PERSONAL DATA PROTECTION COMMISSION

[2020] SGPDPC 21

Case No. DP-2006-B6426

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

And

Singapore Technologies Engineering Limited

… *Organisation*

DECISION

Singapore Technologies Engineering Limited

[2020] SGPDPC 21

Yeong Zee Kin, Deputy Commissioner — Case No. DP-2006-B6426

16 November 2020

Introduction

1 On 10 June 2020, Singapore Technologies Engineering Limited (the "**Organisation**") notified the Personal Data Protection Commission (the "**Commission**") that its subsidiary based in the United States of America ("**USA**"), VT San Antonio Aerospace Inc. ("**VT SAA**"), had discovered a cybersecurity incident where threat actors gained unauthorised access to VT SAA's US-based IT network and deployed a ransomware attack (the "**Incident**").

Facts of the Case

2 The Organisation is a Singapore incorporated company with a network of subsidiaries in Asia, Europe, USA and the Middle East. The ransomware attack was isolated to a limited part of VT SAA's network, but also affected a few of the Organisation's subsidiaries based in the USA that were using IT shared services provided by VT SAA. The Organisation's IT network in Singapore was not compromised during the Incident. However, the following types of personal data belonging to 287 individuals in Singapore ("**Affected**

Individuals") were potentially exposed to the risk of unauthorised access (collectively, the "**Personal Data Sets**")[1]:

(a) Name;

(b) Address;

(c) Email address;

(d) Telephone number;

(e) NRIC number and date of issue;

(f) Passport details;

(g) Photograph;

(h) Date of birth;

(i) Citizenship;

(j) Country of residence;

(k) Place of birth;

(l) USA Social Security number;

(m) USA visa information;

(n) Details regarding government or military service, where applicable;

(o) CV information;

(p) Foreign identification numbers;

(q) Government issued identification (ID) information;

---

[1] This list sets out the personal data types potentially affected in the Incident. Not all of these types of personal data were affected for each Affected Individual, and the type(s) of personal data affected for each Affected Individual varies. The Personal Data Sets of 49 Affected Individuals were assessed to have been "likely exfiltrated", with the remaining Personal Data Sets were assessed to have been "likely affected, may have been exfiltrated".

(r) Associated information about minors; and

(s) Employee status.

3 In this regard, the Affected Individual's Personal Data Sets had been transferred from the Organisation (in Singapore) to VT SAA and the Organisation's other subsidiaries (based in the USA). The purposes of the transfer included making regulatory filings with the USA authorities, secondment or transfers of employment and security clearance in connection with visits to facilities.

4 Upon discovery of the Incident, the Organisation and VT SAA immediately took the following remedial actions:

VT SAA

(a) Notified the federal law enforcement officials in USA;

(b) Immediately disconnected certain systems from the network and retained leading third-party forensic advisors to investigate the Incident;

(c) Conducted a rigorous review of the Incident and its systems, including deploying advance tools to remediate the intrusion and to restore the affected systems;

(d) Strengthened its overall cybersecurity architecture, including enhanced endpoint security controls, additional network monitoring and other security hardening measures; and

(e) Implemented a Security Operations Centre to provide 24/7 monitoring, detection and response capabilities.

The Organisation

(f) Reprioritised and accelerated its existing IT harmonisation plan (including the enhancement and hardening of internal controls and external program elements) for all its entities.

Findings and Basis for Determination

5 As a preliminary point, the data protection obligations in the Personal Data Protection Act 2012 ("**PDPA**") did not apply to VT SAA and the Organisation's other subsidiaries (based in the USA) with respect to the Incident. This is because they did not carry out any activities in relation to the collection, use or disclosure of the Affected Individual's Personal Data Sets in Singapore. The Commission will defer to the ongoing investigations by the US federal law enforcement officials into VT SAA and the Organisation's subsidiaries based in the USA. The Commission's investigations in the present case focused on whether the Organisation's transfer of the Affected Individual's Personal Data Sets from Singapore to the USA met the requirements under the PDPA.

