PERSONAL DATA PROTECTION COMMISSION

[2020] SGPDPC 20

Case No. DP-1908-B4369

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

And

(1) Everlast Projects Pte Ltd
(2) Everlast Industries (S) Pte Ltd
(3) ELG Specialist Pte Ltd

… *Organisations*

DECISION

Everlast Projects Pte Ltd & Others

[2020] SGPDPC 20

Yeong Zee Kin, Deputy Commissioner — Case No. DP-1908-B4369

30 October 2020

Introduction

1 On 29 September 2019, Everlast Projects Pte Ltd ("**EPPL**") notified the Personal Data Protection Commission ("**Commission**") that its server ("**Server**") had been hacked and all the files within it were encrypted by ransomware sometime in August 2019 (the "**Incident**").

Facts of the Case

2 EPPL, Everlast Industries (S) Pte Ltd ("**EIPL**") and ELG Specialist Pte Ltd ("**ESPL**") (collectively, the "**Organisations**") specialise in the supply and installation of architectural metal works, glass and aluminium products. The Organisations are owned by the same shareholder, managed by the same directors, and operate from common premises. Two of the Organisations also have a common name, "Everlast". The Organisations operated like a group of companies and centralised their payroll processing, such that the human resources ("**HR**") department of EPPL was in charge of processing payrolls of not only its own employees, but also the employees of EIPL and ESPL. The Organisations' employees' personal data were stored in the Server, which was owned and maintained by EPPL.

3 On 10 August 2019, EPPL discovered the Incident. EPPL had both an onsite physical backup and a secondary cloud backup of the contents of the Server. The physical backup was affected by the ransomware and rendered unusable. A total of 384 individuals were affected by the Incident (the "**Affected Employees**"):

Name of Organisation	Number of employees affected
EPPL	141
EIPL	239
ESPL	4
Total number of individuals	**384**

4 The types of personal data of the Affected Employees that were at risk of unauthorised access included the following (collectively, the "**Personal Data Sets**"):

(a) Name;

(b) NRIC/FIN number;

(c) Date of birth;

(d) Bank account details; and

(e) Information relating to salary.

5 The cause of the ransomware infection was not identified. EPPL's investigations could not determine how the ransomware gained entry to the Server. EPPL was also unable to confirm whether any of the Personal Data Sets had been exfiltrated as a result of the Incident. Upon discovery of the Incident, EPPL took prompt remedial action by ceasing to use the Server immediately.

6 Findings and Basis for Determination

7 The two issues to be determined in this case are as follows:

(a) Whether the Organisations had each complied with their obligations under section 12 of the Personal Data Protection Act 2012 (the "**PDPA**"); and

(b) Whether the Organisations had each complied with their obligations under section 24 of the PDPA.

Whether EPPL, EIPL and ESPL had each complied with their obligations under section 12 of the PDPA

8 Section 12 of the PDPA requires organisations to, *inter alia*, develop and implement policies and practices that are necessary for the organisation to meet its obligations under the PDPA, and to communicate information about such policies and practices to its staff (the "**Accountability Obligation**").

9 In this regard, it is important to reiterate that an organisation's Data Protection Policies should be documented in a written policy, as per *Re Furnituremart.sg* [2017] SGPDPC 7 at [14]:

> *"[t]he lack of a written policy is a big drawback to the protection of personal data. Without having a policy in writing, employees and staff would not have a reference for the Organisation's policies and practices which they are to follow in order to protect personal data. Such policies and practices would be ineffective if passed on by word of mouth, and indeed, the Organisation may run the risk of the policies and practices being passed on incorrectly. Having a written policy is conducive to the conduct of internal training, which is a necessary component of an internal data protection programme."*

10 As mentioned at [2], EPPL, EIPL and ESPL operated as a group of companies in the sharing of payroll processing services, which are centralised within the HR department of EPPL. The Commission recognises the commercial benefits which arise from centralising common corporate functions within a group of companies. In such situations, one entity (the "**Servicing Organisation**") provides corporate services to other entities in the same corporate group (each a "**Contracting Organisation**"). If the shared common corporate services involve the processing of personal data, the Servicing Organisation would be acting as a data intermediary for each Contracting Organisation.[1]

11 The common corporate service shared by the Organisations in the present case was the payroll processing function. EIPL and ESPL were therefore permitted to collect, without consent, their respective Affected Employees' Personal Data Sets and

[1] See the Commission's *Advisory Guidelines on Key Concepts in the PDPA* (revised 2 June 2020) at [6.28].

disclose the same to EPPL for the purposes of managing the employment relationship.[2] In these circumstances, EPPL was:

(a) A data controller with respect to its own Affected Employees' Personal Data Sets; and

(b) EIPL and ESPL's data intermediary with respect to their respective Affected Employees' Personal Data Sets that EPPL was processing on their behalf.

