PERSONAL DATA PROTECTION COMMISSION

[2020] SGPDPC 8

Case No. DP-1903-B3501

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

And

Secur Solutions Group Pte Ltd

… *Organisation*

DECISION

Data Protection *– Protection obligation – Unauthorised access to personal data – Insufficient security arrangements*

Secur Solutions Group Pte Ltd

[2020] SGPDPC 8

Tan Kiat How, Commissioner — Case No. DP-1903-B3501

30 March 2020

Introduction

1 This case relates to an incident where one of Secur Solutions Group Pte Ltd's (the "**Organisation**") servers, which stored a database (the "**Database**") containing personal data of blood donors, was discovered to be accessible from the internet (the "**Incident**").

2 The Personal Data Protection Commission (the "**Commission**") received a formal request from the Organisation requesting for this matter to be handled under the Commission's Expedited Breach Decision procedure. In this regard, the Organisation voluntarily provided and unequivocally admitted to the facts as set out in this Decision and that it was in breach of section 24 of the Personal Data Protection Act (the "**PDPA**").

Facts of the Case

3 The Organisation has been engaged by the Health Sciences Authority ("**HSA**") since 2013 to develop and maintain various IT systems. One of the projects for which the Organisation was engaged was the development, maintenance and enhancement of its queue management system ("**QMS**") for blood donors (the "**QMS Engagement**"). Pursuant to the QMS Engagement, HSA provided the Organisation with files containing copies (in part or otherwise) of the Database ("**Files**") for the purposes of testing and developing the QMS. HSA would also provide the Organisation with copies or updates of the Database ("**Updates**") from time to time during the period of the QMS Engagement (hereinafter, the use of the phrase "Files" will include "Updates", unless the context specifies otherwise).

4 The Organisation stored the Files in a storage server that was designated for the purposes of testing and development (the "**Testing and Development Server**"). The Testing and Development Server was accessible through the Internet and unsecured as it was not intended to be used to store personal data or other confidential information. The Server's system was not actively patched or updated, the router to which the Server was connected did not have a perimeter firewall setup, and there were no firewalls or any other security protocols to restrict access to the Server.

5 At the material time, the Files contained registration-related information (the "**Personal Data**") of about 800,000 individual blood donors (the "**Affected Individuals**"), specifically:

(a) Name;

(b) NRIC;

(c) Gender;

(d) Handphone number[1];

(e) Number of blood donations;

(f) Dates of the last 3 blood donations; and

(g) (In some cases) blood type, height and weight.

6 A cybersecurity expert discovered that he could access the Personal Data in the Database through one of the Organisation's servers. Based on the forensic investigations conducted by the Organisation, the number of records from the Database that had been exfiltrated amounted to anywhere between 236,023 to 328,546.

[1]This was based on the information provided by the Organisation.

7 Upon being notified of the Incident on 13 March 2019, the Organisation took the following remedial actions:

(a) Disconnected the Testing and Development Server from the Internet and removed all physical devices connected to the compromised ports to the server;

(b) Disabled all remote access to the Organisation's servers to ensure that all development zones were protected by firewalls;

(c) Organised an employee townhall session addressing the Incident;

(d) Appointed external vendors to undertake forensic analysis of the affected servers;

(e) Issued press releases to keep the public informed of the Incident and the status of ongoing investigations;

(f) Informed its employees not to receive personal data from clients if it was not necessary and to escalate the receipt of personal data (inadvertently or otherwise) to senior management;

(g) Conducted further investigation on the security of its Internet lines and Internet-facing services;

(h) Began reviewing and improving its internal processes and taking steps to enhance its cybersecurity posture, including appointing a second Data Protection Officer, requiring employees to complete an e-learning program and identifying and remediating any gaps in protection; and

(i) Began reviewing its security infrastructure with the assistance of an external vendor, and implementing certain measures, including (i) ensuring all devices used by employees are secured and the anti-virus software installed on these devices are up-to-date, (ii) implementation of a Network Access Control measure, (iii) adoption of a "defence-in-depth" approach (including segregation of servers containing sensitive information) and (iv) enhancement of endpoint security measures.

