**PERSONAL DATA PROTECTION COMMISSION**

**[2025] SGPDPCS 1**

Case No. DP-2408-C2786

29 December 2025

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

And

(1) SESAMi (Singapore) Pte Ltd

(2) Abecha Pte Ltd

## SUMMARY OF THE DECISION

1 SESAMi (Singapore) Pte Ltd ("**SPL**") is a B2B e-commerce service provider that offers solutions for value chain processes. Abecha Pte Ltd ("**APL**"), a wholly-owned subsidiary of SPL, is an authorised reseller of ESSO fuel and managed an Abecha-ESSO Corporate Fleet Discount Programme (the "**ESSO Programme**") for corporations and corporate employees. ESSO is not involved in the events.

2 On 14 August 2024, SPL notified the Personal Data Protection Commission (the "**Commission**") of unauthorised access to its servers by a threat actor ("**TA**")

and encryption of files containing personal data, on or around 13 August 2024 (the "**Incident**").

3 On 18 November 2024, SPL applied for the investigation to proceed under the Expedited Decision Procedure ("**EDP**"), which the Commission acceded to. To this end, SPL voluntarily and unequivocally admitted to the facts set out in this decision, and to SPL's breach of section 24 of the PDPA.

**Facts of the Case**

4 On 13 August 2024, SPL employees discovered that they were unable to access the Network Accessible Storage (NAS)[1] on the office network that was shared by SPL and APL (the "**Shared Drive**"). Files containing personal data which were stored on the Shared Drive (the "**Affected Data**") were encrypted and a ransom note was found.

5 Apart from the Shared Drive, the Incident also affected virtual machines on a server located at Kim Chuan Telecommunications Complex 1 ("**KC1**"), which contained SPL's cloud infrastructure and three workstations. However, the KC1 server did not contain any Affected Data.

6 SPL admitted that it was responsible for maintaining and managing the shared office network, including the Shared Drive and the other affected systems. This also included being responsible for securing the network.

[1] An NAS is a storage device connected to a network that allows multiple authorised users and devices to store, access and share data from a central location.

7 The Affected Data consisted of the following:

(a) The personal data of approximately 20,471 individuals who had been customers and/or ex-customers of the ESSO Programme (the "**Group 1 Data**"), broken down as follows. APL had collected the Group 1 Data from these customers in order to process payment, requiring them to submit credit card details or bank account details for GIRO deductions.

| **Group 1 Data** | |
|---|---|
| **Personal Data Affected** | **No. of Affected Individuals** |
| - Name<br>- Bank details for GIRO deductions, namely, bank account number, bank code, branch code and purchase amount<br>- Transaction data, namely, transaction date and time, purchase amount, reference number and transaction type | 9,695 |
| - Unexpired credit card information – full credit card number with expiry date, but without CVV, name, images or scans | 4,018 |
| - Expired credit card information – full credit card number with expired expiry | 6,758 |

| | |
|---|---|
| date, but without CVV, name, images or scans | |

(b) The personal data of up to 18,837 individuals whose data had been collected by SPL as part of companies' registration for its B2B e-commerce platform (the "**Group 2 Data**"), broken down as follows.

| **Group 2 Data** | |
|---|---|
| **Personal Data Affected** | **No. of Affected Individuals** |
| - Name<br>- Unexpired credit card information<br>- Bank details for GIRO deduction, including bank account numbers | Up to 6,026 |
| - Billing-related details that are no longer valid, e.g., expired credit card information | Up to 12,811 |

8 The Commission found no evidence to suggest that any of the Affected Data was exfiltrated.

9 Due to insufficient forensic evidence, including the limited availability of firewall logs, SPL and APL were unable to definitively determine how the TA

gained initial access to the Affected Data. However, the investigations established the following lapses that could have contributed to the Incident:

(a) Important security software had not been installed or kept up-to-date. SPL's firewall and VPN firmware were unpatched and at end-of-life. Furthermore, SPL did not install any endpoint detection and response solutions, and its installed antivirus was not up-to-date;

(b) Poor password management and access controls. Password rotation was not implemented for the KC1 server, and SPL's password and access control policies (which SPL also implemented and enforced for APL), which included the requirement for VPN/administrator accounts to have multi-factor authentication (MFA), were not strictly enforced. Since the KC1 server is linked to SPL's and APL's systems, the TA could have used it as an entry point to access the Shared Drive; and

(c) Files containing personal data were not encrypted at the file level. If the files were encrypted, the TA would not have been able to access the personal data contained therein.

