PERSONAL DATA PROTECTION COMMISSION

[2021] SGPDPC 7

Case No DP-2007-B6670

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

And

Terra Systems Pte. Ltd.

… *Organisation*

DECISION

Data Protection *– Protection obligation – Unauthorised access to personal data – Insufficient security arrangements – Failure to implement reasonable access controls*

Terra Systems Pte. Ltd.

[2021] SGPDPC 7

Lew Chuen Hong, Commissioner — Case No. DP-2007-B6670

6 August 2021

[Editorial note: An application for reconsideration was filed against this decision. In Terra Systems Pte Ltd [2022] SGPDPCR 1, the Commissioner affirmed the finding of the organisation's breach of section 24 of the PDPA and the financial penalty imposed.]

Introduction

1 On 14 July 2020 and 21 July 2020, a customer relationship management portal ("**the Portal**") owned and operated by Terra Systems Pte Ltd (the "**Organisation**") containing the personal data of persons served with "Stay-Home Notices" [1] ("**SHNs**") was accessed and modified without the Organisation's authorisation (the "**Incident**").

2 On 27 July 2020, the Singapore Police Force notified the Personal Data Protection Commission ("**Commission**") of the Incident, and the Commission commenced its own investigations thereafter.

Background

3 The Organisation is in the business of providing communication solutions and services, including call centre services, to businesses in Singapore and the region. On 17 June 2020, the Organisation was awarded a government contract to provide call centre services to help verify the whereabouts of persons serving SHNs ("**the Call Centre**").

[1] Legal notices issued under the Infectious Diseases Act (Cap 137) requiring a person to remain at their place of residence or at a Stay-Home Notice Dedicated Facility at all times for a stipulated period

4 To facilitate the operations of the Call Centre, the Immigration and Checkpoints Authority ("**ICA**") provided the Organisation with a daily spreadsheet containing the personal data of persons serving SHNs, including their:

(a) Name

(b) Last 4 digits of NRIC;

(c) Gender;

(d) Contact Number;

(e) Last Day of SHN;

(f) Address where SHN was served; and

(g) COVID-19 Test Appointment dates

(collectively, the "**SHN Data**")

5 The Organisation created the Portal for the purposes of its internal administration of the Call Centre. On account of the movement restrictions in force at the time owing to the COVID-19 pandemic, the Portal was designed to be accessible by the Organisation's staff from home via the Internet.

6 Users in the Organisation were granted different levels of access to the Portal:

(a) Directors and managers were assigned unique user IDs and passwords and were able to view all cases in the Portal.

(b) Team leaders were also assigned unique user IDs and passwords and were able to view all cases assigned to agents in their teams.

(c) Agents (i.e. the persons actually contacting the persons serving SHNs) were temporary staff assigned simple user IDs based on their respective teams (e.g. the user ID "D03" referred to agent number 3 in team D). Agents were also given a common

daily password which was shared with them during a morning Zoom briefing by the Organisation's management.

7 Agents logged in to the Portal were only able to view the cases assigned to them, and type in remarks in a specific "remarks" column after a case had been attended to. At the end of each day, the SHN Data would be submitted to ICA with the agents' remarks, and all data in the Portal would be purged.

8 On 14 July 2020, crude remarks were found to have been inserted in the remarks field of 3 cases in the Portal. The two agents assigned to deal with those cases and their team leader denied inserting the remarks. The Organisation changed the common password for the day and began informing agents of the new daily common password via Whatsapp instead. The Organisation also implemented a web server logging function to track the actions of users logged in to the Portal. This functionality had not enabled previously.

9 On 21 July 2020, another crude remark was inserted in the remarks field of a case assigned to one of the same agents. The Organisation traced the action to an unauthorized user based on the IP address from which the Portal was accessed and reported the Incident to the police.

10 The perpetrator of the Incident is believed to be a disgruntled ex-employee of the Organisation. On 14 July 2020, the perpetrator is believed to have obtained the daily common password by attending the morning Zoom briefing, after obtaining the login details for the morning Zoom briefing from other employees. On 21 July 2020, the perpetrator is believed to have directly obtained the daily common password from another employee who was unaware that his employment had been terminated.

