Singapore Management University Alumni Association

[2018] SGPDPC 6

Tan Kiat How, Commissioner — Case No DP-1706-B0828

Data Protection – Protection obligation – Disclosure of personal data – Insufficient administrative security arrangements

30 April 2018.

Background

1 The Organisation, Singapore Management University Alumni Association, is a registered society under the Societies Act (Cap. 311), and is a society which caters to persons who are alumni of the Singapore Management University ("**SMU**").

2 On 7 June 2017, the Complainant informed the Personal Data Protection Commission (the "**Commission**") that by entering an identification number (e.g. NRIC number) on a webpage[1] of the Organisation's website, one could retrieve and access the membership application status and personal data of an individual to whom that identification number relates.

---

1 https://members.smuaa.org.sg/app_smuaa/smuaa-check-application-status.

3 On account of the complaint made, an investigation was commenced under section 50 of the Personal Data Protection Act 2012 (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

4 The Organisation introduced the webpage on 28 February 2017 to enable applicants, who had applied to be members of the Organisation, to check on the status of their membership application. The webpage was publicly accessible online and the URL of the webpage was also provided by the Organisation to applicants by way of an email. Instructions on how to use the webpage could be found on the Organisation's website.

5 An applicant could, by entering his identification number, specifically either a FIN or NRIC number, onto the webpage, gain access to details associated with his application such as the application status, and also his personal data such as name, identification number, contact number, address, email, and other details relating to his education at SMU (e.g. graduation year and course).

6 Apart from this requirement to enter an identification number, no other security measures or access controls were implemented to restrict access to personal data of the applicants through the webpage. Hence, from 28 February 2017 until 12 June 2017 (when remedial actions were taken by the Organisation), any person with the identification number of an applicant would have been able to access the personal data of that applicant through the webpage.

7 In contrast, the Organisation indicated that it had comparatively much stronger internal controls for access to the same data in question. The data was

stored in their Customer Relationship Management (CRM) systems and only authorised employees who had been issued individual login credentials could access the data with their credentials.

8 As at 12 June 2017, the personal data of some 297 applicants were rendered accessible through the webpage in such a manner.

9 After receiving notice of the complaint, the Organisation undertook the following remedial actions:

(a) When informed of the complaint on 12 June 2017, the Organisation, on the same day, disabled the webpage to prevent any unauthorised access to the personal data. Subsequently, the Organisation introduced additional requirements of inputting an applicant's email or mobile number (in addition to his identification number) to access his data on the webpage, with the data accessible also reduced to the applicant's application status, receipt number and date (i.e. the removal of personal data not otherwise required to ascertain the application status). From 4 July 2017, this feature and the webpage were entirely removed from the Organisation's website.

(b) The Organisation formed a committee to handle all matters relating to the complaint, and also undertook investigations, including a security audit, to determine the extent to which the personal data of the applicants had been compromised for the relevant period between 28 February 2017 and 12 June 2017. The server access logs for the webpage were examined to determine if any persons had exploited the vulnerability of the webpage (in using only an identification number as an access control) to gain unauthorised access to personal data. From the

investigation results presented by the Organisation, it appears that it is unlikely that any such unauthorised access had occurred.

(c) The Organisation also represented that it had implemented organisation governance measures to improve PDPA awareness and compliance within the Organisation, including (i) implementing internal operating procedures on data protection; (ii) requiring employees handling personal data to complete the data protection e-learning modules on the Commission's website; and (iii) plans to conduct risk assessment exercises to determine data protection competency.

Findings and Basis for Determination

Issues 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 by only securing personal data of the applicants in the manner described in paragraphs 5 and 6 above.

12 There is no question or dispute that the data in question concerned "personal data" as defined under the PDPA. The data concerned comprised of names, identification numbers, contact information and addresses. There is also no question or dispute that the personal data was under the control of the Organisation.

13 The issue that remains is whether the Organisation had taken reasonable security arrangements to protect the personal data concerned, by securing personal data of the applicants in the manner described in paragraphs 5 and 6 above.

