PERSONAL DATA PROTECTION COMMISSION

[2021] SGPDPC 9

Case No. DP-2006-B6440

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

And

J & R Bossini Fashion Pte Ltd

… *Organisation*

DECISION

J & R Bossini Fashion Pte Ltd

[2021] SGPDPC 9

Yeong Zee Kin, Deputy Commissioner — Case No. DP-2006-B6440

18 August 2021

Introduction

1 On 13 June 2020, J & R Bossini Fashion Pte Ltd ("**the Organisation**") notified the Personal Data Protection Commission ("**the Commission**") of a ransomware attack which had affected the IT systems of the Organisation's group of companies on or around 27 May 2020 ("**the Incident**"). The Commission commenced investigations to determine whether the circumstances relating to the Incident disclosed any breaches by the Organisation of the Personal Data Protection Act 2012 ("**PDPA**").

Facts of the Case

2 The Organisation is a company incorporated in Singapore, and a subsidiary of Bossini International Holdings Limited, a company listed on the Stock Exchange of Hong Kong ("**Bossini Holdings**"). Bossini Holdings and its subsidiaries ("**the Group**") are in the business of garment retail and brand franchising.

3 The Group's IT systems and infrastructure across different regions (including Singapore) are centrally managed by Bossini Holdings from Hong Kong. While most of the Group's production servers are located in Hong Kong, at the material time, the Organisation maintained two servers and various workstations for its staff in Singapore which were connected to the Group's network in Hong Kong by way of a virtual private network ("**VPN**").

Personal data collected by the Organisation

4 Sometime prior to 2017, the Organisation collected personal data from customers and prospective customers in Singapore for the purposes of administering a customer loyalty programme. The personal data collected comprised of each individual's:

(a) Name;

(b) NRIC number,

(c) Phone number,

(d) Email address,

(e) Residential address,

(f) Date of birth; and

(g) Gender.

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

5 The Customer Data was initially stored locally by the Organisation in its servers in Singapore. The Organisation transferred the Customer Data out of Singapore to a server in Hong Kong around July 2017, as part of a Group level consolidation exercise with a view to hosting the data in a cloud environment in the future.

6 Other than the Customer Data, the Organisation also collected and stored personal data pertaining to its employees in its Singapore servers. This included each employee's:

(a) Name;

(b) NRIC number,

(c) Phone number,

(d) Email address,

(e) Residential address,

(f) Date of birth;

(g) Gender;

(h) Marital status;

(i) Salary details;

(j) Bank account details, and

(k) Medical claims records.

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

The Incident

7 Sometime before 27 May 2020, attackers gained access to the Group's network in Hong Kong by exploiting a vulnerability in the Group's off-the-shelf VPN software. The vulnerability allowed the attackers to extract valid VPN credentials and bypass the Group's perimeter network security measures.

8 The vulnerability exploited by the attackers had been fixed by a patch released by the VPN software developer in September 2019. However, Bossini Holdings had not deployed the patch for the Group as at the time of the Incident on 27 March 2020 (i.e. nine months later). The patch was subsequently deployed after the Incident on 3 June 2020.

9 After gaining a foothold into the Group's network in Hong Kong, the attackers moved laterally across the Group and compromised various administrative and user accounts to conduct reconnaissance and escalate privileges. Eventually, with Group-level administrative privileges, the attackers disabled endpoint security systems across the Group and executed the ransomware attack.

10 The personal data of approximately 200,000 of the Group's customers stored in the Hong Kong server was encrypted and rendered inaccessible in the Incident. Relevantly, this included the Customer Data of 154,213 customers originally collected by the Organisation in Singapore. Of this, the Customer Data of at least 14,082 Singapore customers was exfiltrated and exposed on the dark web. The Employee Data of 120 of the Organisation's employees stored in the servers in Singapore was similarly encrypted and rendered inaccessible in the Incident.

11 All backups of the Customer Data and Employee Data maintained by Bossini Holdings and the Organisation were affected and encrypted in the Incident, and no data restoration was possible.