11 After being notified of the Incident, the Organisation took the following remedial actions on ICA's instructions:

(a) The practice of using common passwords was ceased, and agents were required to adopt unique passwords,

(b) Agents were assigned unique user IDs which were different from the generic IDs based on their teams;

(c) Two-factor authentication was implemented for all access to the Portal; and

(d) Security scanning was performed on the Portal.

Findings and Basis for Determination

Whether the Organisation had contravened 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 ("**Protection Obligation**").

13 For the reasons set out below, the Organisation is found to have failed to implement reasonable security arrangements to protect the SHN Data from the risk of unauthorised access.

Failure to implement reasonable IT access controls

14 Firstly, the Organisation failed to implement reasonable IT access controls to the SHN Data in the Portal. The use of (i) generic user IDs for agents which were known to all or guessable, and (ii) a daily common password for all agents, were poor practices that posed serious security risks.

15 Employing simple user IDs and a common password defeated the purpose of segregating agents' access to cases in the Portal. Any agent could have accessed another agent's cases by using that agent's commonly known or guessable user ID and the common password. While there is only evidence that the perpetrator in this case accessed *and modified* the SHN Data of 4 persons (based on the distinct cases in the Portal in which crude remarks were inserted), the perpetrator *could* have accessed the SHN Data of all 125 persons assigned to his former team.

16 The Incident could have been prevented had all agents been assigned unique user IDs and passwords.

Failure to implement policies to mitigate risks from using common password

17 Secondly, the Organisation failed to implement adequate policies to mitigate the risks created by the use of a daily common password to access the Portal. Having made the decision to use a common password for access to the Portal, the Organisation attempted to identify the associated risks and adopt suitable policies and practices. Unfortunately, their efforts proved to be inadequate

18 The Organisation clearly recognised some risks associated with use of a common password – this was why they adopted the *practice* of changing the common password daily. However, it was foreseeable that agents would ask each other for the daily common password, for example, when they had forgotten the password or had missed the morning Zoom briefing. An agent may not have suspected that anything was amiss if someone they believed to be another agent had asked them for the daily password or the login details for the morning Zoom briefing. This risk was exacerbated by the fact that all of the agents were temporary staff and that personnel changes were to be expected. Thus, on both 14 July 2020 and 21 July 2020, the perpetrator is believed to have obtained either the login details for the morning Zoom briefing or the common daily password itself from the Organisation's employees.

19 If the Organisation had properly appreciated this risk, it could have implemented policies (i) prohibiting agents from disseminating or sharing the daily common password under any circumstances, and (ii) requiring any agents who missed the daily morning Zoom briefings to obtain the daily common passwords directly from their team leaders or managers, who would be better placed to verify the requestor's employment status. Admittedly, such policies would have been difficult to police. However, they would have at least reduced the risk of disclosure of the common password to unauthorised persons.

20 It is acknowledged that the Organisation was under pressure to operationalise the Call Centre and Portal within a short timeframe to support ICA's operations in the midst of the

COVID-19 pandemic. Even so, its failures to implement reasonable access controls gave rise to the present Incident. The Organisation failed to make reasonable security arrangements to protect the SHN Data from unauthorised access and modification in breach of its obligation under section 24 of the PDPA.

The Commissioner's Decision

21 In determining whether any directions should be imposed on the Organisation under section 48I of the PDPA, and/or whether the Organisation should be required to pay a financial penalty under section 48J of the PDPA, the factors listed at section 48J(6) of the PDPA were considered, with particular emphasis on the following aggravating and mitigating factors:

Aggravating Factor

(a) The SHN Data was sensitive in nature considering the climate of the COVID-19 pandemic and unauthorised disclosure could have caused the individuals to experience discrimination or social stigma;

Mitigating Factors

(b) The Organisation had to operationalise the Portal under urgent circumstances;

(c) The Organisation took prompt remedial actions following the Incident; and

(d) The Organisation was cooperative during the investigations.

22 Having considered the above factors and circumstances, the Commissioner preliminarily determined that a financial penalty of $12,000 would be imposed in respect of the Organisation's negligent contravention of the Protection Obligation. On 22 April 2021, the Organisation was notified of the Commissioner's preliminary decision, including the full findings set out above, and given 14 days to make written representations.

