PERSONAL DATA PROTECTION COMMISSION

[2022] SGPDPC 4

Case No. DP-2008-B6707

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

And

(1) Toll Logistics (Asia) Limited
(2) Toll Global Forwarding (Singapore) Pte. Limited
(3) Toll Offshore Petroleum Services Pte. Ltd.
(4) Toll (TZ) Pte. Ltd.

… *Organisation*

DECISION

Data Protection *– Protection obligation – Unauthorised access of personal data – No breach – Reasonable security arrangements implemented*

Data Protection *– Transfer Limitation obligation – Failure to ascertain and ensure that the recipient of the personal data outside Singapore is bound by legally enforceable obligations to provide a comparable standard of protection*

Toll Logistics (Asia) Limited and others

[2022] SGPDPC 4

Yeong Zee Kin, Deputy Commissioner — Case No. DP-2008-B6707

14 March 2022

Introduction

1 Toll Holdings Limited ("**Toll Holdings**") is an integrated logistics services provider headquartered in Australia. Toll Logistics (Asia) Limited ("**Toll Logistics**"), Toll Global Forwarding Singapore Pte. Ltd. ("**Toll Forwarding**"), Toll Offshore Petroleum Services Pte. Ltd. ("**Toll Offshore**"), and Toll (TZ) Pte. Ltd. ("**Toll TZ**") are Singapore-registered entities (collectively, "**the Organisations**") that are part of a multinational group of companies headed by Toll Holdings ("**the Group**").

2 On 11 June 2020, Toll Holdings notified the Personal Data Protection Commission ("**the Commission**") of a ransomware attack which had affected the Group's IT systems, including servers in Australia and Singapore containing the personal data of current and former employees of the Organisations ("**the Incident**"). The Commission subsequently received complaints from 3 former employees of Toll Logistics in relation to the Incident. Investigations were commenced to determine whether the circumstances relating to the Incident disclosed any breaches by the Organisations of the Personal Data Protection Act 2012 ("**PDPA**").

Facts of the Case

3 In July 2013, Toll Holdings contracted with a vendor in Ireland ("**the HR Vendor**") for the Group's use of the HR Vendor's human resources software platform ("**the HR Platform**"). To facilitate use of the common HR Platform, the respective Group entities (including the Organisations) uploaded the personal data of their employees to the HR Platform. The data uploaded to the HR Platform was hosted by the HR Vendor in data centres in the European Economic Area.

4 Subsequently in 2019, a series of Corporate Services Agreements ("**CSAs**") and accession agreements were executed with the net effect that Toll Holdings undertook to provide finance, human resources ("**HR**"), information technology ("**IT**"), legal, and other corporate services to all the Organisations. Although the CSAs were inked in 2019, they took retrospective effect from 1 April 2018.

5 The services provided by Toll Holdings to the Organisations under the CSAs included:

(a) Development and maintenance of HR policies and procedures;

(b) Development and maintenance of IT strategy;

(c) Development and maintenance of IT policies and procedures; and

(d) Provision of IT support services.

6 Under the terms of the CSAs, Toll Holdings was permitted to appoint subcontractors to perform part or all of the services subject of the CSAs but was responsible to the same extent as if it had performed the services itself.

7 The scope of IT services to be provided by Toll Holdings under the CSAs specifically excluded the "*development or implementation of IT systems*", which responsibility presumably remained with the Organisations. To this end, the Organisations maintained ten servers in Singapore to support their operations. Three of these servers ("**the Singapore Servers**") were used by the Organisations' corporate teams (i.e. finance, legal, HR) in the ordinary course of their work and contained personal data within the email archives and other working documents.

8 The Group (including the Organisations) had implemented various industry-standard security solutions for its IT systems such as end-point protection software, logging and monitoring software and/ services, firewall and intrusion prevention software, security detection and response software, identity access management and control software and services, vulnerability scanning software and services, and patching software. A Managed Security Service Provider ("**MSSP**") was also engaged to provide cyber security detection and incident response services for the Group. With the assistance of the MSSP and other external vendors, the Group carried out regular vulnerability scanning and penetration testing of its IT systems.

Transfer of personal data to Australia

9 Sometime prior to the Incident, Toll Holdings' Chief Human Resources Officer extracted personal data relating to 1,748 of the Organisations' current and former employees from the HR Platform and transmitted them to a server in Australia ("**the Australia Server**"). Toll Holdings represented that this personal data was transferred for the purposes of performing services for the Organisations pursuant to the CSAs.

10 The personal data downloaded by Toll Holdings comprised each employee's:

(a) Name;

(b) Address

(c) Age; and

(d) Salary.