The Transfer Limitation Obligation under Section 26 of the PDPA

6 Section 26(1) of the PDPA provides that an organisation shall not transfer any personal data to a country or territory outside Singapore except in accordance with requirements prescribed under the PDPA to ensure that organisations provide a standard of protection to personal data so transferred that is comparable to the protection under the PDPA (the "**Transfer Limitation Obligation**"). The relevant requirements are prescribed in Part III of the Personal Data Protection Regulations 2014 ("**PDPR**"). In particular:

(a) Regulation 9(1)(b) of the PDPR requires an organisation that transfers personal data to a country or territory outside of Singapore to take appropriate steps to ensure that the recipient of personal data is bound by legally enforceable obligations (in accordance with Regulation 10) to provide to the transferred personal data a standard of protection that is at least comparable to that under the PDPA;

(b) Regulation 10(1)(c) of the PDPR provides that such legally enforceable obligations include, amongst other things, any binding corporate rules in accordance with Regulation 10(3) of the PDPR; and

(c) Regulation 10(3) of the PDPR provides that such binding corporate rules must require every recipient of the transferred personal data to provide a standard of protection for the transferred personal data that is comparable to that of the PDPA, and must specify (i) the recipients of the transferred personal data to which the binding corporate rules apply; (ii) the countries and territories to which the personal data may be transferred under the binding corporate rules; and (iii) the rights and obligations provided by the binding corporate rules. Further such binding corporate rules may only be used by recipients that are related to the transferring organisation.

Whether the Organisation complied with the Transfer Limitation Obligation

7 The Commission's investigations revealed that the Organisation had complied with the Transfer Limitation Obligation for the reasons explained below.

8 At the material time, the Organisation had put in place binding corporate rules set out in the St Engineering's Group Binding Corporate Rules for

Transfers of Personal Data (PDP-04) ("**BCRs**"), which met the requirements of Regulation 9(1)(b) read together with Regulations 10(1)(c) and 10(3) of the PDPR:

(a) The BCRs were applicable to and legally binding upon all of the Organisation's direct and indirect subsidiaries worldwide (each a "**Group Company**" and collectively, the "**Group**"), concerning the transfers (including international transfers) of personal data within the Group;

(b) The BCRs specified the countries and territories to which personal data may be transferred (which included the USA);

(c) Each Group Company that received transferred personal data was bound by legally enforceable obligations to provide a standard of protection for the personal data transferred that is at least comparable to the protection under the PDPA. In particular:

"5.6 The Receiving Company shall protect the transferred Personal Data in its possession or under its control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or other similar risks to the transferred Personal Data.

6.1 Each Group Company warrants and undertakes that it has implemented and maintained appropriate security, technological and organisational measures in accordance with the Group Company's legal obligations under the PDPA or other applicable Data Protection Laws to protect Personal Data and to prevent unauthorised access,

collection, use, disclosure, copying, modification, disposal or other similar risks to the transferred Personal Data."

(d) Rights and obligations provided by the BCRs are specified. These included the permitted purposes for transfer of personal data, data protection obligations of the receiving company, and protection and security of personal data. The permitted purposes set out in the following clauses in the BCRs included the purposes of transfer of the Affected Individual's Personal Data Sets at [3]

"1. Managing or terminating the employment relationship …

… (xvii) Preparing and making travel arrangements for employees' work or business travel (including visa applications, transport and accommodation arrangements) …

… 2. Evaluative purposes …

… (iii) Evaluation for secondment / transfer of employment to another entity within the Group / for extension of contract (for contract staff) / termination / redundancy / restructuring …

… 3. Group's business operations, including the Group's internal business management, administration and operations: …

… (vi) Submission to government agencies and authorities for permits and approvals …

… (xiii) To facilitate security clearance / entry access into premises of customers, vendors, consultants and other business partners".

9 Having carefully considered all the relevant circumstances and for the reasons set out above, I find that the Organisation complied with the Transfer

Limitation Obligation in relation to its transfer of the Affected Individual's Personal Data Sets to VT SAA and its other subsidiaries based in the USA.

YEONG ZEE KIN
DEPUTY COMMISSIONER
FOR PERSONAL DATA PROTECTION