DECISION OF THE PERSONAL DATA PROTECTION COMMISSION

Case Number: DP-1408-A030

ABR HOLDINGS LIMITED [UEN 197803023H]

... Respondent

Decision Citation: [2016] SGPDPC 16

GROUNDS OF DECISION

23 September 2016

BACKGROUND

1. On 18 March 2014, the Complainant informed the Personal Data Protection Commission (the "**Commission**") that by entering either,

   (a) a random 8-digit number as a simulated membership number; or

   (b) a simulated Unique Identification Number (**UIN**) number (e.g. NRIC or Birth Certificate number with a valid check digit),

   on the Respondent's Swensen's Kids Club website, http://swensens.prism4u.com (the "**Website**"), one could access a Swensen's Kids Club member account associated with that membership or UIN number. Once accessed, the member's name and date of birth ("**DOB**") would be shown.

2. The provisions in the Personal Data Protection Act 2012 (the "**PDPA**") relating to the protection of personal data were not in force at the time of the complaint. The Commission wrote to the Respondent on 2 April 2014 to notify the Respondent of the complaint and that the provisions relating to protection of personal data would come into force on 2 July 2014.

3. On 15 July 2014, the Complainant submitted a further complaint claiming that on that date, the Respondent's Website still allowed access to a member's name and DOB by entering either a simulated membership number or valid UIN number.

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

MATERIAL FACTS AND DOCUMENTS

5. The Respondent has been operating the Swensen's chain of restaurants since 1978. The Swensen's Kids' Club is a membership programme which the Respondent runs for children between 4 and 12 years of age. By accumulating a certain number of electronic "stamps", Swensen's Kids' Club members may be eligible for various promotional offers from the Swensen's chain of restaurants (eg a free Kids' Club Sundae every month with dine-in food order). Each member would be assigned an 8-digit membership number by the Respondent. Membership numbers run sequentially.

6. The Website supports the Swensen's Kids' Club membership programme and allows a member to access information relating to his membership account. The Website has been in operation since 2013 and is maintained and operated by the Respondent's vendor, Prism4u (Singapore).

7. As part of the investigation, the Commission verified that access can be obtained to a member account on the Website by (a) entering a random number sequence simulating a valid membership number; or (b) entering a valid UIN number in the form of a birth certificate number. The Website did not require any password to be entered nor authentication in any other form before granting access.

8. The following details about a member were made available through the Website:

   (a) Name;

   (b) DOB;

   (c) Redemption status of Kids' Club Sundaes and "stamps";

   (d) Number of "stamps" accumulated; and

   (e) Membership expiry date.

9. The Respondent was notified of the further complaint by the Commission on 5 August 2014.

10. On the same day, the Respondent made changes to the Website to remove the display of the member's name and DOB. The effect of the changes was such that when the account is accessed using either a valid membership number or valid UIN number, the only details available would be information concerning redemption status, the number of "stamps" accumulated and the membership expiry date.

COMMISSION FINDINGS AND BASIS FOR DETERMINATION

Issue to be determined

11. 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.

12. The issue in the present case is whether the Respondent had breached Section 24 of the PDPA (during the period between 15 July 2014 and 5 Aug 2014), when personal data (of members of the Swensen's Kids' Club) could be accessed on the Website (in the manner described in paragraphs 7 and 8 above).

Whether Respondent had complied with Section 24

13. The personal data accessible on the Website included the name and DOB of members of the Swensen's Kids' Club. The names of the members fall within the definition of "personal data" under the PDPA.

14. The personal data accessible on the Website was also under the control of the Respondent. The Respondent demonstrated this control when it was able to promptly effect changes to the Website to block access to such personal data when contacted by the Commission.

15. The Respondent's system allowed the use of either (a) the membership number assigned to each member, or (b) the UIN number of the member, to serve the separate functions of identification of member and authentication to access personal data. These numbers were therefore the only security arrangement put in place by the Respondent to protect personal data on the Website.

16. 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, the numbers can possibly constitute reasonable security arrangements depending on the sensitivity of the personal data being protected, and only if this number was unique, unpredictable and reasonably well-protected.

17. In this case, the Respondent's use of membership numbers or UIN numbers did not constitute reasonable or adequate security arrangements for the personal data in its possession or under its control because:

    (a) the membership numbers assigned by the Respondent to its members were issued in running sequence. The Complainant was able to easily ascertain the number of characters required for a valid membership number and deduce another member's membership number since they were issued sequentially. Tools that are able to generate number sequences, which can be entered as membership numbers, are also

readily available online making it relatively easy to simulate other membership numbers;

(b) tools are readily available online that can simulate or generate UIN numbers (such as NRIC and birth certificate numbers); and

(c) once a generated membership or UIN number coincided with an assigned membership number or a member's UIN number, unauthorised access to the member's account and his personal data was possible. Until the system was altered to display only the accumulated "stamps", expiry date and redemption status, the child's name and date of birth were also displayed.

18. In view of the above, the Commission finds that the Respondent had failed to make reasonable security arrangements to protect personal data in its possession or under its control in the period between the commencement of the PDPA on 2 July 2014, and 5 August 2014, when the Commission notified the Respondent a second time regarding the same vulnerability. As such, the Respondent was in breach of Section 24 of the PDPA.

ACTIONS TAKEN BY THE COMMISSION

19. Given the Commission's findings that the Respondent 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 Respondent such directions as it deems fit to ensure compliance with the PDPA. This may include directing the Respondent to pay a financial penalty of such amount not exceeding S$1 Million.

20. In determining the direction, if any, to be made, the Commission considered the following factors:

(a) the Respondent was first notified of the vulnerability on 2 April 2014, before the PDPA came into force, thereby giving it ample time to take corrective measures;

(b) this infraction took place during the first month that the PDPA took effect;

(c) the personal data that was disclosed was largely limited to members' names and DOBs; and

(d) the Respondent took prompt action to remedy the breach within the same day when notified by the Commission a second time on 5 August.

21. In view of the factors noted above, the Commission has decided not to issue any direction to the Respondent to take remedial action or to pay a financial penalty. Instead, it has decided to issue a Warning to the Respondent for the breach of its obligations under section 24 of the PDPA.

22. The Commission takes a very serious view of any instance of non-compliance with the PDPA, and it urges organisations to take the necessary action to ensure that they comply with their obligations under the PDPA. The Commission will not hesitate to take the appropriate enforcement action against the organisation(s) accordingly.

YEONG ZEE KIN
COMMISSION MEMBER
PERSONAL DATA PROTECTION COMMISSION