National Healthcare Group Pte Ltd

[2019] SGPDPC 46

Yeong Zee Kin, Deputy Commissioner — Case No DP-1802-B1703 and DP-1802-B1765

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

26 December 2019

Introduction

1 On 10 February 2018, the National Healthcare Group Pte Ltd (the "**Organisation**") notified the Personal Data Protection Commission (the "**Commission**") about a complaint it had received in relation to a list containing personal information of partner doctors of the Organisation (the "**List**") which was accessible on the Internet (the "**Incident**"). Subsequently, on 28 February 2018, the Commission received a separate complaint over the Incident.

Facts of the Case

2 On 17 March 2015, the Organisation awarded a developer ("**Website Developer**") a contract to develop its website (the "**Website**"). The Organisation specified the Website's functional requirements and contents. A company specialising in IT services ("**IT Services Provider**") provided the Organisation with IT support. In this regard, the IT Services Provider ensured that the IT specifications of the Organisation were complied with by the Web

Developer, which included coordinating and verifying bug fixes and remedies of security vulnerabilities implemented by the Web Developer. During the process of developing the Website, a section for restricting access to the Website (including the List) was not included in a web configuration file.[1] The Organisation, Website Developer and IT Services Provider signed off on the Website's functional requirements specification, user acceptance test cases, and website commissioning. The relevant web configuration file was not examined before the Website went "live" in December 2015.

3 Around June or July 2016, a vendor (the "**Vendor**") was engaged to conduct a penetration test of the Website. The penetration test report (the "**Penetration Test Report**") highlighted the unrestricted access to the List through the Internet as a vulnerability. The Penetration Test Report also recommended the remedy, which was to ensure that the authorisation rules be configured to restrict Internet access to authorised users only.

4 On 7 February 2018, a general practitioner ("**GP**"), who had signed up to be a partner doctor of the Organisation, found the List through a Google search of her name and notified the Organisation. The List contained personal information of 129 GPs who had registered to be partner doctors of the Organisation via an online form on the Website ("**NHG Partners**"), and personal information of 5 members of public which were generated when they submitted feedback on the Website.

---

[1]Web configuration files determine the way a website or directory on a website behaves. Web configuration files placed in the root directory of a website will affect the behavior of the entire site.

5 The types of information contained in the List (collectively, the "**Disclosed Data**") include:

(a) With respect to the 129 GPs:

(i) their full names (128 GPs), mobile numbers (111 GPs), mailing address (14 GPs), email address (117 GPs) and clinic address (115 GPs) (collectively, "**GP's Contact Information**");

(ii) Singapore Medical Council ("**SMC**") registration numbers of 129 GPs ("**GP's Registration Numbers**"); and

(iii) NRIC numbers (111 GPs), dates of birth (112 GPs) and photographs (41 GPs) (collectively, "**GP's Other Data**").

(b) With respect to the 5 non-GPs, full names and email addresses, as well as mobile numbers of 3 of them ("**Other Individual's Data**").

6 Upon being notified of the Incident on 7 February 2018, the Organisation promptly carried out the following remedial actions:

(a) On 8 February 2018, the Organisation took the Website offline, as well as found and fixed the cause of the Incident;

(b) The Organisation sent several requests to Google to remove cached copies of the List indexed from 9 to 13 February 2018. From 21 February 2018, the Organisation performed daily Google searches on the 129 affected records until the cached links could no longer be found on 5 March 2018. Thereafter, the Organisation conducted periodic Google searches until 8 May 2018; and

(c) From 19 February 2018 to 6 March 2018, the Organisation contacted all affected GPs to inform them of the Incident.

7 In addition, to prevent a recurrence of a similar Incident, the Organisation has also adopted the following practices:

(a) Two additional checks at front-end publishing site for SharePoint websites will be carried out during user acceptance test and prior to going "live":

(i) The project manager would check for configuration which controls publishing of "visible" pages (lists) after the vendor submits the web configuration prior to the deployment; and

(ii) The test script would include testing of authorised access to the relevant web pages. The web pages would also generally be tested to ensure non-public web pages cannot be accessed by non-authorised users.

(b) Performing penetration tests prior to websites going "live".

Findings and Basis for Determination

Whether the Protection Obligation under Section 24 of the PDPA applies to the Disclosed Data

8 While the Disclosed Data is personal data as defined in section 2(1) of the Personal Data Protection Act 2012 ("**PDPA**"), the Protection Obligation under section 24 did not apply to the following 2 categories of Disclosed Data – GP's Contact Information and GP's Registration Numbers.

9 In relation to GP's Contact Information, pursuant to section 4(5) of the PDPA, Parts III to VI of the PDPA do not apply to business contact information. GP's Contact Information falls within the definition of "business contact information" as defined in section 2(1) of the PDPA because it was provided by the GPs to the Organisation for the purposes of registration as NHG Partners, and as a means of contacting them in their professional capacity.

10 In relation to GP's Registration Numbers, the same information is generally available to the public on the SMC website and hence it is "publicly available" as defined in section 2(1) of the PDPA. The raison d'etre for making such information available is to assist in the identification of licensed medical practitioners and the nature of their qualification and practice. The register of medical practitioners is maintained by the Singapore Medical Council under section 19 of the Medical Registration Act. It is maintained as multiple lists, i.e., locally-trained doctors, international medical graduates, provisional, conditional, temporary or full registrations, as well as specialist registration and family physician registration. This information enables an inquisitive patient to verify the nature of medical practice that a physician is permitted to practice. To my mind, this is information that falls under the "other similar information about the individual" limb of the definition of business contact information as it assists in the identification of the medical practitioner to whom the business contact information relates.