*Remedial Action*

10 After the Incident, SPL and APL respectively informed the individuals whose Group 2 Data and Group 1 Data were affected in the Incident. SPL also took the following remedial actions:

(a) Implemented endpoint detection and response solutions across all endpoints and servers;

(b) Implemented / strictly enforced password rotation and MFA policies;

(c) Disconnected the KC1 servers and migrated all customers to another cloud computing platform (Microsoft Azure); and

(d) Migrated files containing personal data from the Shared Drive to Office 365 Sharepoint.

**Findings and Basis for Determination**

*Whether SPL was data intermediary for APL*

11 The Commission finds that SPL was, at the time of the Incident, a data intermediary for APL in respect of the Group 1 Data:

(a) SPL was responsible for maintaining and managing the Shared Drive, and accordingly processed the Group 1 Data on APL's behalf;

(b) Where an organisation processes personal data on behalf of another organisation, the absence of a written contract as in this case, does not absolve the first organisation from being a data intermediary (and being subject to the attendant obligations); and

(c) While a written contract is not required in order to find a data controller-data intermediary relationship, it is well-established that a data controller should have in place a written contract with its data intermediary that clearly specifies the data intermediary's duties to protect personal data. Where the data controller and data intermediary belong to the same group of companies, this written contract requirement may be met instead by binding group-level written policies, intra-group agreements or binding corporate rules ("**BCRs**")[2].

12 SPL was also the data controller in respect of the Group 2 Data collected by it, as it processed the Group 2 Data for the purposes of its own B2B e-commerce platform.

*Whether SPL had contravened the Protection Obligation*

13 Under section 24(a) of the PDPA (the "**Protection Obligation**"), organisations must protect personal data in their possession or under their control

[2] See *Re (1) Everlast Projects Pte Ltd (2) Everlast Industries (S) Pte Ltd (3) ELG Specialist Pte Ltd* [2020] SGPDPC 20 at [18].

by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification or disposal, or similar risks.

14 Taking into account SPL's admissions, and for the reasons set out below, the Deputy Commissioner determines that SPL failed to implement reasonable security arrangements to protect the personal data in its possession and/or under its control, thus contravening the Protection Obligation. This applies to SPL in its capacity as both (i) the data controller in respect of the Group 2 Data; and (ii) the data intermediary for APL in respect of the Group 1 Data. Particulars of the breach are stated below:

(a) Failure to ensure that security arrangements were in place and up-to-date. SPL admitted that it had failed to update its firewall, VPN firmware and its antivirus software, which heightened the risk of unauthorised access by threat actors. Furthermore, the Commission found no evidence of any patch management process or periodic security review, which would have assisted in detecting vulnerabilities. Endpoint detection and response solutions were also not installed; and

(b) Failure to implement reasonable access controls. The sensitive nature of some of the personal data in SPL's possession, e.g., full credit card numbers and bank account details, meant that SPL should have implemented enhanced access controls such as (i) MFA for VPN / administrator accounts; (ii) network segmentation to isolate

critical systems between its datacenter and office network; and (iii) periodic blacklisting of unauthorised applications to proactively prevent the installation of tools that could be used for malicious activity. However, SPL failed to take any of these measures. SPL also admitted that its password policy, which also included other requirements such as password rotation and password complexity, was not strictly enforced.

15 For the above reasons, SPL is found to have negligently breached the Protection Obligation under section 24 of the PDPA.

*Whether APL had contravened the Protection Obligation*

16 The Commission notes that the lapses outlined above are, in the first instance, failures on the part of SPL as the entity responsible for maintaining and managing the shared office network, including the Shared Drive. However, pursuant to section 4(3) of the PDPA, APL also owed an obligation as data controller for the Group 1 Data to ensure that reasonable security arrangements were implemented. However, APL did not take this or any other step to ensure that SPL implemented reasonable security arrangements to protect the Group 1 Data.

17 The Commission recognises that APL is a subsidiary of SPL and did not have the autonomy to depart from centrally-managed group-level security arrangements, or lack thereof. However, subsidiaries are still required to comply

with a minimum standard of conduct in such situations[3], namely (i) a subsidiary should not adopt group-level data protection policies without considering whether these need to be adapted to their circumstances and contexts; and (ii) when there is a centralisation of corporate functions, group-level policies should be put in place such that roles and responsibilities are clear.