The Organisation's representations

23 On 7 May 2021, the Organisation submitted written representations requesting that it be issued a warning in lieu of a financial penalty. While the Organisation did not dispute that it had breached the Protection Obligation, it claimed that the circumstances of its case were similar or less egregious to recent enforcement decisions of the Commission in which warnings had been given to organisations for breaches of the Protection Obligation[2].

24 According to the Organisation, unlike in the precedent cases cited:

(a) Only 4 individuals' personal data was affected in the Incident (i.e. a very low number);

(b) The personal data affected (i.e. the SHN Data) was not sensitive;

(c) There was no exfiltration or public exposure of the SHN Data;

(d) Prompt remedial measures were implemented within 48 hours with no loss of personal data; and

(e) Reports were voluntarily made to the authorities (including ICA and the police) and the Organisation was not held to ransom or complained about by any members of the public.

25 The Organisation also claimed that unauthorised disclosure of the SHN Data would not have caused the affected individuals to experience discrimination or social stigma. The Organisation claimed that it was normal for anyone entering Singapore at the time to be subject to an SHN, and that many persons had even publicised this fact. With reference to the precedent cases cited, the Organisation claimed that the disclosure of (i) students' grades, (ii) church members' marital statuses, and (iii) employees' salaries, carried a greater risk of the affected persons experiencing discrimination or social stigma in the relevant circumstances.

[2] Chan Brothers Travel Pte Ltd (DP-1905-B3936, Summary of the Decision); Horizon Fast Ferry Pte Ltd (DP-1912-B5464, Summary of the Decision); MRI Diagnostics Pte Ltd (DP-1811-B2975, Summary of the Decision); Water+Plants Lab Pte Ltd (DP-2004-B6182, Summary of the Decision); R.I.S.E Aerospace Pte Ltd (DP-2007-B6832, Summary of the Decision); Everlast Projects Pte Ltd [2020] SGPDPC 20; Chapel of Christ the Redeemer (DP-2010-B7132, Summary of the Decision); St Joseph's Institution International Ltd (DP-2010-B7196, Summary of the Decision); and ACCA Singapore Pte Ltd (DP-2011-B7385, Summary of the Decision).

26 After careful consideration, the Organisation's representations were rejected.

27 While there may have been facts in specific domains of the precedent cases which appeared either similar or more egregious than the Incident, this did not mean that the Organisation was deserving of a warning. Every case is decided based on an evaluation of *all* the relevant facts and circumstances, and in a manner that is fair and appropriate for the particular organisation investigated.

28 There are two main distinguishing factors which justifies the imposition of a financial penalty in the Organisation's case compared to the precedent cases cited:

(a) First, contrary to the Organisation's representations, the SHN Data is considered to have been sensitive at the material time, during the early days of the COVID-19 pandemic when there was uncertainty about its virulence and high levels of public health concerns. The Organisation was engaged to help administer the SHN regime as part of a national effort to manage the pandemic. While the SHN Data did not include positive diagnoses for COVID-19, the fact of being subject to an SHN nevertheless denoted risk of exposure to the virus. The fact that the Incident occurred in July 2020 just after the end of "circuit breaker" measures and when public concern was high, was important context.

(b) Second, within the same context of a national health emergency, the Organisation's level of culpability was much higher than that of the organisations in the cited precedents. The Organisation employed very poor access control measures which were easily circumvented by an unsophisticated actor. A common password was used by over 50 users and shared over an unsecure platform, with no audit trail. While the Organisation's representations focused solely on the alleged harm caused by the Incident and the remedial steps taken afterwards, the extent of the Organisation's negligence in the Incident was also an important factor which justified the imposition of a financial penalty in its case.

29 For completeness, the Organisation's representations also failed to account that the personal data of 125 individuals was exposed to the risk of unauthorised access in the Incident, notwithstanding that only 4 records had been modified. In any event, the fact that the Incident only affected a limited number of persons has been taken into account in calibrating the quantum of the financial penalty imposed. Other factors raised by the Organisation such as the prompt implementation of remedial measures and voluntary reporting have similarly been accounted for.

30 Having considered all the relevant factors of this case, the Commissioner hereby requires the Organisation to pay a financial penalty of $12,000 within 30 days from the date of the relevant 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.

31 In view of the remedial actions that have already been taken by the Organisation, no other directions are necessary.

YEONG ZEE KIN
DEPUTY COMMISSIONER
FOR COMMISSIONER FOR PERSONAL DATA PROTECTION