Findings and Basis for Determination

8 Section 24 of the PDPA requires an organisation to protect 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 similar risks. As a preliminary point, the Organisation has accepted that it is a data intermediary of HSA and is required to comply with section 24 of the PDPA with respect to the Personal Data in its possession.

Whether the Organisation Complied with Section 24

9 The Organisation has admitted that it has breached section 24 of the PDPA by failing to put in place reasonable security arrangements to protect the Personal Data.

10 The Organisation informed the Commission that it had stored the Files containing the Database in its Testing and Development Server as it did not anticipate that it would be receiving actual copies of production databases from HSA and, as such, did not take any steps to designate any specific security infrastructure set up to receive or store such data on premise.

11 The Organisation admitted that it ought to have been aware that the Files contained personal data even though they had not been specifically informed of this by HSA. In past projects between them, the Organisation had directly retrieved personal data from a production environment on the servers on HSA's premises for the purposes of testing and development. On this occasion, even though the Files were provided by HSA to the Organisation for the QMS Engagement, from July to August 2018, the Organisation was given access to HSA's server rooms to retrieve Updates directly from HSA's servers, an arrangement that made sense if the Files also contained actual personal data (as opposed to dummy data). Accordingly, the Organisation ought to have been

aware that personal data was contained in the Files, but most definitely in the Updates.

12 In this regard, the Organisation admitted that the Files should not have been stored on the Testing and Development Server, and this was a breach of the Organisation's own data protection policies and practices, which required that personal data be protected and secured regardless of the purposes for which it was provided.

13 The Organisation has accepted that there were gaps in its data governance and processes with respect to the receipt of test data from its clients.

14 In view of the above, the Commissioner found the Organisation in breach of section 24 of the PDPA.

Representations by the Organisation

15 In the course of settling this decision, the Organisation made representations to request that the financial penalty as set out in [19] be paid in the following manner:

(a) $60,000 within 30 days from the date of the directions; and

(b) $60,000 within 7 months from the date of the directions.

16 The Organisation raised the following factors for the Commissioner's consideration:

(a) The Organisation is a small medium enterprise in a highly competitive IT services industry. It has to contend with rising wage costs and increased rentals while battling depressed prices that customers are willing to pay for their services;

(b) Arising out of the Incident, the Organisation has:

(i) Expended significant resources when it appointed reputable advisors to undertake forensic activities, and sought the advice and assistance of professionals to respond to the police and the Commission's investigations;

(ii) Invested heavily to shore up its data protection and cybersecurity measures, including conducting research and exploring various technologies and methods which may be deployed in protecting data (at rest and in transit) without compromising ease of use of the data; and

(c) Payment of the entire financial penalty of $120,000 in one lump sum would negatively affect the Organisation's cash flow.

17 Having carefully considered the representations, the Commissioner has decided to reject the Organisation's request at [15]. For the purposes of supporting a request that a financial penalty be paid in instalments, organisations are required to furnish supporting documents on their financial status to the Commission. However, despite the Commission's repeated requests, the Organisation did not furnish its financial statements and was unable to provide any explanation why it could not to do so. There was therefore no evidence to support the Organisation's representations on its financial status at [16]. If the Organisation is able to secure documentary evidence of its financial position before the due date for payment as set out at [19], it may submit another request that the financial penalty be paid in instalments.

The Commissioner's Directions

18 In determining the directions to be imposed on the Organisation under section 29 of the PDPA, the Commissioner took into account the following factors:

Mitigating factors

(a) The Organisation was cooperative during the Commission's investigations;

(b) As set out above, the Organisation voluntarily and unequivocally admitted to its contravention of the PDPA; and

(c) The Organisation implemented remedial actions swiftly to address the Incident; and

Aggravating Factor

(d) A subset of the Personal Data was subject to unauthorised access and exfiltration.

19 Having carefully considered all the relevant factors of this case, the Commissioner hereby directs the Organisation to pay a financial penalty of $120,000 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.

20 The Commissioner took the view that the remedial actions set out at paragraph [7] had sufficiently addressed the risks to the Personal Data arising from the Incident. The Commissioner has therefore not set out any further directions for the Organisation.