DECISION OF THE PERSONAL DATA PROTECTION COMMISSION

Case Number: [DP-1510-A558]

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

And

JP Pepperdine Group Pte. Ltd. [UEN 198601026G]

... Organisation

Decision Citation: [2017] SGPDPC 2

GROUNDS OF DECISION

25 January 2017

BACKGROUND

1. On 25 October 2015, the Complainant informed the Personal Data Protection Commission (the "**Commission**") that any member of the public could readily access the personal data of members that had joined the Organisation's membership programme by,

   (a) entering a randomly simulated membership number on a webpage (http://goo.gl/5BX9Rr, a Google URL Shortener that redirects to http://ascentis.com.sg/microcrm/JacksPlace_memberportal/searchprofile.aspx) listed on the Organisation's membership brochure (the "**Webpage**"); or

   (b) performing a search (without inputting any search parameters) using the search functions available on the Webpage.

2. On account of the complaints made, the Commission commenced an investigation under Section 50 of the PDPA to ascertain whether the Organisation had breached its obligations under the PDPA. The material facts of the case are as follows.

MATERIAL FACTS AND DOCUMENTS

3. The Organisation operates a number of restaurants in Singapore under various brands (e.g. Jack's Place, Eatzi Gourmet). The Organisation has a membership programme for its customers. Participating in the membership programme entitles members to special promotions and discounts across the different restaurants operated by the Organisation.

4. Each member would be assigned a 7-digit membership number by the Organisation. Membership numbers run sequentially. At the time of the investigation (December 2015), the Organisation had approximately 30,000 members.

5. As part of the investigation, the Commission verified that personal data of members of the Organisation's membership programme was publicly accessible through the Webpage by:

   (a) entering a randomly simulated membership number in the search facility on the Webpage, which would retrieve membership details associated with that account; or

   (b) simply clicking on the "Search" button in the search facility without any search parameters, i.e. the search fields were left blank, which would randomly retrieve the details of a membership account.

6. The personal data that was publicly accessible through the Webpage included, names of members, gender, marital status, nationality, race, NRIC/Passport number, date of birth, mobile phone number, home phone number, email addresses, residential addresses, and other membership account details.

7. The material facts from the Commission's investigations are as follows:

   (a) The Webpage was developed for the purposes of a one-off promotional event held in the first half of 2013 to recruit new members and to encourage existing members to update their personal particulars. The Webpage was created by the Organisation's vendor, Ascentis Pte Ltd ("**Ascentis**"). The Webpage contained a search facility that enabled searches and retrieval of personal particulars of the members of the Organisation's membership programme.

   (b) The Organisation claims that the Webpage was intended for internal use, and for the Organisation's staff to remotely search and access the Organisation's member database. Although the Webpage was not intended for public access, the Organisation did not put in place security measures (or require Ascentis to design any security measures), to control access and ensure that the Webpage was inaccessible to the public. The Webpage was not removed after the end of the promotional event in 2013 and remained accessible to both staff and the public until 29 October 2015.

   (c) The Organisation listed on its membership brochures hyperlink that was truncated using a Google URL shortening service ("**a Google URL Shortener**") that redirected any person who accessed it to the Webpage. These membership brochures, which contained the Google URL Shortener and other information on the membership application process, were disseminated by the Organisation to all the restaurants under its different brands. The Organisation claims that the redirection to the Webpage was a mistake and that the public should have been redirected to the Organisation's membership portal located at another URL. Yet, for

the entire period the membership brochure was in circulation at the Organisation's restaurants (from as early as 2013), the URL listed in the brochures had not been corrected.

(d) The Webpage had a security loophole, as described above at paragraph 5(b), that caused the random retrieval of members' account details whenever the "Search" button was clicked with no search parameters. The Organisation admitted that the loophole was caused by an unpatched bug in the original version of the Webpage. The Organisation was not aware of the existence of the bug in the Webpage or the resulting security loophole until it was notified by the Commission.

8. On 29 October 2015, after receiving the Commission's notification, the Organisation introduced security features to the Webpage by incorporating a password protection feature such that the Webpage was no longer publicly accessible and could only be accessed after authentication.

9. Subsequently, the Organisation implemented further measures to address the complaint:

(a) the Organisation secured the Webpage with a landing page which was password-protected. Access to the Webpage would only be granted through inputting user credentials known only to the Webpage's administrators; and

(b) the Organisation also took steps to ensure that all references to the Google URL Shortener listed in the Organisation's membership brochures that were still in available in the Organisation's restaurants were removed.

COMMISSION FINDINGS AND BASIS FOR DETERMINATION

Issue to be determined

10. Section 24 of the PDPA requires an organisation to protect personal data in its possession or under its control by taking reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks.

11. The issue in the present case is whether the Organisation had breached Section 24 of the PDPA, when personal data (of members of the Organisation's membership programme) could be accessed on the Webpage (in the manner described in paragraph 5 above).

Whether the Organisation had complied with Section 24

12. The data accessible on the Webpage included the names of members of the Organisation's membership programme, their contact information, addresses and identification numbers. These data fall within the definition of "personal data" under the PDPA.

13. The personal data accessible on the Webpage was also under the control of the Organisation. The Organisation demonstrated this control when it was able to promptly effect changes to the Webpage to restrict public access to such personal data when contacted by the Commission.

14. In the course of investigations, Ascentis confirmed that the Webpage was designed without any security measures as per the Organisation's specifications. The Organisation claims that it did not require security features to be incorporated because the Webpage was intended for (a) internal (and not public) purposes; and (b) temporary use at the Organisation's 2013 promotional event.

