PERSONAL DATA PROTECTION COMMISSION

Case No. DP-1905-B3827

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

And

Honestbee Pte Ltd

SUMMARY OF THE DECISION

1. Honestbee Pte Ltd (the "Organisation") is an online food and grocery delivery service. Third party merchants, which either engaged or were planning to engage the Organisation for delivery services, provided it with personal data of their customers in order to test its logistics service delivery platform. The Organisation stored this personal data in its Amazon Web Services ("AWS") file repository. The personal data (the "Personal Data") included names, email addresses, residential addresses and mobile numbers.

2. The Personal Data Protection Commission (the "Commission") was informed on 2 May 2019 that the Personal Data was accessible to the public. The number of individuals whose personal data was accessible was about 8,000. The Organisation admitted that it had mistakenly placed the Personal Data in a 'bucket' (which is similar to a file folder) without access restrictions. This allowed anyone with knowledge of AWS's command line to gain access to the Personal Data.

3. The Commission found that the Organisation omitted to put in place the most rudimentary security measures necessary to protect the Personal Data. For example, the

Organisation could have implemented a requirement to conduct checks to confirm that any personal data used in testing was stored in a 'bucket' with the appropriate access restrictions. In the circumstances, the Organisation had not implemented reasonable security arrangements to protect the Personal Data and is therefore in breach of section 24 of the Personal Data Protection Act 2012.

4. The Organisation has since blocked public access to the Personal Data by modifying the relevant access settings and circulated a report to its engineering team to ensure that similar mistakes would not be repeated in code reviews. The Organisation is also in discussions with cybersecurity companies to perform regular security audits on its systems.

5. The Organisation is directed to pay a financial penalty of $8,000 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 the financial penalty until the financial penalty is paid in full. In view of the remedial measures taken by the Organisation, the Commission has not imposed any other directions.

6. The Organisation's prompt co-operation in the course of the Commission's investigation, its prompt actions taken to remediate the breach and the limited unauthorized disclosure of the Personal Data were mitigating factors taken into consideration in determining the quantum of the financial penalty.