PERSONAL DATA PROTECTION COMMISSION

Case No. DP-2004-B6162

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

And

Worksmartly Pte. Ltd.

SUMMARY OF THE DECISION

1. On 2 April 2020, Roche Singapore Pte Ltd ("**Roche**") informed the Personal Data Protection Commission (the "**Commission**") of a data security incident involving its former vendor, Worksmartly Pte. Ltd. (the "**Organisation**"). Roche had detected an unauthorised disclosure of their employees' data on GitHub repository ("**GitHub**") on 3 March 2020 (the "**Incident**").

2. The Organisation subsequently requested for this matter to be handled under the Commission's expedited 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 sections 24 and 25 of the Personal Data Protection Act (the "**PDPA**").

Background

3. The Organisation was engaged by Roche in 2017 to provide finance and payroll processing services. In order for the Organisation to provide the said services, Roche handed over its employees' personal data to the Organisation. The contract between the parties was subsequently terminated, and the Organisation's last day of service was 31 December 2018.

The Incident

4. On or around 28 February 2020, one of the Organisation's employees uploaded a file on the Organisation's GitHub account (the "**File**"). When doing so, the employee changed the setting of the GitHub account from "private" to "public" under the mistaken belief that the File would only be accessible to other members of the Organisation. In fact, the change in setting had resulted in the File being accessible to the public.

5. The File contained the personal data of 308 individuals, which comprised Roche's current and former employees (the "**Employees**"), and their dependents (the "**Dependents**"). The personal data included:

    a. For the Employees: name, NRIC/FIN/Passport number, address, date of birth, race, citizenship, employee ID, Roche email address, role title, employment commencement date, salary, bank account name and numbers and name of bank; and

    b. For the Dependents: name, NRIC/FIN/Passport number, date of birth and contact number.

6. The File was used for data migration during the initial service engagement in 2017. The File was supposed to have been deleted—along with other files containing Roche's employees' data—before the Organisation's last day of service, i.e. 31 December 2018. However, because the File was stored in a different folder from the other files, the Organisation had inadvertently omitted to delete the File. This led to the File being exposed to the public when the Organisation's employee set the GitHub folder's setting to "public" as stated at [4] above.

7. The File was exposed to the public for a period of five days from 28 February 2020 to 3 March 2020. Based on GitHub's logs, the repository containing the File was accessed 23 times and downloaded 11 times during this time.

The Contraventions

8. The Organisation admitted that it lacked checks to manage the correct security settings of its GitHub account and had relied solely on employees to do the right thing. The Organisation also admitted that it had not conducted the necessary housekeeping and maintenance of files, which resulted in retaining the File when it was no longer required for business or legal purposes.

9. In the circumstances, the Deputy Commissioner for Personal Data Protection finds the Organisation in breach of the Protection Obligation under section 24 and Retention Obligation under section 25 of the PDPA.

10. Upon realising the Incident, the Organisation took the following remedial action:

    a. Immediately set the GitHub access to "private" and deleted the File;

    b. Reset the passwords for all the databases and servers;

    c. Conducted housekeeping to ensure removal of obsolete files from GitHub;

    d. Directed its GitHub account administrator to always set the repositories to "private" and introduced a disciplinary framework for the mishandling of its GitHub accounts.

The Decision

11. The Deputy Commissioner for Personal Data Protection notes that the Organisation had admitted to a breach of Protection and Retention Obligations under the PDPA, and had cooperated with the Commission's investigation and taken prompt remedial action.

12. On account of the above, the Deputy Commissioner for Personal Data Protection directs the Organisation to pay a financial penalty of $5,000 within 30 days from the date of this direction (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).

13. In view of the remedial actions taken by the Organisation, the Commission will not be issuing any other directions.