18 APL fell short of this minimum standard, and accordingly, APL is found to have negligently breached the Protection Obligation under section 24 of the PDPA.

**The Deputy Commissioner's Decision**

*Financial Penalty*

19 The Commission considers that it would be appropriate to impose a financial penalty on SPL under section 48J of the PDPA, given the negligent contravention of the Protection Obligation and its role as the organisation responsible for managing the shared network and protecting the personal data contained therein.

20 In deciding the appropriate amount of financial penalty to be imposed on SPL, the Commission first considered the type of personal data affected, the fact that there was no exfiltration of the Affected Data, and the nature of SPL's non-compliance with the PDPA. In addition, in order to ensure that the financial penalty imposed is proportionate and effective, having regard to achieving compliance and

[3] See *Re J & R Bossini Fashion Pte Ltd* [2021] SGPDPC 9 at [22].

deterring non-compliance with the PDPA, the Commission also considered SPL's turnover.

21 The Commission also considered the following factors:

(a) SPL was cooperative during the course of investigations;

(b) SPL took prompt and effective remediation actions; and

(c) SPL voluntarily admitted to breach of the Protection Obligation under the EDP.

22 For the reasons above, the Deputy Commissioner hereby requires SPL to pay a financial penalty of $8,750 for its breach of the Protection Obligation within 30 days of the date of the relevant notices 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.

23 Notwithstanding that a financial penalty may have been imposed on APL as well for its negligent breach of the Protection Obligation under section 24 of the PDPA, the Commission determines that it is appropriate in this case to impose a financial penalty on SPL only, given that:

(a) While APL failed to meet the minimum standard of conduct stipulated at [17] above, its limited autonomy as a wholly-owned

subsidiary of SPL meant that its level of culpability was relatively lower;

(b) SPL was the central actor in the Incident, being responsible for maintaining and managing the shared office network; and

(c) The Commission is of the view that the quantum of the financial penalty imposed on SPL alone would be proportionate and effective in achieving the objectives stated in section 48J(6)(h) of the PDPA, namely, achieving compliance and deterring non-compliance with the PDPA, in relation to both SPL and APL.

24 That said, the Commission's approach in this case should not be taken as indicative of any general approach to matters involving multiple entities from the same corporate group.

*Directions*

25 In addition, to ensure SPL's compliance with the PDPA, the Deputy Commissioner directed SPL to carry out the following within 90 days of the relevant notices accompanying this decision:

(a) Enforce a strong password policy across its network, including internal guidelines for strong passwords and use of MFA for administrator accounts, and evaluate the need to implement

password management solutions to manage local administrator passwords;

(b) Develop a documented process to conduct periodic security reviews for all systems and software across SPL's IT infrastructure and network, at least annually;

(c) Establish a robust patch management process to regularly update and apply security patches to all systems and software;

(d) Evaluate and implement network segmentation to isolate critical systems and sensitive data;

(e) Improve logging of firewall, VPN authentication and server events, with logs to be retained in a central repository for a minimum of 30 days;

(f) Implement whitelisting of approved applications that are allowed to run on the network and blacklisting of unauthorised applications to proactively block malicious activity;

(g) Ensure robust user access controls and logging capabilities are enabled on SPL's IT infrastructure and network post-data migration; and

(h) Prepare and submit to the Commission a written report (accompanied by documentary proof) on SPL's compliance with the above directions.

26 To ensure APL's compliance with the PDPA, the Deputy Commissioner also directed APL to carry out the following within 90 days of the relevant notices accompanying this decision:

(a) Implement documented policies to stipulate data intermediary roles and data protection responsibilities in an intra-group agreement, contracts, BCRs or similar legal requirements for compliance with the PDPA;

(b) Review the necessity to collect GIRO / credit card personal data and, where collection is assessed to be necessary, make reasonable data protection policies to ensure organisational compliance with the PDPA; and

(c) Prepare and submit to the Commission a written report (accompanied by documentary proof) on APL's compliance with the above directions.

**WONG HUIWEN DENISE**
**DEPUTY COMMISSIONER**
**FOR PERSONAL DATA PROTECTION**

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.