**PERSONAL DATA PROTECTION COMMISSION**

**[2023] SGPDPCS 2**

Case No. DP-2206-B9934

In the matter of an investigation under section 50(1) of the

Personal Data Protection Act 2012

And

Sembcorp Marine Ltd

## SUMMARY OF THE DECISION

1. On 25 July 2022, Sembcorp Marine Ltd (the "**Organisation**") notified the Personal Data Protection Commission (the "**Commission**") of a personal data breach that had occurred through the exploitation of the Log4J zero-day vulnerability (the "**Incident**").

2. As a result of the Incident, the personal data of 25,925 individuals was exfiltrated. The personal data affected included their name, address, email address, NRIC number, telephone number, passport number, photograph, date of birth, bank account details, salary, and medical screening results.

3. The Organisation engaged an external cybersecurity company, Sygnia, to investigate the Incident. Its investigations found that the threat actor had exploited three Log4J vulnerabilities present in an application (the "**Application**") to gain unauthorised access to a server as early as on 4 January 2022. The threat actor also deployed the "Cobalt Strike" beacon, conducted reconnaissance, and made lateral movements across several machines, before exfiltrating data between 10 and 23 June 2022, and deploying a ransomware on 28 June 2022.

4. Threat intelligence research revealed that the ransomware campaign which affected the Organisation began targeting users of the Application in January 2022. Given that reports of the Log4J vulnerability were first made in December 2021, it would have been difficult for the Organisation to detect and prevent the infiltration when it was one of the early targets, having been infiltrated as early as 4 January 2022.

5. After finding out about the Log4J vulnerability, the Organisation took prompt actions to identify instances of Log4J vulnerabilities across all the software application it was using. The Organisation started identifying instances of Log4J vulnerabilities across its systems on 14 December 2021. It applied the security patches immediately when they were made available by the respective software vendors. The Organisation also implemented workarounds recommended by the vendors, for systems which patches were not available or had not been released. Additional measures such as blocking incoming and outgoing Log4J traffic were also taken.

6. We are satisfied that the Organisation had made reasonable security arrangements to protect personal data in its possession and/or control in relation to the Incident. The Organisation had in fact adopted good practices in relation to its Information and Communications Technology (ICT) systems. This included a cybersecurity testing programme, regular vulnerability assessment and penetration testing, and cyber security monitoring.

7. In view of the above, the Deputy Commissioner for Personal Data Protection is satisfied that the Organisation had met its Protection Obligation under section 24 of the PDPA. No enforcement action therefore needs to be taken in relation to the Incident.

The following provision(s) of the Personal Data Protection Act 2012 had been 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.