PERSONAL DATA PROTECTION COMMISSION

Case No. DP-2011-B7351

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

And

Nature Society (Singapore)

SUMMARY OF THE DECISION

1. On 6 November 2020, the Personal Data Protection Commission (the "**Commission**") received information of an online article reporting about hacked databases being made available for downloads on several hacking forums and Telegram channels. In the article, Nature Society (Singapore) (the "**Organisation**") was named as one of the affected Organisations (the "**Incident**").

2. The personal data of 5,131 members and non-members who had created membership and user accounts on the Organisation's website were affected in the Incident. The datasets affected comprised of names, usernames, passwords (encrypted), email addresses, telephone numbers, types of membership, gender, mailing addresses, dates of births, occupation, company and nationality.

3. Following the Incident, the Organisation engaged two IT professionals to carry out an investigation and analysis of the Organisation's website. The investigation and analysis revealed vulnerabilities in the Organisation's website and suspicious SQL injection activities prior to the Incident. The possible attack vector was identified as a SQL injection attack which led to personal data on the Organisation's website database being accessed and exfiltrated by unknown parties.

4. The Organisation took the following remedial measures after the Incident:

   (a) Edited the website to stop all online membership sign-ups/renewals and logins to the website;

   (b) Removed all members' and users' data from the website database;

   (c) Backed up the website database and kept all personal data offline;

   (d) Change all login passwords;

   (e) Notified all affected individuals of the Incident via email;

   (f) Appointed a Data Protection Officer ("**DPO**")

   (g) Developed and implemented a personal data policy; and

   (d) Engaging vendors to develop a new website to improve security.

5. In its representations to the Commission, the Organisation admitted to having breached the Accountability Obligation under sections 11(3) and 12(a) and the Protection Obligation under section 24 of the Personal Data Protection Act 2012 ("**PDPA**"), and requested for the matter to be dealt with in accordance with the Commission’s Expedited Decision Procedure.

Breach of Section 11(3) of the PDPA

6. First, the Organisation admitted it did not designate one or more individuals (typically referred to as a DPO) to be responsible for ensuring that the Organisation complies with the PDPA. The responsibilities of a DPO includes (a) ensuring compliance with the PDPA, (b) fostering a data protection culture, (c) handling and managing personal data queries and complaints, (d) alerting management to any risks with regard to personal data and (e) liaising with the Commission if necessary. From the foregoing, it is clear that the DPO plays a vital role in implementing and building a robust data protection framework to ensure an organisation's compliance with its obligations under the PDPA.

Breach of Section 12(a) of the PDPA

7. Second, the Organisation admitted it did not develop and implement any personal data protection policy prior to the Incident. In this regard, it is important to reiterate that at the very basic level, an overarching personal data protection policy has to be developed and implemented to ensure a consistent minimum data protection standard across an organisation's practices, procedures and activities.

Breach of Section 24 of the PDPA

8. Third, the Organisation admitted that it did not make reasonable security arrangements to protect the personal data on its website database. After the Organisation's website was designed and developed by an external vendor in 2011, the Organisation did not have any contract/retainer agreement with the external vendor to maintain the website's security. As a result, the responsibility of protecting its website fell squarely on the Organisation. However, the Organisation failed to carry out any security measures e.g. conducting necessary security updates, patches and penetration tests, thus leaving its website vulnerable to attacks.

9. In the circumstances, the Organisation is found to have breached sections 11(3), 12(a) and 24 of the PDPA.

Commission's Decision

10. After considering the factors listed at section 48J(6) of the PDPA and the circumstances of this case, including (i) the Organisation's upfront voluntary admission of liability which significantly reduced the time and resources required for investigations; (ii) the fact that the Organisation is a non-profit, registered society and (iii) the Organisation's prompt remedial actions, the Organisation is given notice to pay a financial penalty of $14,000.

11. The Organisation must make payment of the financial penalty within 30 days from the date of the notice accompanying this decision, 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.

12. In view of the remedial actions taken by the Organisation, the Commission will not issue any directions under section 48I of the PDPA.

The following are the provision of the Personal Data Protection Act 2012 cited in the above summary:

Compliance with Act
11(3). An organisation shall designate one or more individuals to be responsible for ensuring that the organisation complies with this Act.

Policies and practices
12(a). An organisation shall develop and implement practices that are necessary for the organisation to meet the obligations of the organisation under this Act.

Protection of personal data
24. An organisation must protect personal data in its possession or under its control by making reasonable security arrangements to prevent –
(a) unauthorised access, collection, use, disclosure, copying, modification or disposal or similar risks and;
(b) the loss of any storage medium or device on which personal data is stored.