PERSONAL DATA PROTECTION COMMISSION

Case No. DP-2013-B8138

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

And

Vhive Pte Ltd

SUMMARY OF THE DECISION

1. On 26 March 2021, Vhive Pte Ltd (the "**Organisation**") notified the Personal Data Protection Commission (the "**Commission**") of a ransomware attack that affected its customer database (the "**Incident**"). Approximately 186,281 individuals' names, addresses, email addresses, telephone numbers, hashed passwords and customer IDs were affected.

2. The Organisation subsequently requested for this matter to be handled under the Commission's expedited breach decision procedure. This means that the Organisation voluntarily provided and unequivocally admitted to the facts set out in this decision, and admitted that it was in breach of section 24(a) of the Personal Data Protection Act (the "**PDPA**").

3. The Organisation's forensic investigation results revealed that the Organisation's IT infrastructure had been outdated, with multiple vulnerabilities at the time of the Incident. The Organisation's e-commerce server ran on an outdated webserver service. This, together with an unpatched firewall, allowed the threat actor to

remotely execute unauthorised code on the e-commerce server, and gained backdoor access to the e-commerce server to carry out the ransomware attack.

4. The Organisation had engaged an IT vendor to host, manage and maintain the e-commerce server and all its other IT systems. However, our investigations revealed that despite the purported "engagement", there was in fact no written contract between the Organisation and its IT vendor at the time of the Incident.

5. In Re Spize Concepts Pte Ltd [2019] SGPDPC 22 at [22], we had stated that section 4(2) of the PDPA imposes on organisations that engage data intermediaries to do so "pursuant to a contract which is evidenced or made in writing". In that case, we also highlighted that one specific category of policies and practices under section 12(a) of the PDPA that an organisation should develop and implement is the contractual documentation relating to the scope of the data intermediary relationship, and failure to do so would amount to a breach. The raison d'etre is that the outsourcing of data processing activities must be clearly scoped, and the respective roles and responsibilities between the organization and the data intermediary clearly identified from the outset. In the absence of any written contract and the lack of evidence to show the scope, roles and responsibilities of the data processing outsourcing, the Organisation remained solely responsible for complying with the obligations under the PDPA, including the obligation to make reasonable security arrangements to protect the personal data in its possession or under its control under section 24 of the PDPA.

6. The Organisation's outdated webserver was used to host the Organisation's website and its online storefront. In this regard, the Commission had previously

issued a Guide on Building Websites for SMEs in 2016, which was subsequently updated and revised in July 2018. In this Guide, the Commission emphasized the importance of ensuring the protection of personal data and the security of the website throughout the life cycle, including ensuring the clear delineation of responsibilities when an organization engages an IT vendor.

7. We wish to reiterate our observations in [4.2.1] of the Guide, where we highlighted the need to consider and properly document an IT vendor's scope of work, and stated as follows:

> Organisations should emphasise the need for personal data protection to their IT vendors, by making it part of their contractual terms. The contract should also state clearly the responsibilities of the IT vendor with respect to the PDPA. When discussing the scope of outsourced work, organisations should consider whether the IT vendor's scope of work will include any of the following:
>
> - Requiring that IT vendors consider how the personal data should be handled as part of the design and layout of the website.
>
> - Planning and developing the website in a way that ensures that it does not contain any web application vulnerabilities that could expose the personal data of individuals collected, stored or accessed via the website through the Internet.
>
> - Requiring that IT vendors who provide hosting for the website should ensure that the servers and networks are securely configured and adequately protected against unauthorised access.
>
> - Requiring IT vendors to ensure that all work done is fully documented and that all documentation is handed over to the organisation at the completion of the project. Documents should capture the website's requirements, design specifications, user test scripts, user test results, as well as server and network configurations.
>
> - When engaging IT vendors to provide maintenance and/or administrative support for the website, requiring that any changes they make to the website do not contain vulnerabilities that could expose the personal data. Additionally, discussing whether they have technical and/or non-technical processes in place to prevent the personal data from being exposed accidentally or otherwise.

- Requiring that IT vendors providing maintenance and/or administrative support to ensure that all changes to the website are secure and documented, and that the document is kept up to date.

8. The Organisation admitted the weakness in its IT infrastructure and its failure to give due attention to the protection of the personal data of its customers had contributed to the Incident.

9. On the facts, the Organisation's failure to ensure that there was a written contract with its IT vendor not only meant that there was a lack of clarity on the scope of work expected from the IT vendor, but also that the Organisation had failed to stipulate clear written security maintenance requirements and data protection requirements to its IT vendor to ensure the protection of personal data it was in control or in possession of. This ultimately resulted in a lack of system maintenance, including security maintenance by the Organisation.

10. Investigations further revealed that the Organisation did not have a security maintenance policy, which would have made up for the lack of specification of these requirements to its IT vendor, nor did the Organisation conduct any of its own scheduled security reviews, through which it could have detected any security inadequacy or vulnerabilities within its IT infrastructure.

11. In the above circumstances, the Organisation is found to have breached the Protection Obligation under section 24(a) of the PDPA.

12. Following the Incident, the Organisation decommissioned its e-commerce webserver and overhauled its IT infrastructure. Apart from deciding to conduct online sales solely through third party websites, the Organisation also rebuilt its ERP server in a secure environment with new set of firewalls, updated its

operating systems and software, implemented the use of SSL-VPN for remote access, and engaged a new IT vendor with the data security and data protection provisions properly specified in a written contract. The Organisation also reviewed and updated all its internal policies relevant to the protection of personal data.

13. In deciding the appropriate outcome in this case, the Commission acknowledges the cooperation extended by the Organisation to the Commission throughout the course of our investigations. The Organisation had also voluntarily admitted to its breach of the Protection Obligation, and took prompt remediation actions to address its security gaps. The Organisation was able to restore fully the personal data affected without loss, thereby minimizing any disruptions to its operations.

14. Having considered the circumstances set out above and the factors listed at section 48J(6) of the PDPA, the Commissioner for Personal Data Protection hereby finds the Organisation in breach and requires the Organisation to pay a financial penalty of $22,000 within 30 days from the notice accompanying date 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.

15. In view of the remedial action by the Organisation, no directions under section 48I are necessary.

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

Protection of personal data

24. An organisation shall 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, disposal or similar risks; and

(b) the loss of any storage medium or device on which personal data is stored.