14 In *Re ABR Holdings Limited* [2016] SGPDPC 16 ("***Re ABR Holdings***"), it was stated at [16] that:

> "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."

15 Accordingly, in the case of *Re ABR Holdings*, it was found at [17] that the use of identification numbers to serve the separate functions of identification and authentication to access personal data on the website of a membership programme could not constitute reasonable security arrangements (within the meaning of section 24 of the PDPA) given, amongst other things, that *"tools were readily available online that can simulate or generate UIN numbers (such as NRIC and birth certificate numbers)".*

16 In the present case, the Commissioner for Personal Data Protection ("**Commissioner**"), following from the decision in *Re ABR Holdings*, likewise finds that securing the personal data of applicants using only identification numbers to serve the functions of identification and authentication to access personal data does not constitute reasonable security arrangements.

17 The Organisation represented that it had instituted internal organisational measures and security standards to protect and restrict access to such personal data within its Organisation (see paragraph 7 above). Yet, when

it came to protecting and restricting access to the same data from the public, where the risks of unauthorised access is undoubtedly higher, the Organisation inexplicably failed to extend at least similar standards of protection, and instead relied on a standard that was much lower. The Organisation itself, in its response to the Commissioner's 2nd Notice to Require Production of Documents and Information ("**NTP**"), admitted that its use of FIN/NRIC numbers as an individual's sole login credentials for the website was "not a good enough protection as it [would] reveal the full application details of the individual". The Organisation further admitted that the unauthorised access of personal data via its website came about due to the "lack of PDPA knowledge in [its] team".

18 Accordingly, the Commissioner finds that the Organisation has contravened section 24 of the PDPA.

The Commissioner's Directions

19 Given the Commissioner's findings that the Organisation is in breach of its obligations under 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.

20 In assessing the breach and determining the directions (if any) to be made, the Commissioner considered, as an aggravating factor, the sensitivity of the personal data involved, which included FIN/NRIC numbers. In this regard, the Organisation made representations intimating that the fact that FIN/NRIC numbers were involved should not have been included as an aggravating factor given that a person trying to access the personal data would have already known the FIN/NRIC numbers. Although the potential population that is at risk is

small, the risk to the affected individual is high. Moreover, the use of an NRIC Number generation tool would make it relatively easy for a motivated hacker to systematically query the webpage and, if successful, he would have been able to definitively link the NRIC number to the full name, address and other personal data of the member, potentially resulting in significant harm to the individual, such as through identity theft or an unauthorised person impersonating the affected member.

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

(a) there was no evidence to suggest there had been any actual loss or damage resulting from the risk of unauthorised access or disclosure of personal data. In this regard, we refer to the server logs provided by the Organisation as set out at paragraph 9(b) above which showed that it was unlikely that any unauthorised access of personal data occurred. The Organisation also confirmed in it its representations that there has been no actual exposure of personal data;

(b) the Organisation had cooperated fully with the investigations; and

(c) the Organisation took prompt action (described in paragraph 9) to remedy the breach when notified.

22 In its representations, the Organisation also asked the Commissioner to consider the alleged obscurity of the website and the difficulty in finding the personal data in question as a mitigating factor. The Commissioner does not view this as a mitigating factor. Once the information is accessible on the internet, the fact that it may not be immediately found is not by itself a

mitigating factor. Instead, what is important is whether there was evidence of actual loss or damage as a result of the incident. The Commissioner had already taken into consideration the lack of actual loss or damage as a mitigating factor in determining the financial penalty quantum in this case before the Organisation submitted its representations.

23 In view of the factors noted above, pursuant to section 29(2) of the PDPA, the Commissioner hereby directs that the Organisation pay a financial penalty of S$5,000 within 30 days of the Commissioner'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 the financial penalty until the financial penalty is paid in full.

YEONG ZEE KIN
DEPUTY COMMISSIONER
FOR COMMISSIONER FOR PERSONAL DATA PROTECTION