PERSONAL DATA PROTECTION COMMISSION

[2020] SGPDPC 16

Case No DP-1905-B3865

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

And

Singapore Red Cross Society

… *Organisation*

DECISION

Singapore Red Cross Society

[2020] SGPDPC 16

Tan Kiat How, Commissioner — Case No DP-1905-B3865

5 May 2020

Facts of the Case

1 Singapore Red Cross Society (the "**Organisation**") operates a website at http://www.redcross.sg (the "**Website**") which allows the public to make appointments for blood donations. For this purpose, the Organisation collects personal data of individuals such as their names, contact numbers, email addresses and blood types (the "**Personal Data**"). The Personal Data was stored in the Organisation's blood donor appointment database (the "**Database**") accessible via the Website.

2 On 9 May 2019, the Organisation notified the Personal Data Protection Commission (the "**Commission**") that unauthorised individual(s) accessed and ex-filtrated the Personal Data of approximately 4,297 individuals ("**Affected Individuals**") from the Database (the "**Incident**").

3 Upon being notified of the Incident, the Organisation took the following remedial actions:

(a) Removed the appointment booking system on its Website in order to temporarily cease its collection of Personal Data through that channel; and

(b) Revised and strengthened its internal procedures to comply with the PDPA.

The Commissioner's Findings and Basis for Determination

The Organisation admitted that it had contravened Section 24 of the PDPA

4 Section 24 of the Personal Data Protection Act 2012 ("**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**").

5 The Organisation admitted that it failed to implement adequate security measures to protect the Personal Data stored in the Database, and had breached the Protection Obligation. In particular, the Organisation admitted to the following specific mistakes:

(a) The Organisation employed a vendor to develop the Website. However, there was a lack of supervision over the vendor's work which led to a failure to detect the presence of a phpMyAdmin database administration tool (the "**Tool**") which was used to manage the Database. There was also no password management policy requiring strong passwords of sufficient length and complexity during the development phase. This resulted in a weak password (i.e. "12345") being set for the Tool;[1] and

(b) The Organisation did not conduct any regular security reviews, e.g. vulnerability assessment, on its systems that would identify applications that it did not need.[2] Consequentially, the Organisation did not realise that the Tool remained connected to the Website even after development of the Website had been completed. This allowed unauthorised individual(s) to gain access to the Database through the Tool which had a weak password.

[1]For examples of the Commission's previous decisions on the need for proper password management policies, see *Re Orchard Turn Developments Pte Ltd* [2017] SGPDPC 12 at [35] – [36] and *Re Spize Concepts Pte Ltd* [2019] SGPDPC 22 at [15].

[2] For examples of the Commission's previous decisions on the requirement for periodic security reviews, see *Re Watami Food Services Singapore Pte Ltd* [2018] SGPDPC 12 at [6]; *Re WTS Automotive Services* [2018] SGPDPC 26 at [18]; *Re Bud Cosmetics* [2019] SGPDPC 1 at [24]; *Re Chizzle Pte Ltd* [2019] SGPDPC 44 at [6].

The Organisation admitted that it had contravened Section 25 of the PDPA

6 Under Section 25 of the PDPA, an organisation is obliged to cease to retain its documents containing personal data, or remove the means by which the personal data can be associated with particular individuals, as soon as it is reasonable to assume that: (a) the purpose for which the personal data was collected is no longer served by retaining the data; and (b) the retention is no longer necessary for legal or business purposes (the "**Retention Limitation Obligation**").

7 The Organisation admitted that there had been unnecessary retention of Personal Data of approximately 900 Affected Individuals, and this was a breach of the Retention Limitation Obligation.

(a) Prior to the Incident, the Organisation intended to purge Personal Data of these 900 Affected Individuals from the Database. However, the Organisation provided wrong instructions to its vendor for the purging exercise. The Organisation had instructed its vendor to only remove some data elements instead of entire records of the 900 Affected Individuals' Personal Data; and

(b) The Organisation also did not conduct any verification checks to ensure the purging exercise was properly carried out. As a result, the Organisation failed to detect that the Database still retained records of the 900 Affected Individual's Personal Data.

8 In view of the above, the Commissioner found the Organisation in breach of sections 24 and 25 of the PDPA.

The Organisation's Representations

9 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 is a charity that depends on public donations to run its operations and programmes, all which are for the benefit of the community. Such a high financial penalty would set the Organisation back significantly, and would mean less help for the disadvantaged and the vulnerable;

(b) The Organisation takes its obligations under the PDPA seriously and already had in place various IT security measures and had embarked on a consultancy to ensure its compliance with the PDPA even before the Incident;

(c) The attackers were skilled hackers who utilised sophisticated hacking tools to exploit a weak administrator password for the Tool which left the Database vulnerable to unauthorised access. The Tool was never used by the Organisation's staff and was likely created during the development stage of Database;

(d) Upon being informed of the Incident, the Organisation immediately made a police report and promptly informed various public authorities including the Health Sciences Authority and the Commission. The Organisation has also extended full cooperation and provided prompt responses during the Commission's investigations;

(e) The Organisation promptly informed all affected individuals and there were no registered complaints on the case;

(f) Since the Incident, the Organisation had taken immediate steps to remove the Database from the Website and put in place more security measures. This included layered and restricted access, isolation of sensitive systems at the network level, password training for staff, review and strengthening of standard operating procedures, practising more stringent oversight of vendor actions, implementation of vulnerability assessment and penetration testing regime for critical systems before deployment and on a regular basis annually; and

(g) The financial penalty that the Commissioner intended to impose seemed excessive in light of previous decisions for similar or even more serious breaches.

10 With respect to the representations on the nature and purpose of the Organisation, the fact that the Organisation is a charity cannot be a mitigating factor, and its charitable status cannot lower the standard expected of it in complying with its obligations under the PDPA. The admitted failures on the Organisation's part at [5] clearly fell short of the standard of protection required for the Personal Data stored in the Database.

11 As for the Organisation's representations comparing the present case to previous decisions, it needs only to be said that each decision is based on the unique facts of each case. The decision in each case takes into consideration the specific facts of the case so as to ensure that the decision and direction(s) are fair and appropriate for that particular organisation.

The Commissioner's Directions

12 Having carefully considered the representations, the Commissioner has decided to reduce the financial penalty to the amount set out at [13]. The quantum of financial penalty has been determined after due consideration of the appropriate weight to be given to:

(a) the Organisation's upfront voluntary admission of liability which significantly reduced the time and resources required for investigations under the Expedited Breach Decision procedure;[3] and

(b) the Organisation's comprehensive remedial actions at [9(f)] to address the inadequacies in its procedures and processes that contributed to the Incident.

13. Taking into account all the relevant facts and circumstances, the Commissioner directs the Organisation to pay a financial penalty of $5,000 within 30 days from the date of the 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 the financial penalty until the financial penalty is paid in full. Although a lower financial

[3] See the Commission's *Guide on Active Enforcement* at page 21

penalty has been imposed in this case, this is exceptional and should not be taken as setting any precedent for future cases.

14. In view of the remedial measures taken by the Organisation, the Commissioner has not imposed any other directions.

YEONG ZEE KIN
DEPUTY COMMISSIONER
FOR COMMISSIONER FOR PERSONAL DATA PROTECTION