12 The Organisations admitted that they did not have any written data protection policies and relied only on verbal instructions to employees. Although the Organisations are in the construction industry and, in this case, do not typically collect personal data from customers, the Accountability Obligation required the Organisations to put in place data protection policies in relation to the protection of personal data of their respective employees.

13 In this regard, organisations 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.[3] Where the corporate group is a multinational corporation ("**MNC**") and the Contracting Organisation transfers personal data to an overseas Servicing Organisation, the binding group-level written policies, intra-group agreements or BCRs which meet the

[2] See Second Schedule of the PDPA, para 1(o) and Fourth Schedule of the PDPA, para 1(s).

[3] The Transfer Limitation Obligation under Section 26 of the PDPA 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 to provide to the transferred personal data a standard of protection that is at least comparable to that under the PDPA.

requirements of the Protection Obligation under section 24 of the PDPA[4] would also meet the requirements of section 26(1) of the PDPA in relation to the Protection Obligation.[5]

14 In the present case, the Organisations did not have any such binding group-level written policies, intra-group agreements or BCRs. In the circumstances, I find each of EPPL, EIPL and ESPL in breach of the Accountability Obligation.

Whether EPPL, EIPL and ESPL had contravened section 24 of the PDPA

15 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 or similar risks (the "**Protection Obligation**"). The obligation to make reasonable security arrangements does not attach unless the organisation is in possession or control of personal data.

16 As mentioned at [10], EPPL was (i) a data controller with respect to its own Affected Employees' Personal Data Sets; and (ii) EIPL and ESPL's data intermediary with respect to their Affected Employees' Personal Data Sets that EPPL was processing on their behalf. In this regard, EPPL, EIPL and ESPL had possession and/or control of the Affected Employees' Personal Data Sets at the material time.

(a) EPPL was in possession and control of the Affected Employees' Personal Data Sets. This was because the Organisations' payroll processing functions were centralised within the HR department of EPPL.

(b) While EIPL and ESPL did not have possession of their respective Affected Employees' Personal Data Sets because they were centrally hosted on EPPL's Server, I find that EIPL and ESPL remained in control of their respective Affected Employees' Personal Data Sets as data controllers. This is because the

[4] The Protection Obligation is explained at paragraph 14.

[5] See, for illustration, *Re Cigna Europe Insurance Company S.A.-N.V.* [2019] SGPDPC 18 at [13].

processing of EIPL's and ESPL's Affected Employees Personal Data Sets by EPPL was for EIPL's and ESPL's respective business purposes.[6]

17 Each of the Organisations were therefore obliged to put in place reasonable security arrangements to protect the Affected Employees Personal Data Sets, including preventing the risk of unauthorised modification. In the present case, the Commission's investigations into the Incident revealed that the ransomware had encrypted all the files in the Server and its physical backup, including the Affected Employees' Personal Data Sets. The unauthorised modification of the Affected Employees' Personal Data Sets by the ransomware made it unreadable and unusable.

18 It is well established that a data controller should have in place a written contract with its data intermediary that clearly specifies the data intermediaries' obligation to protect personal data.[7] That said, the relationship between the Organisations is a relevant factor in determining the reasonable security measures expected of them to comply with the Protection Obligation. In this regard, for a group of companies, the written contract requirement between a Servicing Organisation and the Contracting Organisation may be met by binding group-level written policies, intra-group agreements or BCRs as discussed at [13] above.

19 In addition to a written agreement specifying data protection requirements, a Contracting Organisation should also implement operational processes so as to be able to exercise some form of supervision or control over the activities of the Servicing Organisation when it processes personal data on the Contracting Organisation's behalf.[8] Where the Servicing Organisation has specialised knowledge, skills and/or tools for processing personal data, having a robust audit framework could be an appropriate form of oversight. This may be particularly suited for MNCs which typically

---

[6] See *Re The Cellar Door Pte Ltd and another* [2016] SGPDPC 22 at [17] – [18]*; Re AIG Asia Pacific Insurance Pte Ltd* [2018] SGPDPC 8 at [18].

[7] See the Commission's *Guide on Data Protection Clauses for Agreements relating to the Processing of Personal Data* (20 July 2016) at [4]; *Re Singapore Telecommunications Limited* [2017] PDPC 4 at [14]

[8] The Commission's *Advisory Guidelines on Key Concepts in the PDPA* (revised 2 June 2020) at [17.5] provides that "[e]nsuring that IT service providers are able to provide the requisite standard of IT security" is an example of a technical measure an organisation may use to protect personal data.

conduct periodic internal and/or external audits and assessments to monitor compliance by each organisation within the corporate group.[9] Conversely, small and medium-sized enterprises that only operate in Singapore are less likely to conduct such compliance audits on each organisation in the corporate group in the areas of cybersecurity and/or data protection. In such situations, appropriate oversight could involve more simple processes. For example, requiring the Servicing Organisation to explain to the Contracting Organisation the measures which would be taken to secure personal data, with appropriate documentation to evidence this process (e.g. written acknowledgement given by the Contracting Organisation to the Servicing Organisation), and provide regular reports showing that it has put these processes in place.

