PERSONAL DATA PROTECTION COMMISSION

Case No. DP-2006-B6449

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

And

Seriously Keto Pte. Ltd.

SUMMARY OF THE DECISION

1. On 16 June 2020, Seriously Keto Pte Ltd (the "**Organisation**") notified the Personal Data Protection Commission (the "**Commission**") of a ransomware infection that occurred on or about 15 June 2020 (the "**Incident**"). The affected personal data comprised approximately 3,073 individuals' names, addresses, email addresses and telephone numbers ("**the Affected Personal Data**").

2. The Organisation requested that the Commission investigate the Incident under its Expedited Decision Procedure. In this regard, the Organisation voluntarily provided and unequivocally admitted to the facts set out in this decision. It also admitted that it was in breach of the Protection Obligation under section 24 of the Personal Data Protection Act (the "**PDPA**").

3. Investigations revealed the presence of an unprotected file in the Organisation's network infrastructure which contained unencrypted login credentials to access the server containing the Affected Personal Data. The unprotected file could be located by infrastructure scanning, and this provided a channel for unauthorised access to the server. Server logs retrieved by the Organisation after the Incident indicated that there had been unauthorised access to the file.

4. The Organisation admitted that it had failed to conduct any periodic security reviews prior to the Incident which could have revealed the existence of the unprotected file within its network infrastructure.

5. The Organisation had engaged a vendor to develop its e-commerce and membership website and claimed to have relied on the vendor to make the necessary security arrangements to protect the Affected Personal Data. However, in this case, there were no clear business requirements (e.g. contractual stipulations) specifying that the Organisation was relying on the vendor to recommend and/or implement security arrangements to protect personal data hosted in the e-commerce and membership website that the vendor was engaged to develop. Protection of personal data in the possession or under the control lies primarily with the Organisation, although it may contract the operations to a vendor who is more knowledgeable and with expertise. To do so, the Organisation has to be clear about the scope of outsourcing and the vendor has to also agree to do so. In the absence of clear outsourcing, the responsibility to implement reasonable security arrangements to protect the Affected Personal Data remained squarely with the Organisation.

6. Overall, the Organisation admitted that it had failed to give due attention to personal data protection prior to the Incident and had neglected to implement reasonable security arrangements to protect the Affected Personal Data.

7. In the above circumstances, the Deputy Commissioner for Personal Data Protection finds that the Organisation negligently contravened the Protection Obligation under section 24 of the PDPA.

8. Following the Incident, the Organisation underwent a full security audit and remedied vulnerabilities identified. The Organisation also set up a new website with a more robust internal security infrastructure, implemented a mandatory password change for all users of its new website, and activated a firewall to safeguard access to the new website. It also engaged a cybersecurity vendor to develop further

measures and policies to strengthen its internal IT infrastructure. Additionally, the Organisation committed to engaging consultants to improve its data protection policies and outsource data protection functions.

9. The Organisation cooperated with the Commission's investigation, admitted to its breach of the Protection Obligation, and took prompt remedial action. There was no evidence of exfiltration of the Affected Personal Data, and the Organisation was able to restore the Affected Personal Data from a backup and did not lose any data as a result of the Incident. The practice of having regular and separately located data backup(s) is to be encouraged to prevent organisations from losing data to ransomware.

10. Having considered the above circumstances and the factors listed at section 48J(6) of the PDPA, the Deputy Commissioner for Personal Data Protection requires the Organisation to pay a financial penalty of $8,000 within 30 days from the date of the notice accompanying this decision, 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.

11. In view of the remedial actions taken by the Organisation, no other directions are necessary.