would also receive a copy of the Confirmation Email by way of blind carbon copy.

4 These Confirmation Emails are generally sent via a service account linked to the Portal. The service account is hosted by an external vendor which has a password expiry policy of 180 days. While the employee concerned had previously reset the service account password before its expiry, he had failed to do so punctually in the latest round due to an oversight and a lack of reminders or warnings on password expiry. This led to 427 NSmen not receiving any Confirmation Emails for their redemption requests submitted between 22 May 2018 and 24 May 2018. This issue was detected by the Organisation on 23 May 2018.

The Incident

5 To rectify the issue, the Organisation wrote a separate programme script to regenerate and send out the Confirmation Emails which the Portal had

previously failed to send out due to the service account's password expiration. The programme script was intended to achieve the following objectives:

(a) accurately reflect the redemption request submitted by the NSman concerned and some of his basic details (i.e., his login identification, email address, delivery address and mobile number) on each regenerated Confirmation Email; and

(b) send the Confirmation Email only to its intended recipient.

6 The format of these Confirmation Emails were identical. To achieve objective (a), the programme script was meant to generate each of the 427 Confirmation Emails by extracting the relevant details of the intended recipient from the Organisation's backend database and including these details as part of the content of the email. To achieve objective (b), the programme script was meant to address the Confirmation Email only to the intended recipient's email address. This process performed by the programme script was iterative, and all 427 Confirmation Emails were to be generated in the same manner.

7 The programme script, however, did not behave as envisioned. While the content of each of these Confirmation Emails was correctly generated by the programme script, the programme script left the email address(es) of the recipient(s) of the preceding Confirmation Emails in the "To:" field of the email each time a new Confirmation Email was generated (the "**Error**"). It merely added on the intended recipient's email address, instead of replacing the previous recipient's email address with the intended recipient's.

8 In practice, this resulted in the first recipient of the Confirmation Email receiving the Confirmation Email that was intended for him as well as the Confirmation Emails of all the other 426 recipients. The second recipient

received the Confirmation Email which was intended for him as well as the Confirmation Emails of the subsequent 425 recipients; the second recipient would not have received the Confirmation Email of the first recipient as the second recipient's email address would not have been included in the Confirmation Email generated for the first recipient. Likewise, the third recipient received the Confirmation Email generated for him as well as the Confirmation Emails generated for the subsequent 424 recipients; the third recipient would not have received the Confirmation Emails generated for the first and second recipients as the third recipient's email address would not have been included in the Confirmation Emails generated for the first and second recipients. This pattern of addressing the Confirmation Emails continued until the last recipient, who received only the Confirmation Email intended for him.

9 This Error resulted in the personal data of up to 426 NSmen being accidentally disclosed (the "**Incident**"). These personal data comprised the relevant NSman's:

(a) login identification for the Portal;

(b) email address;

(c) delivery address; and

(d) mobile number.

10 After discovering the Incident, the Organisation took the following steps to mitigate the damage caused:

(a) On 12 June 2018, the Organisation:

(i) emailed all the affected NSmen an apology and requested for them to delete all emails not intended for them from redemption@uniqrewards.com; and

(ii) notified the Commission of the Incident.

(b) On 13 June 2018, all the affected NSmen received a text message from MINDEF and MHA respectively apologising for the Incident and requesting the deletion of the same emails.

(c) In July 2018, the Organisation gave all the affected NSmen a gift voucher worth S$80 as a gesture of apology.

11 In addition to the above, the Organisation introduced the following further steps to prevent the recurrence of the Incident:

(a) All future changes to the Portal would be subjected to a secondary check during the development testing stage. Specifically, the person conducting integration testing would be required to print out the expected output in the development environment and have it validated by a checker before starting the user acceptance test.

(b) All coding scenarios would have a separate person reviewing the source code written by the developer.

(c) The Organisation began work to enhance the Portal's backend system to allow Confirmation Emails to be resent directly.

(d) The Organisation introduced a standard operating procedure to document the process of resending Confirmation Emails. Under this procedure, only authorised users, with the approval of the

Organisation's data protection officer, may resend Confirmation Emails. An audit trail would also be created during this process.

(e) The Organisation would deploy an application, Sonarcloud, to analyse the quality of source codes. Sonarcloud would be used to detect bugs, vulnerabilities and code smells during the development process.

Findings and Basis for Determination

12 As a preliminary point, section 4(1)(c) of the PDPA excludes an organisation which acts on behalf of a public agency in relation to the collection, use or disclosure of personal data from Parts III to VI of the PDPA (i.e., the data protection provisions). Nevertheless, the Commission's investigations revealed that the Organisation was a subcontractor of MINDEF and MHA and was not engaged by both public agencies to act on their behalf as a data intermediary. As such, section 4(1)(c) does not apply to the Organisation and the Organisation is required to comply with the data protection provisions of the PDPA.

13 The main issue for determination is whether the Organisation breached section 24 of the PDPA. 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.

14 As the administrator of the Portal, the Organisation had full possession and control over the personal data that the Portal collects, uses, discloses and processes at all material times. Accordingly, the Organisation had full responsibility for the security of the Portal, any changes to it, as well as the personal data processed by it. In this regard, the Commissioner found that the

Organisation had failed to conduct sufficient testing before rolling out the programme script.

15 In this case, software testing (i.e., development testing and user acceptance testing) was carried out on the programme script prior to its actual implementation. Investigations revealed a fundamental flaw in designing the test scenarios. The test scenario consisted of generating all 427 test emails but instead of picking up the recipient emails from a list of email addresses, each email was hardcoded to be sent to the same internal email address. Unsurprisingly, the Error, which would only have manifested itself if there was more than one recipient, was not detected. A more thoroughly designed test scenario that more closely approximated the anticipated real world deployment environment could have included:

(a) the use of several test email addresses;

(b) the programme script retrieving these test email addresses from a database (e.g. the main database of email addresses or a database of email addresses created for the job) instead of using a single hardcoded email address; and

(c) the programme script being used to send the Confirmation Emails to the retrieved test email addresses.

16 For the reasons above, the Commissioner finds the Organisation in breach of section 24 of the PDPA.

The Commissioner's Directions

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

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

(a) the Organisation voluntarily notified the Commission of the breach;

(b) the Organisation fully cooperated with the Commission's investigations;

(c) the Organisation took prompt action to mitigate the effects of the breach by informing the affected individuals via email on the same day (12 June 2018) and offering them a voucher worth $80 in July 2018; and

(d) the Organisation took prompt corrective action to resolve the vulnerability and further remedial measures to enhance its backend system to prevent the recurrence of similar incidents.

19 In consideration of the relevant facts and circumstances of the present case, the Commissioner hereby directs the Organisation to pay a financial penalty of $4,000 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 on the outstanding amount of such financial penalty until the financial penalty is paid in full.

20 The Commissioner has not set out any further directions for the Organisation given the remediation measures already put in place.

YEONG ZEE KIN
DEPUTY COMMISSIONER
FOR PERSONAL DATA PROTECTION