20 In the present case, both EIPL and ESPL failed to put in place reasonable security arrangements to ensure that EPPL (who was their data intermediary for the purposes of payroll processing) would protect their respective Affected Employees' Personal Data Sets. There was no written contract, intra-group agreement or group-level written policies/BCRs setting out data protection requirements that EPPL was obliged to comply with when processing EIPL's and ESPL's respective Affected Employees' Personal Data Sets. Notwithstanding that the Organisations conducted their business operations from the same premises, both EIPL and ESPL also did not implement any operational processes to supervise or exercise some form control over EPPL to ensure EPPL protected their Affected Employees' Personal Data Sets. In the circumstances, I find each of EIPL and ESPL in breach of the Protection Obligation.

21 EPPL was also obliged to comply with the Protection Obligation. As mentioned in [10], it was: (i) a data controller with respect to its own Affected Employees' Personal Data Sets; and (ii) EIPL and ESPL's data intermediary with respect to their Affected Employees' Personal Data Sets. The Commission's Investigations revealed that EPPL did not put in place reasonable security arrangements to protect the Personal Data Sets as explained below:

[9] As an example, see *Re Cigna Europe Insurance Company S.A.-N.V.* [2019] SGPDPC 18 at [7(c)].

(a) EPPL did not install a firewall for the Server. Without a firewall, the Server and corporate network was vulnerable to web-based security threats;[10]

(b) EPPL did not conduct periodic security reviews of its IT systems, including vulnerability scans of the Server, to assess the overall security of its IT infrastructure. The requirement for organisations to conduct periodic security reviews of its IT systems has been emphasized in previous decisions.[11] Conducting regular information and communication technology ("**ICT**") security audits, scans and tests to detect vulnerabilities help organisations to ensure that ICT security controls developed and configured for the protection of personal data are properly implemented.[12] The comprehensiveness of such security reviews should be scoped based on the organisation's assessment of its data protection needs, and be conducted to a reasonable standard. The scope and level of the review would depend on the type of personal data to be protected. In this case, as the Personal Data Sets included personal data of a financial nature (e.g. information relating to bank accounts and salaries), a higher standard of periodic security review was required of EPPL in order to comply with the Protection Obligation. If EPPL had conducted a security review of its IT system to a reasonable standard, it would have discovered the absence of a firewall for the Server; and

(c) EPPL was unable to provide any written IT security policies (e.g. password policy, policies for patching and updating of the company server, etc.).[13] In this regard, EPPL conceded that they did not know what was required in order to protect personal data in electronic form.

---

[10] The Commission's *Guide to Securing Personal Data in Electronic Medium* (20 January 2017) at [9.1] states as follows: "It is important for an organisation to ensure that its corporate computer networks are secure. Vulnerabilities in the network may allow cyber intrusion, which may lead to theft or unauthorised use of electronic personal data. Defences that may be used to improve the security of networks include: […] Firewalls".

[11] See, for example, *Re WTS Automotive Services Pte. Ltd.* [2018] SGPDPC 26 at [18], *Re Bud Cosmetics* [2019] SGPDPC 1 at [24] and *Re Chizzle Pte. Ltd.* [2019] SGPDPC 44 at [6] to [8].

[12] Commission's *Guide to Securing Personal Data in Electronic Medium* (revised 20 January 2017) at [6.1].

[13] The Commission's *Advisory Guidelines on Key Concepts in the PDPA* (revised 2 June 2020) at [17.5] provides that "[s]ecurity arrangements may take various forms such as administrative measures, physical measures, technical measures or a combination of these". Having robust policies and procedures is an example of an administrative measure an organisation may implement by way of security arrangements.

22 For the reasons above, I also find EPPL in breach of the Protection Obligation.

Directions

23 In determining the directions, if any, to be imposed on EPPL, EIPL and ESPL under section 29 of the PDPA, I took into account the following factors:

(a) The Organisations had voluntarily notified the Commission of the Incident;

(b) The Commission did not receive any complaints of the Personal Data Sets being disclosed online or otherwise misused;

(c) There was no evidence of exfiltration of the Personal Data Sets; and

(d) An imposition of a financial penalty would impose a crippling burden and cause undue financial hardship due to the financial position of the Organisations.

24 Having considered all the relevant factors of this case, I direct EPPL, EIPL and ESPL to:

(a) Develop and implement intra-group agreements or binding corporate rules that set out a common and binding standard for the processing of personal data when centralising common corporate activities within the group, within 90 days from the date of this direction;

(b) Review and ensure that the internal policies within each of EPPL, EIPL and ESPL are in line with the standards set forth in the intra-group agreements or binding corporate rules, within 90 days from the date of this direction; and

(c) Inform the Commission of the completion of the directions set out at [23(a)] and [23(b)] within one week.

YEONG ZEE KIN
DEPUTY COMMISSIONER
FOR PERSONAL DATA PROTECTION