PERSONAL DATA PROTECTION COMMISSION

[2022] SGPDPCS 15

Case No. DP-2010-B7246

In the matter of an investigation under section 50(1) of the

Personal Data Protection Act 2012

And

Thomson Medical Pte. Ltd.

SUMMARY OF THE DECISION

1. On 26 October 2020, the Personal Data Protection Commission (the **"Commission"**) was notified that the Thomson Medical Pte. Ltd. (the **"Organisation"**) Health Declaration Portal was not secure, enabling public access to the personal data of visitors (the "**Incident**") stored in a **CSV** (comma separated values) file.

2. Visitor data collected on the Organisation's Health Declaration Portal had been stored concurrently in a publicly-accessible CSV file as well as a secured

database from 16 April 2020, when the health declaration portal was first used by the Organisation to 8 September 2020, when the storage of the visitor data was changed to only the secured database instead of the CSV file. The CSV file was hosted on the Organisation's web server.

3. The Organisation admitted that, contrary to the instructions given to the employee to switch the data storage from the CSV file to secured database exclusively, and the organisation's protocols, its in-house developer had omitted to remove a software code, causing the visitor data to be stored in the CSV file and the same in-house developer had omitted to change the default web server configuration, thereby allowing public access to the hosted CSV file. The switch to storage in a secured database would have ensured access controls by requiring user login ID and secure password protection, as well as encryption of data transfers using SSL certificates. The access controls would ensure that only authorized users would be able to access the data.

4. The Commission's investigations revealed that the affected CSV file contained the personal data of 44,679 of the Organisation's visitors, including the date and time of visit, temperature, type of visitor (purpose of visit), name of visitor, name of newborn, contact number, NRIC/FIN/passport number, doctor/clinic name or room visiting, and answers to a health declaration questionnaire (which included a declaration by the visitor that he/she did not have any symptoms or recent exposure to the Covid-19 virus).

5. The Organisation accepted that it was in breach of the Protection Obligation under section 24 of the Personal Data Protection Act ("PDPA"). The Commission finds that the Organisation had breached section 24 of the PDPA for two reasons.

6. First, even though the Organisation's existing policies required the visitor data collected to be stored in a secured database, the Organisation failed to ensure that there were processes in place to ensure these policies and instructions would be complied with. The Organisation stated that the in-house developer had been the only staff in its IT department familiar with the programming language used for the health declaration form. This, however, should not have prevented the Organisation, as an example, from requiring the in-house developer to demonstrate to another staff member, and for that staff member to verify that the storage instructions had been complied with. As noted in *Re Aviva Ltd* [2017] SPDPC 14, relying solely on individual employees to perform their tasks diligently, with no oversight or supervision, is not a reasonable security arrangement.

7. Second, the Organisation failed to conduct reasonable pre-launch testing before the Health Declaration Portal went live. While acceptance testing and some technical tests were conducted, there had been no security testing to verify that there were access controls to the visitor data collected.

8. Having said that, it is a mitigating fact that the Organisation's in-house developer sought to comply with the Organisation's policies and swiftly rectified the software code on 8 September 2020, when he first discovered the coding error whilst updating the health declaration questionnaire.

9. The forensic investigator engaged by the Organisation did not uncover any evidence that the disclosed data had been exported and posted online, including on the Dark Web. The Organisation's server logs also revealed that the CSV file was only accessed 4 times from 3 different local IP addresses. Given the timing of the access instances, it is probable that these instances were made by the complainant and by the Commission when investigating this matter, which suggests that the impact of this Incident was limited.

10. The Commission noted a parallel between the facts of this case and *Re Spear Security Force Pte. Ltd.* [2016] SGPDPC 12, in that both cases arose from a single complaint about a potential breach of the PDPA, with no other evidence suggesting that the personal data had actually been exposed to unauthorised third parties due to the lapses by the Organisation.

11. The personal data exposed here included the clinic or room that the individual intended to visit, and the reason for the visit. This could be to seek treatment, accompany a patient, or a business visit made by a sales representative of a pharmaceutical or medical device company. While the personal data exposed

included some health-related information, this had essentially been health declaration information for the purpose of containment of the pandemic. The information did not in fact reveal any potentially sensitive information such as whether the visitor was Covid-19 positive.[1]

12. The personal data disclosed is also not on par with *Re Singapore Health Services Pte. Ltd.& Ors.* [2019] SGPDPC 3 ("Singhealth"). In the Singhealth case, we recognised the sensitivity involved in the exposure of the affected individuals' personal data in their "clinical episode information, clinical documentation, patient diagnosis and health issues and Dispensed Medication Records" as the information and personal data affected may allow one to deduce the condition for which a patient had sought treatment, and may lead to the unintended disclosure of serious or socially embarrassing illnesses.[2] While there is some personal data in the present case which may reveal the clinic which an affected individual had sought treatment, this is of a much more limited scope as compared to the Singhealth case.

13. The Commission accepted that the Organisation took prompt remedial action to contain the exposure. This include removing the affected CSV file and changing all the passwords to the database, even though it was not affected by the Incident. To prevent a recurrence of a similar incident, the Organisation also

[1] Cf *Re Terra Systems Pte Ltd* [2021] SGPDPC 7.
[2] See *Re Singapore Health Services Pte. Ltd.& Ors.* [2019] SGPDPC 3, at [139].

reviewed its application deployment process to take into consideration data security, and rectified all potential gaps discovered during a vulnerability scan.

14. Given the lack of evidence suggesting that personal data had actually been exposed to unauthorised third parties due to the lapses by the Organisation and the limited impact of the Incident, the Commission considered that it would be most appropriate in lieu of imposing a financial penalty, to impose directions.

15. Another factor which prompted the Commission to impose directions in lieu of a financial penalty was the fact that at the material time, such health declaration information was widely collected across the island. There was also a corresponding acceptance and support from members of the public of the need for the collection of such health declaration information in order for the relevant authorities to effectively respond to and control the potential spread of COVID-19.

16. Given the above, the Commission directs the Organisation to carry out the following within 60 days:

    a. In relation to the Organisation's remedial action of reviewing its application deployment process to take into consideration data security,

        i. The Organisation shall ensure that the intended measures include arrangements for reasonable pre-launch security testing

to be conducted before the launch of any new website, application, portal or other online feature for the processing of personal data; and

ii. The Organisation shall ensure that the intended measures include the development and implementation of a data retention policy to meet the Retention Limitation Obligation under section 25 of the PDPA.

b. In relation to the Organisation's remedial action of scanning the Dark Web for evidence of exfiltration of the personal data,

i. The Organisation shall conduct a scan of the Clear/Surface Web, as well as a renewed scan of the Dark Web to confirm that there is no evidence of publication of the affected personal data online.

c. By no later than 14 days after the above actions have been carried out, the Organisation shall submit to the Commission a written update providing details of the actions taken.

The following provision(s) of the Personal Data Protection Act 2012 had been cited in the above summary:

Protection Obligation

24(a) Failure to 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, disposal or similar risks