11 5 employees of Toll Logistics and 2 employees of Toll Forwarding also had other datasets disclosed including:

(a) Driver's licence number;

(b) Emergency contact details;

(c) National ID;

(d) Fingerprint;

(e) Medical details; and

(f) Passport details.

The Incident

12 On 26 April 2020, a malicious actor gained access to Toll Holdings' IT environment in Australia using credentials stolen from a third-party vendor. The third-party vendor had been granted administrative access to two servers in Toll Holding's IT environment in order to provide support services for a software solution.

13 Having gained access to the Group's IT environment, the malicious actor used advanced malware and a range of hacking tools to move through the Group's network, conduct reconnaissance, and escalate account privileges. The malicious actor also made various efforts to bundle and compress data from the Australia Server and stage it for exfiltration.

14 Threat monitoring software deployed by the Group detected events related to the malicious actor's account takeover and privilege escalation during the Incident and raised alerts to the MSSP. However, according to Toll Holdings, no alerts were brought to its attention. On 3 May 2020, the malicious actor exfiltrated less than 2% (two percent) of the data stored on the Australia Server using a web-based file sharing service. The malicious actor then ran scripts to disable various endpoint protections across the Group and executed a ransomware attack. The ransomware attack encrypted files on a number of the Group's servers, including the Australia Server and the Singapore Servers.

15 When subsequently making ransom demands, the malicious actor provided Toll Holdings a summary of the files exfiltrated from the Australia Server and eventually uploaded portions of the exfiltrated files onto the dark web. Based on (i) the summary provided by the malicious actor, (ii) the Group's review of the available logs and records on the Australia Server, and (iii) a review of the files eventually published by the malicious actor on the dark web, the Organisations concluded that there was no evidence of exfiltration of the personal data of its current or former employees from the Australia Server.

16 The Organisations also concluded that there was no evidence of data exfiltration from the Singapore Servers, or any other servers in the Group's IT environment in the Incident, other than the Australia Server. The Organisations were able to restore the encrypted data in the Singapore Servers from securely stored back-ups.

Remedial actions

17 Following the Incident, Toll Holdings implemented the following remedial measures on a Group-wide basis:

(a) Temporarily disconnected from the Internet, and undertook a rolling shutdown of IT systems in order to mitigate spread of any infection;

(b) Isolated all impacted servers and implemented network restrictions to prevent spread of the ransomware within the Group's network;

(c) Engaged third-party experts to assist with incident response, including investigation and remediation;

(d) Upgraded its user access system and reset all administrator passwords;

(e) Blocked the malware used in the Incident;

(f) Removed access privileges obtained by the malicious actor;

(g) Implemented additional vulnerability scanning across the Group's IT systems to harden the Group's network perimeter;

(h) Strengthened the Group's Active Directory infrastructure;

(i) Implemented additional end point protection, forensic tools, and monitoring tools;

(j) Introduced a shadow security operations centre and initiated transition to a new MSSP;

(k) Initiated plans for an asset lifecycle review to identify legacy critical business applications and treatment required to address cyber risks;

(l) Commenced a logging, monitoring and alerting uplift to review existing policies and standards;

(m) Completed the rollout of multi-factor authentication for all remote access;

(n) Updated organisational measures such as incident response plans, policies, and playbooks; and

(o) Rolled out a cyber awareness programme containing training and assignments for its employees

Findings and Basis for Determination

18 Based on the circumstances of the Incident, the Commission's investigation centred on:

(a) Whether the Organisations had breached their respective obligations under section 26 of the PDPA to not transfer any personal data to a country or territory outside Singapore except in accordance with requirements prescribed under the PDPA (the "**Transfer Limitation Obligation**"); and

(b) Whether the Organisations had breached their respective obligations under section 24 of the PDPA to protect personal data in their possession or under their control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks (the "**Protection Obligation**").

Whether the Organisations had contravened the Transfer Limitation Obligation

19 The HR Platform was implemented on a Group-wide basis on or around July 2013. The Organisations began uploading the personal data of their employees to the HR Platform for storage in the HR Vendor's servers in the European Economic Area around this time, and would have continued to do so as part of the normal course of HR functions (for example, when new employees joined). Any transfers of personal data by the Organisations out of Singapore after 2 July 2014 would have been subject to the Transfer Limitation Obligation and the requirements prescribed in Part III of the Personal Data Protection Regulations 2014 ("**PDPR 2014**"). For transfers of personal data outside of Singapore which occurred after 1 February 2021, such transfers would have been subject to the requirements in Part 3 of the Personal Data Protection Regulations 2021 ("**PDPR 2021**").