11 In the circumstances, the Protection Obligation only applied to GP's Other Data and Other Individual's Data (collectively, the "**Disclosed Personal Data**").

Whether the Organisation had breached the Protection Obligation under section 24 of the PDPA

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

13 As a preliminary point, the Organisation owned the Website and had possession and control over the Disclosed Personal Data at all material times. While the Website Developer was engaged to develop the Website and the IT Services Provider provided IT support to the Organisation (including maintenance and technical support for the Website), the investigations revealed that neither of these parties processed the Disclosed Personal Data on the Organisation's behalf with respect to the Website. The IT Service Provider and Website Developer were accordingly not data intermediaries with respect to the operation of the Website, and the Organisation was solely responsible for the protection of the Disclosed Personal Data.

14 Based on the investigations, the Organisation had failed to put in place reasonable security arrangements to protect the Disclosed Personal Data as explained below.

15 The Penetration Test Report expressly pointed out that web services could be used to access SharePoint data (which included the List containing the Disclosed Personal Data) via the Internet and recommended that this vulnerability be remediated by reconfiguring the web configuration to restrict access to authorised users only. The Penetration Test Report was issued more than a year prior to the Incident. This was more than sufficient time for the Organisation to remedy the vulnerability which caused the Incident.

16 According to the Organisation, the vulnerability was inadvertently left unfixed as it was not sufficiently highlighted by the Vendor in the Penetration Test Report. This was an unsatisfactory excuse. First, the relevant findings and recommendations were the first item in the Penetration Test Report. Second, they were expressed in terms that no technical expertise was required for their significance to be understood. If the Organisation did not understand the findings and/or recommendations, it should have consulted the Vendor for clarifications.

17 The Organisation also asserted that it had relied on IT Services Provider and Website Developer to act on any issues identified in the Penetration Test Report. It should be reiterated that while an organisation may delegate work to vendors to comply with the PDPA, the organisation's responsibility for complying with its statutory obligations under the PDPA may not be delegated.[2] In this case, the Organisation failed to exercise reasonable oversight with respect to the review of the Penetration Test Report and rectification of the vulnerabilities of its Website.

Representations by the Organisation

18 In the course of settling this decision, the Organisation made representations and asked that a warning to be imposed in lieu of a financial penalty. The Organisation raised the following factors in its representations:

(a) As the appointed public healthcare shared services provider, the IT Services Provider was responsible for the overall management,

[2] See *WTS Automobile Services Pte Ltd* [2018] SGPDPC 26 at [14] and [23].

deployment and maintenance of the Organisation's IT systems, including the Website. Similar to the facts of *Re Singapore Health Services Pte Ltd & Ors* [2019] PDPC 3, the IT Services Provider's staff was deployed to the Organisation to support day-to-day operations and provide technical support. As there was no IT staff employed by the Organisation, it had to rely on the technical expertise provided by the IT Services Provider. In particular, the Chief Information Officer ("**CIO**") and Cluster Information Security Officer ("**CISO**") for the Organisation was employed by the IT Services Provider and seconded to the Organisation;

(b) The IT Services Provider was a data intermediary. The Website's database was hosted on the Healthcare Data Centre (H-Cloud) network which was (and is still) operated, maintained and managed by the IT Services Provider;

(c) The IT Services Provider was in charge of the penetration test, as well as coordinating and deploying the fixes. The vulnerability on the Website that caused the Incident was not highlighted to the Organisation; and

(d) The Disclosed Personal Data was not medical data, and therefore not personal data of a particularly sensitive nature which should be accorded a higher standard of protection.

19 Having considered the representations, I have decided to maintain the financial penalty set out in [21] for the following reasons:

(a) While the IT Services Provider's staff deployed to fill the CIO and CISO role may have been employed by the IT Services Provider, to

the extent that they were carrying out the functions of the Organisation's CIO and CISO in accordance to the terms of their secondment, they were acting on behalf of the Organisation. As such, I find that their actions should be attributed to the Organisation and not the IT Services Provider;

(b) The Incident did not arise from a compromise of the Healthcare Data Centre (H-Cloud) network that hosted the Website's database. Instead, and as mentioned at [2], the cause of the Incident was that a section for restricting access to the Website (including the List) was not included in a web configuration file. While the IT Services Provider provided technical support for the Website, it did not process the Disclosed Personal Data through the Website. The IT Services Provider was accordingly not a data intermediary with respect to operation of the Website;

(c) As explained at [15] to [17], the Organisation failed to exercise reasonable oversight with respect to review of the Penetration Test Report and rectification of vulnerabilities of the Website. In this regard, the Penetration Test Report had expressly pointed out that web services could be used to access SharePoint data (which included the List containing the Disclosed Personal Data) and recommended that this vulnerability be remediated by reconfiguring the web configuration to restrict access to authorised users only; and

(d) The fact that the Disclosed Personal Data was not medical data had already been taken into account in the quantum of financial penalty set out in [21], which would have been higher if the Disclosed Personal Data had been of a more sensitive nature, such as medical data.

Directions

20 In determining the directions, if any, to be imposed on the Organisation under section 29 of the PDPA, I took into account the following mitigating factors:

(a) the Organisation took prompt remedial actions following the Incident as set out in [6] and [7];

(b) the Organisation was fully cooperative during the investigations;

(c) the Organisation took immediate steps to notify the affected individuals of the Incident; and

(d) there was unauthorised disclosure to one individual and no modification or exfiltration of the Disclosed Personal Data.

21 Having considered all the relevant factors of this case, I hereby direct the Organisation to pay a financial penalty of $6,000 within 30 days from the date of the directions, 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. I have not set out any further directions for the Organisation given the remediation measures already put in place.