Remedial actions

12 Following the Incident, the remedial actions of Bossini Holdings and the Organisation included:

(a) Appointing a leading cybersecurity vendor to contain the impact of the Incident and investigate its causes;

(b) Publishing a data breach announcement on the Group's website and via the Stock Exchange of Hong Kong;

(c) Notifying affected customers via the email addresses provided when registering for the customer loyalty programme;

(d) Blocking the IP addresses used by the attackers in the Incident and restricting outbound network traffic to limit the ability of any malware in the Group's network to "call back" to the attackers;

(e) Upgrading the VPN software to patch the vulnerability;

(f) Enforcing multi-factor authentication for all remote access via VPN;

(g) Enforcing a password change for all user account passwords and resetting all domain user credentials;

(h) Performing a review to limit and restrict public-facing services on network perimeters;

(i) Performing vulnerability scanning for critical servers to identify and rectify immediate risks;

(j) Reviewing and enhancing endpoint protection tools;

(k) Implementing monitoring of perimeter firewalls and planning upgrades to the server firewalls; and

(l) Engaging a third-party security operations centre to monitor the Bossini group's network infrastructure.

13 For completeness, the Privacy Commissioner for Personal Data, Hong Kong ("**PCPD**") was notified of the Incident by Bossini Holdings on 24 June 2020 and conducted its own compliance check. The Commission was informed that the PCPD would not be proceeding with any further investigations after considering the circumstances of the case and the remedial measures taken by Bossini Holdings.

Findings and Basis for Determination

14 Based on the circumstances of the Incident, the Commission's investigation focused on:

(a) Whether the Organisation had breached its obligation under section 26 of the PDPA to transfer personal data to a country or territory outside Singapore in accordance with requirements prescribed under the PDPA (the "**Transfer Limitation Obligation**") in respect of the Customer Data transferred to Hong Kong on 17 July 2017; and

(b) Whether the Organisation had breached its obligation under section 24 of the PDPA 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 (the "**Protection Obligation**") in respect of the Employee Data encrypted in the Organisation's servers in Singapore during the Incident.

15 For the reasons set out below, the Organisation was determined to have breached both the Transfer Limitation and Protection Obligations.

16 As a preface to the discussion below, it is relevant to highlight that both of the Organisation's breaches were attributable to its failure to implement policies and practices to meet its obligations under the PDPA, as required by section 12 of the PDPA ("**the Accountability Obligation**").

17 For corporate groups which engage in (i) centralisation of corporate functions involving intra-group dataflows and/or (ii) "outsourcing" of data processing activities to another member of the same group, policies and practices ought to be developed and implemented at the group level for the benefit of all members of the group. As stated in *Everlast Projects Pte Ltd and others* [2020] SGPDPC 20 ("***Everlast***") at [13]:

> "(O)*rganisations operating as a group of companies may comply with the Accountability Obligation through binding group-level written policies or intra-group agreements that set out a common and binding standard for the protection of personal data across all organisations in the same corporate group. These binding group-level written policies or intra-group agreements are akin to binding corporate rules ("**BCRs**") imposed by an organisation on its overseas recipient of the personal data (in compliance with the Transfer Limitation Obligation under Section 26(1) of the PDPA), which oblige the overseas recipient to provide a standard of protection to the transferred personal data that is at least comparable to that under the PDPA. When the corporate group is a multinational corporation ("**MNC**") and the Contracting Organisation* (i.e. a member of a corporate group) *transfers personal data to an overseas Servicing Organisation* (i.e. an overseas member of the same corporate group), *the binding group-level written policies, intra-group agreements or BCRs which meet the requirements of the Protection Obligation under section 24 of the PDPA*

would also meet the requirements of section 26(1) of the PDPA (i.e. the Transfer Limitation Obligation)"

Whether the Organisation breached the Transfer Limitation Obligation

18 As the Customer Data was transferred from Singapore to Hong Kong on 17 July 2017, the requirements in Part III of the Personal Data Protection Regulations 2014 ("**PDPR**")[1] governed the Organisation's compliance with the Transfer Limitation Obligation.

19 Regulation 9(1)(b) of the PDPR requires an organisation that transfers personal data outside of Singapore to take appropriate steps to ensure that the recipient of the personal data is bound by *legally enforceable obligations* to provide the transferred personal data a standard of protection at least comparable to that under the PDPA. Under regulation 10 of the PDPR, such legally enforceable obligations can be imposed on the recipient organisation under (a) any law (e.g. the law of the recipient country); (b) any contract between the parties[2]; (c) binding corporate rules[3]; or (d) any other legally binding instrument.

