PERSONAL DATA PROTECTION COMMISSION

[2022] SGPDPCS 17

Case No. DP-2207-B8974

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

And

CPR Vision Management Pte Ltd

L'Oreal Singapore Pte Ltd

L'Occitane Singapore

SUMMARY OF THE DECISION

1. The Personal Data Protection Commission (the "**Commission**") received data breach notification reports from (i) L'Oreal Singapore Pte Ltd ("**L'Oreal**") on 29 October 2021 and (ii) L'Occitane Singapore Pte Ltd ("**L'Occitane**") on 1 November 2021 respectively of a ransomware attack on their customer relationship management ("**CRM**") system vendor, CPR Vision Management Pte Ltd (the "**Organisation**"). The Organisation is a data intermediary that helped to process personal data collected by L'Oreal and L'Occitane.

2. The ransomware attack affected a server and three network attached storage ("**NAS**") devices in the Organisation's office ("**office network**"), and led to the

encryption of the personal data belonging to 83,640 L'Occitane's customers and 35,079 L'Oreal's customers, which included their name, address, email address, mobile number, NRIC number, date of birth, age, gender, race, nationality, loyalty points and amount spent.

3. The Organisation requested, and the Commission agreed, for this matter to proceed under the Expedited Decision Breach Procedure. To this end, the Organisation voluntarily and unequivocally admitted to the facts set out in this decision. It also admitted to a breach of the Protection Obligation under Section 24 and the Retention Limitation Obligation under Section 25 of the Personal Data Protection Act (the "**PDPA**").

4. The Organisation's internal investigations found the threat actor had first gained access to the office network via a compromised user account VPN connection on 13 October 2021 before executing the ransomware attack on or about 15 October 2021. However, due to the limited data logs available on the Organisation's FortiGate firewall and VPN appliance, the Organisation was not able to determine how the threat actor gained access to the compromised user account VPN. As part of the immediate remediation efforts, the Organisation reset the credentials of the compromised user account VPN and the password credentials of all VPN accounts across the Organisation.

5. The Organisation admitted that its endpoint security solution would have been able to detect and block the unauthorised entry attempts to the office network affected in the Incident. However, the Organisation failed to extend the deployment of this protection solution to the affected office network. This could have been because the domain controller server within the affected office network had been earmarked to be decommissioned after the data was copied to MS365 Sharepoint. Another reason for the omission may have been the fact that the Organisation set up the affected office network for business continuity purposes, when it shifted to its new premises, sometime between 6 – 9 April 2020, on the eve of the nation-wide COVID-19 circuit breaker in Singapore.

6. The Commission finds the Organisation in breach of the Protection Obligation as it failed to have reasonable security arrangements in place to protect the personal data in its possession and control. As a CRM system vendor, the Organisation processes and processed a high volume of web traffic containing personal data on behalf of many e-commerce retailers, including L'Oreal and L'Occitane, and would ordinarily be held to a higher standard. The Organisation's omission to deploy its endpoint security solution to the affected office network suggests that the Organisation failed to maintain an inventory of its data assets.

7. Even if there were extenuating circumstances in April 2020 which could have partly excused the Organisation's omission to include the affected office network in its data inventory, it was inexcusable for the Organisation to let this state of affairs

persist for more than one and-a-half years, from April 2020 until October 2021. We should add however, that as part of its remediation efforts, the Organisation has since ensured that its endpoint security solution was deployed to all office and end-user devices.

8. The Organisation also admitted to being in breach of the Retention Limitation Obligation. The Organisation admitted that the affected personal data in the Incident had been legacy content, which should have been deleted together with the domain controller server earmarked for decommissioning, and for which no business or legal purpose existed for retention. The Organisation highlighted however, that this lapse was not in accordance with its own data retention policy. Had the Organisation complied with the Retention Limitation Obligation and deleted the personal data in question, the Incident would not have amounted to a breach of the Retention Limitation Obligation under the PDPA.

9. In the course of our investigations, L'Oreal furnished documentary evidence which showed that L'Oreal had specifically instructed the Organisation, pursuant to its data retention policies, to delete the affected personal data on 26 March 2021. This was duly acknowledged by the Organisation, and the Organisation furnished a purported Certificate of Destruction dated 17 May 2021 stating that the personal data had been deleted on 6 May 2021.

10. Similarly, L'Occitane also raised its concerns that the Organisation failed to seek its prior written consent before duplicating the personal data to other non-production environments.

11. The Commission is satisfied that neither L'Oreal nor L'Occitane had any knowledge of the retention and storage of the legacy personal data by the Organisation on the affected NAS device; and neither had any control over the NAS device used by the Organisation to store the personal data affected by the ransomware attack. Both L'Oreal and L'Occitane had also adequately provided in their contracts with the Organisation to ensure compliance with the Protection and Retention Limitation Obligations under the PDPA. The Commission is therefore of the view that despite the personal data breach incident, L'Oreal and L'Occitane had acted consistently with and complied with the relevant obligations under the PDPA.

12. Having considered the circumstances set out above, including the Organisation's upfront admission of liability, and the fact that data analysis conducted by the data security team of the Organisation's parent company did not uncover any evidence to suggest that data exfiltration or modification had occurred, the Commission considered that it would be most appropriate in lieu of imposing a financial penalty, to direct the Organisation to comply with the following action:

    a. Conduct a thorough security audit (with report) of its technical and administrative arrangements for the protection of personal data in its possession or control;

    b. Rectify any security gaps identified in the security audit report;

c. Conduct a comprehensive review of all of the Organisation's databases containing personal data to ensure full compliance with the Retention Limitation Obligation under Section 25 PDPA;

d. Review and update the personal data policies of the Organisation as applicable, including clarification of the roles of data intermediaries and vendors in complying with the Retention Limitation Obligation under section 25 of the PDPA, within 60 days from the date the security audit report is delivered to the Organisation; and

e. Inform the Commission within 1 week of the completion of the steps directed above.

The following are the provision of the Personal Data Protection Act 2012 cited in the above summary:

Protection of personal data

24. An organisation must protect personal data in its possession or under its control by making reasonable security arrangements to prevent –

(a) unauthorised access, collection, use, disclosure, copying, modification or disposal or similar risks and;
(b) the loss of any storage medium or device on which personal data is stored.

Retention of personal data

25. An organisation must cease to retain its documents containing persona data, or remove the means by which the personal data can be associated with particular individuals, as soon as it is reasonable to assume that –

(a) the purpose for which the personal data was collected is no longer being served by retention of the personal data; and
(b) retention is no longer necessary for legal or business purposes.