**PERSONAL DATA PROTECTION COMMISSION**

Case No. DP-2001-B5620

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

And

The Future of Cooking Pte. Ltd.

## SUMMARY OF THE DECISION

1. The Future of Cooking Pte. Ltd. (the "**TFC**") operates an e-commerce website at https://www.thermomix.com.sg (the "**Website**"), retailing kitchen appliances and accessories.

2. On 3 January 2020, the Personal Data Protection Commission (the "**Commission**") received a complaint that a text file (the "**File**") containing personal data was accessible via the URL: https://thermomix.com.sg/wp-content/uploads/2019/10/woocommerce-order-export-1.csv-1.txt. (the "**Incident**").

3. The File contained the personal data of 178 unique individuals who had purchased items from the Website. The File was accessible via the URL from 1 October 2019 until 6 January 2020. It contained the following types of personal data (the "**Personal Data**"):

    a. Name;

    b. Email Address;

c. Billing Address;

d. Shipping Address;

e. Customer Notes (e.g. delivery instructions);

f. Order information (such as payment status, mode of payment, and transaction ID);

g. Product ID of items;

h. Quantity of items ordered; and

i. Telephone number.

**The Commission's Findings**

***No breach by Hachi as a Data Intermediary***

4. TFC had engaged Hachi Web Solutions Pte. Ltd. ("**Hachi**") to re-design the Website and also perform data backup and migration. Insofar as the data backup and migration activities are concerned, Hachi was TFC's data intermediary. The cause of the breach, however, did not relate to the data processing activities but to the Website re-design. Therefore, Hachi was not in breach of the Protection Obligation under section 24 of the Personal Data Protection Act 2012 (the "**PDPA**") by virtue of its role as a data intermediary.

***TFC in breach of the Protection Obligation***

5. The cause of the data breach may be traced to a WordPress plugin (the "**Plugin**") which was installed on the Website. The Plugin contained a bug which caused the File to be generated and uploaded on the Website's directory folder. Although this was a temporary file, it was accessible to the public via the URL.

6. TFC had used the Website to collect the personal data of individuals. At the time of the Incident, TFC's database contained personal data of approximately 3,500 individuals. To discharge its Protection Obligation under section 24 of the PDPA, TFC needed to have put in place reasonable security arrangements to protect the personal data collected.

7. In this case, investigations revealed that TFC had failed to discharge its obligations as data controller when engaging Hachi to undertake data processing activities. First, TFC did not specify any requirements for Hachi to implement any data protection measures to be implemented in the Website, whether in its contract with Hachi or other project documentation. Second, TFC did not conduct any pre-launch security testing (such as vulnerability assessments) on the Website. Had security testing been conducted, TFC would have been able to detect the presence of the publicly accessible temporary file, even if it was unaware of the bug in the Plugin that caused it.

8. Once it knew about the Incident, TFC and Hachi removed the Plugin and disabled the public's access to the relevant directory folder. Hachi also contacted the developers of the Plugin, who acknowledged the existence of the bug and fixed the bug in an updated version. TFC subsequently engaged a vendor to perform penetration testing and other measures to enhance the security of the Website.

9. The Deputy Commissioner found TFC in breach of the Protection Obligation under section 24 of the PDPA. After considering the circumstances of the Incident, including according mitigatory weight to TFC's cooperation with the Commission during investigations and the

remedial action taken by TFC after the Incident, the Deputy Commissioner directs TFC to pay a financial penalty of $9,000 for its breach.

10. TFC must make payment of the financial penalty 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 the financial penalty until it is paid in full.

11. No further directions are required as TFC had taken actions to address the gaps in its security arrangements.