20 In the present case, the Organisation transferred the Customer Data to Bossini Holdings upon instruction and took no steps to ascertain whether the Customer Data would be accorded a comparable level of protection. In this regard, the transfer of the Customer Data was not made pursuant to any intra-group contracts, binding corporate rules, or other legally binding instrument. Accordingly, the Organisation failed to comply with regulation 9(1)(b) of the PDPR and was determined to have breached the Transfer Limitation Obligation.

[1] For transfers which took place on or after 1 February 2021, the relevant requirements are those prescribed in Part 3 of the Personal Data Protection Regulations 2021.
[2] For example, see *Cigna Europe Insurance Company S.A.-N.V.* [2019] SGPDPC 18.
[3] For example, see *Singapore Technologies Engineering Limited* [2020] SGPDPC 21.

Whether the Organisation breached the Protection Obligation

21 At the time of the Incident, Bossini Holdings had implemented group-level security arrangements for all of the Group's IT systems, including the Organisation's servers in Singapore. Notwithstanding, the Employee Data remained in the Organisation's possession in the servers in Singapore, and the Organisation bore the Protection Obligation in respect of the same.

22 It is appreciated that a corporate subsidiary in the circumstances of the Organisation, which is subject to group-level security arrangements managed centrally, may not have the autonomy or power to respond independently to a multinational data breach incident. Nevertheless, the standard of conduct expected of such organisations in order to comply with the Protection Obligation is not onerous. The following principles have been established in past decisions.

(a) First, a subsidiary should not adopt group level data protection policies without considering whether these need to be adapted to their circumstances and contexts: *Tiger Airways Singapore Pte Ltd and others* [2017] SGPDPC 6 at [33]; and

(b) Second, when there is centralisation of corporate functions, group level policies should be put in place in order that roles and responsibilities are clear: *Everlast*.

23 These twin principles provide the guard rails to guide organisations for establishing accountability within a group and how this should cascade. In gist, where there is centralisation of corporate functions, group level policies establish the scope of centralisation and the respective roles and responsibilities of members within the group. This is not dissimilar to a situation in which a data controller outsources certain data protection responsibilities to an external vendor. It is the data controller's obligation to specify and document what

responsibilities the vendor has undertaken, failing which they remain those of the data controller. Once the group level policies are established, the relevant content then needs to be cascaded and adapted in the internal policies implemented by each member of the group at an organisational level.

24 As a subsidiary in a multinational corporate group, it is accepted that the Organisation had to implement the Group's IT policies, including IT security practices. The reality is that its ability to influence these IT policies and how these practices were implemented was likely to also have been limited. Nevertheless in the present case, the Group had no group level policies, intra-group agreements, or binding corporate rules spelling out the data protection responsibilities of the respective members of the Group. This created uncertainty as to whether Bossini Holdings or the Organisation was responsible for software patching and security testing of the Organisation's IT systems in Singapore.

25 It was also accepted that the security lapse and privilege escalation that enabled the attackers to overcome the Organisation's endpoint protections in the Incident occurred abroad out of the control of the Organisation. If the Group had intended for Bossini Holdings to be centrally responsible for developing, implementing, and maintaining security arrangements for all of the Group's IT systems (including those of the Organisation), this should have at least been documented in a binding group-level written policy. There was no evidence of the same, and accordingly, the Organisation continued to bear responsibility in relation to the Employee Data in its possession.

26 In the circumstances, the Organisation was determined to have breached the Protection Obligation.

The Deputy Commissioner's Directions

27 Having considered all the relevant factors of this case, the Deputy Commissioner hereby directs the Organisation to:

(a) within 30 days from the date of the direction accompanying this decision, put in place intra-group agreements, contracts, or binding corporate rules for compliance with sections 24 and 26 of the PDPA; and

(b) inform the Commission of the completion of the above within 7 days of implementation.

YEONG ZEE KIN
DEPUTY COMMISSIONER
FOR PERSONAL DATA PROTECTION