PeopleSearch Pte. Ltd.

[2019] SGPDPC 47

Yeong Zee Kin, Deputy Commissioner — Case No DP-1903-B3521

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

26 December 2019

Introduction

1 PeopleSearch Pte. Ltd. (the "**Organisation**") is a subsidiary of a listed Singapore company ("**Listed Company**") that provides professional recruitment and flexible staffing services in Asia. On 15 March 2019, the Listed Company notified the Personal Data Protection Commission (the "**Commission**") of a ransomware attack suffered by the Organisation on 1 to 2 March 2019, which resulted in the Organisation not being able to access its clients' personal data (the "**Incident**").

Facts of the Case

2 At the material time, the Organisation had a business division that managed outsourced payroll for the Organisation's clients. In order to do so, the Organisation used a payroll software installed in a server in a virtual machine environment (the "**VM Server**"). The Organisation's clients would connect to the VM Server through remote desktop protocol to use the payroll software. All the information (including personal data) in the payroll software was stored in a database that was hosted in the VM Server.

3 At the time of the Incident, the database included the following personal data of 472 individuals employed by 2 of the Organisation's clients[1] (collectively, "**Employee Data**"):

(a) Name;

(b) NRIC number;

[1] The payroll information of the Organisation's other clients had been migrated from the VM Server to another server. This was in preparation for the Organisation's business division managing outsource payroll being incorporated into a separate legal entity.

(c) Residential address;

(d) Contact number;

(e) Email address;

(f) Bank account number; and

(g) Salary details.

4 The database also included the following personal data of the employees' next of kin ("**Next of Kin Data**")[2]:

(a) Name;

(b) Age;

(c) Contact number; and

(d) Relationship to the respective individual.

5 Taking into consideration the individuals whose information were stored as Next of Kin Data, it is estimated that a total of 944 individuals (comprising the 472 individuals with Employee Data and 472 individuals with Next of Kin Data) were affected by the Incident (the "**Affected Individuals**").[3]

6 The Organisation discovered the Incident on 4 March 2019 when a ransom note appeared when it attempted to access the VM Server. The ransom note informed the Organisation that its files had been encrypted, and required payment in Bitcoins in exchange for the decryption key. The Organisation refused to pay the ransom to the cyber-attacker and restored its business operations by using a backup of the VM Server as at 1 March 2019.

[2] Some or all of the Next of Kin Data may also constitute Employee Data in that it may be data about the employee (namely, who is their next of kin) which may enable the employee to be identified. However, as the total number of Affected Individuals includes both the employees and their next of kin, the two sets of data are identified separately for the purposes of this Decision.

[3] The Organisation was unable to provide the Commission with the number of individuals who were listed as "next of kin" in the payroll information of the 472 individuals as it was no longer in possession of the relevant customer data file. It is estimated that each of the 472 individuals would have provided Next of Kin Data of at least 1 individual.

7 Upon discovery of the Incident, the Organisation promptly carried out the following remedial actions:

(a) Disabled remote desktop accounts and/or changed passwords to mitigate any risks relating to credentials; and

(b) Installed the latest windows server updates on the restored VM Server.

8 Based on the Organisation's internal investigations, there was no spike in the outgoing traffic logs from the VM Server at the time of the Incident. This suggested that the risk that Employee Data (including the Next of Kin Data) was exfiltrated by the cyber-attacker was immaterial. On 1 April 2019, the Organisation's business division managing outsource payroll was incorporated into a separate legal entity and the VM Server was decommissioned.

Findings and Basis for Determination

Whether the Organisations had breached section 24 of the PDPA

9 It is undisputed that Employee Data and Next of Kin Data constitutes "personal data" as defined in section 2(1) of the Personal Data Protection Act 2012 (the "**PDPA**"). The Organisation had possession and/or control over the Employee Data and Next of Kin Data at all material times, and accepted its responsibility for protecting such data under the PDPA. While there may have been no exfiltration of the Employee Data, as mentioned at [8], there was unauthorised modification of the Employee Data as the ransomware rendered it inaccessible to the Organisation.

10 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. In assessing the standard of reasonable security arrangements required, I considered the fact that Employee Data included NRIC numbers and personal data of a financial nature (i.e. bank account numbers and salary details).[4] When it comes to the protection of such personal data, there is a need to put in place stronger security measures because of the actual or potential harm, and the severity of such harm, that may befall an individual from an unauthorised use of

[4] *Re Aviva Ltd* [2018] SGPDPC 4 at [17]

such data.[5] In my view, the Organisation failed to put in place reasonable security arrangements to protect the Employee Data and Next of Kin Data for the reasons explained below.

11 The Organisation admitted that it had not carried out any security scans, penetration testing or patching of the VM Server for at least 12 months preceding the Incident. According to the Organisation, its omission was due to a departure of an employee who was responsible for oversight of the VM Server. This explanation is not accepted.

12 As emphasized in previous decisions and the Commission's Guide to Securing Personal Data in Electronic Medium (revised 20 January 2017) at [16.3] and [16.4], regular security testing and patching of IT systems are important security measures that organisations should implement to guard against a possible intrusion or attack.[6] The Organisation's failure to have any process in place to ensure regular security testing and patching of the VM Server resulted in a system that had vulnerabilities and gaps that were exploited by the attacker in planting the ransomware to encrypt the Employee Data. In view of the fact that the VM Server stored personal data of a sensitive nature, this fell far short of the standard of protection required. In the circumstances, I find the Organisation in breach of Section 24 of the PDPA.

13 Nevertheless, I note that the Organisation had a good practice of having regular backups of the VM Server. This significantly mitigated the impact of the Incident on the Organisation's business operations. The Organisation was able to restore the VM Server from a backup as at 1 March 2019, and only lost access to the Employee Data for approximately 2 days from 2 March 2019 to 4 March 2019.

14 In today's digital age where organisations store information (including personal data) online and move towards a paperless future, it is critically important that they have processes in place to backup their data at frequent and regular intervals. The failure to do so may result in crippling consequences to an organisation's business operations in the event of a cyberattack. In this case, the Organisation's good practice of having regular backups is a strong mitigating factor that I have taken into account in determining the quantum of financial penalty to impose.

[5] *Re Credit Counselling Singapore* [2017] SGPDPC 18 at [25]
[6] See for example *Re Genki Sushi Singapore Pte Ltd* [2019] SGPDPC 26 at [20] and [21]

The Deputy Commissioner's Directions

15 Having found the Organisation in breach of section 24 of the PDPA, I took into account the following mitigating factors in determining the directions to be imposed on the Organisation:

(a) the Organisation's regular backup process of the VM Server which significantly mitigated the impact of Incident as discussed at [13] and [14];

(b) The Organisation's prompt actions to mitigate the effects of the Incident and prevent recurrence of a similar breach;

(c) The Organisation's full cooperation with the Commission's investigations;

(d) There did not appear to be any exfiltration of Employee Data from the VM Server; and

(e) The Commission did not receive any complaints about the Incident and there was no indication that the Incident caused harm to the Affected Individuals.

16 Having considered all the relevant facts and circumstances of this case, I hereby direct the Organisation to pay a financial penalty of $5,000 within 30 days from the date of this 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 such financial penalty until the financial penalty is paid in full.