PERSONAL DATA PROTECTION COMMISSION

Case No. DP-2004-B6182

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

And

Water + Plants Lab Pte. Ltd.

SUMMARY OF THE DECISION

1. On 9 April 2020, Water + Plants Lab Pte. Ltd. (the "**Organisation**") informed the Personal Data Protection Commission of a ransomware infection that rendered the Organisation's server (the "**Server**") inaccessible to the Organisation (the "**Incident**").

2. The Incident occurred on or around 30 March 2020. Personal data of 28 employees were encrypted by the ransomware. The personal data affected included the employees' name, NRIC/FIN/Work Permit number, address, date of birth, mobile number and photograph.

3. Investigations revealed that an employee from the Organisation had downloaded and opened an email attachment that contained ransomware. At the time of the Incident, the Organisation had some security measures in place, for example, it had anti-virus protection, and access rights and password control for the Server. It also had a good practice of performing regular backup of its Server, and most of the data was successfully

restored from an external backup. The Organisation therefore suffered minimal data loss as a result of the Incident.

4. However, as admitted by the Organisation, it had not carried out any patching and security scanning of the Server in the 12 months preceding the Incident. Patching and regular security scanning are important security measures to prevent vulnerabilities in an organisation's ICT systems which a hacker may exploit in compromising personal data. For this reason, the Deputy Commissioner for Personal Data Protection found that the Organisation had failed to protect the personal data in its possession or under its control, in breach of section 24 of the Personal Data Protection Act 2012.

5. Following the Incident, the Organisation installed a firewall with greater capabilities to protect the Organisation against external threats, for example, possessing deeper content inspection capabilities to identify malware. The Organisation had also conducted staff training on personal data protection and on how to identify security threats.

6. Upon consideration of the facts, including the impact from the breach, the remediation action taken by the Organisation and that there was no evidence of exfiltration of the data in the Server, the Deputy Commissioner issued a warning to the Organisation.