20 Regulation 9(1)(b) of the PDPR 2014 and regulation 10(1) of the PDPR 2021 require 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 that is at least comparable to that under the PDPA. Under regulation 10 of the PDPR 2014 and regulation 11(1) of the PDPR 2021, such legally enforceable obligations can be imposed on the recipient organisation under

(a) any law; (b) any contract between the parties; (c) binding corporate rules; or (d) any other legally binding instrument.

21 In gist, the Organisations were required to take appropriate steps to ensure that the personal data transferred out of Singapore via the HR Platform for storage in the European Economic Area would be protected to a standard comparable to under the PDPA, *before* any such transfers were made.

22 There was no evidence of any such steps taken by the Organisations. While the contract between Toll Holdings and the HR Vendor included data protection obligations imposed on the HR Vendor, the Organisations were not party to this agreement. The CSAs also did not contain any provisions relating to the protection of personal data or impose obligations on Toll Holdings to protect the personal data of the other Organisations for the purposes of the centralised corporate functions to be undertaken pursuant to the CSAs. Accordingly, the Organisations were determined to have contravened the Transfer Limitation Obligation in relation to the personal data uploaded on to the HR Platform.

23 In the course of investigations, Toll Holdings represented that it had since reviewed the data transfer arrangements under the CSAs and that the Organisations and Toll Holdings have now executed a "Singapore Data Export Agreement" to govern intra-group transfers of personal data from the Organisations to Toll Holdings (and other members of the Group who may subsequently become party to the agreement) to ensure that a standard of protection comparable to the PDPA is provided to any transferred personal data.

Whether the Organisations had contravened the Protection Obligation

24 As held in *Everlast Projects Pte Ltd and others* [2020] SGPDPC 20, members of a corporate group may satisfy the Protection Obligation by relying on binding group-level written policies or intra-group contracts which specify the respective data protection obligations of the members of the group. In the present case, while the Organisations had entered into the CSAs to centralise various corporate functions with Toll Holdings, the CSAs did not deal with data protection obligations. In the circumstances, the Protection Obligation remained with the Organisations, and the Organisations cannot rely on the CSAs to say that certain of its data protection operations had been centralised with Toll Holdings at the Group-level.

25 That being said, under the CSAs, Toll Holdings had undertaken to provide the Organisations with IT support services. It has been held in *WTS Automotive Services Pte Ltd* [2018] SGPDPC 26 that organisations can rely on the technical expertise of their service providers to satisfy the Protection Obligation (subject to clear instructions or business requirements being specified). In the case where a member of a group of companies provides technical support services to others in the group, it is advisable that their respective roles and responsibilities be clearly spelt out.

26 In the present case, the CSAs were intended to perform this role: Toll Holdings was responsible for IT support services while the Organisations remained responsible for development and implementation of IT systems: see [7] above. As part of the IT support services provided, Toll Holdings introduced and implemented Group-level IT security standards. These were communicated through the Group's intranet and implemented by Toll Holdings on a Group-wide basis, as part of the IT support services they provided. In accordance with these standards, a number of industry-standard technical solutions and tools were implemented prior to the Incident to protect the personal data in the Singapore Servers: see [8] above.

27 Having considered these security arrangements, we are satisfied that the Organisations had not breached their Protection Obligation as the security arrangements in place prior to and at the time of the Incident to protect the personal data in the Singapore Servers were reasonable and consistent with existing industry standards. In coming to this decision, we are also of the view that the security lapse and privilege escalation that enabled the malicious actor to overcome the Organisations' endpoint protections in the Incident occurred abroad arising from theft of credentials from Toll Holdings' vendor and was beyond the control of the Organisations.

The Deputy Commissioner's Decision

28 In determining what directions (if any) should be given to the Organisations pursuant to section 48I of the PDPA, the Deputy Commissioner took into consideration:

(a) the Organisations' cooperation with the Commission's investigations;

(b) that access to the transferred personal data was limited to entities within the same corporate group;

(c) that there was no evidence of any loss or damage resulting from the Organisations' contravention of the Transfer Limitation Obligation; and

(d) that the Group had already implemented intra-group contractual arrangements to govern future transfers of personal data by the Organisations to Toll Holdings.

29 Having considered all the mitigating factors listed above, the Organisations are administered a warning in respect of their breach of the Transfer Limitation Obligation. No other directions are necessary in view of the remedial actions already taken by the Organisations.

YEONG ZEE KIN
DEPUTY COMMISSIONER
FOR COMMISSIONER FOR PERSONAL DATA PROTECTION