PERSONAL DATA PROTECTION COMMISSION

Case No. DP-2003-B6000

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

And

Tripartite Alliance Limited

SUMMARY OF THE DECISION

1. On 3 March 2020, Tripartite Alliance Limited (the "**Organisation**") notified the Personal Data Protection Commission (the "**Commission**") that a server hosting its customer relationship management ("**CRM**") system was infected with ransomware on or around 17 February 2020.

2. The Organisation subsequently requested for this matter to be handled under the Commission's expedited breach 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 section 24 of the Personal Data Protection Act (the "**PDPA**").

The Incident

3. The Organisation is in the business of promoting fair and progressive employment practices, as well as providing mediation and advice in employment–related disputes.

4. The CRM system is a Software-as-a-Service ("**SaaS**") solution provided by a software service provider engaged by the Organisation (the "**Vendor**"). The Organisation uses the CRM system to handle employment-related enquiries, feedback and complaints.

5. At the time of the incident, the CRM system contained approximately 12,000 individuals' and 8,000 companies' data (including information of the companies' representatives). The types of data affected for each individual varied, but may include an individual's name, identification number, contact number, email address, age, race, marital status, salary and compensation amount (if applicable).

6. On 17 February 2020, the CRM system was unavailable to users. The Vendor managed to restore the CRM system from a back-up copy within the next three hours.

7. Upon investigations, the Organisation determined that the CRM system suffered a ransomware attack. In particular, security logs obtained from the Vendor showed that hacking attempts were made on the database server between 7 and 14 February 2020.

8. The Organisation claimed that it had, since June 2019, expanded the scope of the IT services procured from the Vendor to include security monitoring services for the CRM system, such as the blocking of cyber-attacks based on alerts. However, there was inadequate process put in place to ensure that the Vendor proactively monitor the alerts and take actions to block malicious activities in a timely manner. Nevertheless, the

Organisation accepts that it had the responsibility to ensure that the Vendor had the same understanding on its duty of care under the monitoring services contract and to oversee and supervise the work of the Vendor through clear instructions on regular reporting and updates by the Vendor.

9. Following the incident, the Organisation started close monitoring of the Vendor's IT services support on a weekly basis to ensure timely update of patches and follow-ups on security alerts received. The Organisation also undertook an organisation-wide review to strengthen its management of all its third-party IT service providers, such as requesting these service providers to conduct cybersecurity audits, vulnerability assessment and penetration testing for the Organisation's existing IT systems. The Organisation also informed the Commission that it will be migrating to a new CRM system and is currently working to terminate the existing CRM system.

10. The Organisation informed the Commission that the database in the CRM system was not protected by encryption at the time of the incident, which made the database vulnerable for exposure. However, there was no evidence that the hacker had exfiltrated the database.

The Organisation's Admission and the Commission's Decision

11. The Organisation admitted that it had breached the Protection Obligation under section 24 of the PDPA in failing to ensure that the Vendor had duly discharged its contractual data protection obligations. In particular, the Organisation admitted that it had not

monitored the Vendor's performance to ensure that the Vendor met the required information security standards.

12. As stated in previous decisions by the Commission[1], organisations have to give proper instructions and exercise reasonable oversight over their vendors to ensure that their outsourced providers are indeed delivering the services contracted. Without reasonable oversight, the risk from any failure will fall on the organisation. In the circumstances, the Commissioner found that the Organisation was in breach of the Protection Obligation under section 24 of the PDPA.

13. As for the Vendor, it was a SaaS provider who provided the CRM system, including maintenance support, and security monitoring services. These services did not entail the processing of personal data. As such, the Vendor was not a "data intermediary" of the Organisation. Accordingly, the Vendor was not responsible for the protection of the individuals' personal data under the PDPA in respect of the incident.

14. In determining the directions to be imposed on the Organisation for the breach, the Commissioner took into account the following factors:

[1] See for example, *Re Smiling Orchid (S) Pte Ltd and Ors* [2016] SGPDPC 19, *Re Royal Caribbean Cruises (Asia) Pte Ltd* [2020] SGPDPC 5, and *Re SCAL Academy Pte. Ltd.* [2020] SGPDPC 2.

Aggravating

(a) The high number of affected individuals, which is approximately 20,000;

(b) The nature of the affected data. In particular, the database contained details of employment-related complaints and disputes. Individuals would expect a high level of confidence when they convey such matters to the Organisation for handling;

Mitigating

(c) The Organisation's upfront admission of breach of the Protection Obligation, and the prompt remedial actions to mitigate the effects and prevent recurrence of the incident; and

(d) There was no evidence of exfiltration of the database in the CRM system.

15. On account of the above, the Organisation is directed to pay a financial penalty of $29,000 within 30 days from the date of this direction. In view of the remedial action of the Organisation, the Commission will not be issuing any other directions.