15. This may be the state of the Organisation's system in 2013; but when the PDPA came into full effect on 2 July 2014, it was incumbent on the Organisation to ensure that it had in place the necessary security arrangements to protect the data. Steps must be taken to ensure that the security that would protect the personal data under the Organisation's possession or control was ready by the time that the PDPA had come into full force. In the Commission's view, one of the first few steps that ought to have been taken was to determine if the system was to continue to be made accessible via the Internet or to keep it wholly within its internal network. Thereafter, the Organisation ought to have conducted a review of its system so as to determine the weakness and vulnerabilities of the system for the type of access and use that was intended. This would allow the Organisation to know where the weaknesses and vulnerabilities are which needed to be addressed.

16. In this case, the loophole in the Webpage was a significant gap in the protection of the system that allowed unauthorised access to personal data stored on the server. The Organisation had not shown that it took any steps (as mentioned at paragraph 15 above) to detect and rectify this problem. No checks or tests were done on the system. No steps were taken to ascertain and limit (or block) the entry points to the personal data stored on the server. Indeed, the Webpage proved to be one such entry point. The Organisation failed to have the Webpage taken down, notwithstanding that the Organisation had, from the outset, intended to do so. In this regard, the Organisation did not ensure the security of the personal data it was obliged to protect.

17. It is clear that the Organisation's system did not have any reasonable or adequate security arrangements to protect the personal data that was accessible through the Webpage:

    (a) there were no security or access controls to the Webpage and any member of the public could have accessed the personal data of the Organisation's members through the Webpage. Even if the Webpage was intended by the Organisation to be for internal use, there would still be an obligation on the Organisation make reasonable security arrangements to prevent unauthorised access to the personal data stored on the system. In the present case, knowing that the personal data was stored online and could be accessed from the Webpage, the Organisation should have at least implemented basic technical security

measures to ensure that the system, including the Webpage, was secure and not accessible by the public.

(b) The Webpage allowed the use of the membership number assigned to each member, to serve the functions of identification and authentication to access personal data. In the Commission's view, where a single string of numbers is the only security arrangement serving both to identify and authenticate access to personal data, such security arrangement could be considered reasonable only if (depending on the sensitivity of the personal data being protected) this number was unique, unpredictable and reasonably well-protected. In this case, the membership numbers assigned by the Organisation to its members were issued in running sequence and easy to ascertain or deduce, and therefore, such a security arrangement could not be considered reasonable.

(c) The Webpage contained a security loophole (described in paragraph 5(b) above) which effectively allowed members of the public free and unfettered access to personal data of random account holders through the Webpage.

18. Additionally, by including the Google URL Shortener in the brochure, which redirected a person to the Webpage, the Organisation was facilitating access to the Webpage, and the personal data held on the system. A user that followed the link would, whether by accident or on purpose, be able to gain access to the personal data of the Organisation's customers. While the Organisation submits that the redirection of the link was wrong and unintended, the Commission does not find this to be excusable. A prudent organisation which was promulgating a link to the public should at least check the link before publication. Had the Organisation done so, it would have noticed that there was something amiss, as the link would have brought up the Webpage, which was not supposed to be in operation.

19. In view of the above, the Commission finds that the Organisation had failed to make reasonable security arrangements to protect personal data in its possession or under its control. As such, the Organisation was in breach of Section 24 of the PDPA.

20. The Commission adds that although the Webpage was designed by Ascentis, on the available facts, Ascentis was not a data intermediary for the Organisation. There is no evidence that Ascentis processed any personal data on behalf of the Organisation. Ascentis's role was limited to designing the Webpage for the Organisation according to the instructions of the Organisation. Accordingly, the Commission makes no findings in respect of Ascentis.

ACTIONS TAKEN BY THE COMMISSION

21. Given the Commission's findings that the Organisation is in breach of its obligations under Section 24 of the PDPA, the Commission 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.

22. In determining the direction, if any, to be made, the Commission considered the following factors related to the case, including the mitigating and aggravating factors set out below:

(a) A substantial amount of personal data of some 30,000 members of the Organisation's membership programme, was placed at risk. This risk has exacerbated by the Organisation's publication of the Google URL Shortener, which redirected individuals to the Webpage with the security loophole, on its membership brochures that were disseminated to all its restaurants.

(b) The personal data at risk involved sensitive personal data such as the NRIC/Passport numbers of members of the Organisation's membership programme.

(c) The data breach may have been avoided (or the impact of the breach reduced) if the Organisation had taken the following simple steps:

(i) reviewing the information in its own membership brochures, at which point it would have realised that members of public were being mistakenly redirected to the Webpage (intended for internal use) instead of the Organisation's membership portal; and/or

(ii) ensuring that the Webpage (intended for internal use) was inaccessible to the public right from the outset, or by promptly removing the Webpage once the 2013 promotional event for which the Webpage was created had concluded.

(d) The Organisation took prompt action to remedy the breach when notified by the Commission.

23. In view of the factors noted above, pursuant to Section 29(2) of the PDPA, the Commission hereby directs that the Organisation pay a financial penalty of S$10,000 within 30 days of the Commission's direction, failing which interest at the rate specified in the Rules of Court in respect of judgment debts shall be payable on the outstanding amount of such financial penalty.

YEONG ZEE KIN
DEPUTY COMMISSIONER
PERSONAL DATA PROTECTION COMMISSION