PERSONAL DATA PROTECTION COMMISSION

Case No. DP-2004-B6189

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

And

Hello Travel Pte. Ltd.

SUMMARY OF THE DECISION

1. On 8 April 2020, the Personal Data Protection Commission (the "**Commission**") received information that a database belonging to Hello Travel Pte Ltd (the "**Organisation**") was posted on an internet forum and was thus made publicly available (the "**Incident**").

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

3. The compromised database contained the personal data of approximately 71,002 users who had created accounts at the Organisation's website (www.havehalalwilltravel.com) from February 2015 to July 2018. The disclosed personal data included their name, email

address, date of birth, nationality and phone number. The table below summarises the number of affected individuals for each corresponding type of personal data disclosed:

S/N	**Type of Personal Data**	**Number of Individuals Affected**
1	Name	71,002
2	Email Address	57,693
3	Phone Number	453
4	Date of Birth	946
5	Nationality	20,754

4. The Organisation's internal investigations pointed to a possible hack as the cause of the Incident. Sometime in year 2018, the server instance which hosted the Organisation's website and the database became corrupted and unusable after the installation of a free open source wordpress plugin. The Organisation believed that unknown parties could have exploited vulnerabilities of the installed plugin at that time and exfiltrated the database.

5. The Organisation admitted that it did not give due attention to personal data protection and had neglected to put in place basic procedural and technical security arrangements to protect the personal data in its possession and control. As examples, it did not have the relevant policies and/or protocols in place to perform regular system patching or to conduct security assessment and/or testing when making changes to its ICT systems.

6. In the circumstances, the Deputy Commissioner for Personal Data Protection finds the Organisation in breach of the Protection Obligation under section 24 of the Personal Data Protection Act 2012 (the "**PDPA**").

7. Following the incident, the Organisation implemented technical measures to secure its systems from potential vulnerabilities. The personal data of its members were also encrypted immediately. Additionally, the Organisation had engaged relevant parties to take down the compromised database and informed the affected individuals of the Incident.

8. In determining the directions, if any, to be imposed on the Organisation. The Deputy Commissioner took into account the following factors:

Aggravating factors

(a) The high number of individuals affected;

(b) The fact that personal data was exfiltrated and posted online; and

(c) The Organisation did not put in place basic procedural and technical security arrangements.

Mitigating factors

(a) The Organisation had cooperated with the investigation;

(b) The Organisation's upfront voluntary admission of liability to a breach of the Protection Obligation under the PDPA;

(c) The Organisation's prompt remedial actions at [7] to address the inadequacies in its procedures and processes; and

(d) There was no evidence that the personal data affected in the Incident had been misused in any form.

9. In the course of settling this decision, the Organisation made representation on the amount of financial penalty which the Commission intends to impose and requested that the financial penalty to be paid in instalments. The Organisation raised the following factors for the Commission's consideration:

(a) The Organisation had been suffering substantial loss due to the impact to the travel industry by the Covid-19 pandemic; and

(b) The Organisation had already spent quite a substantial amount of money to fix the security breach.

10. Having carefully considered the representations, the Deputy Commissioner has decided to reduce the financial penalty to the amount set out in [11a] and is agreeable for the financial penalty to be payable in instalments. The quantum of financial penalty has been calibrated after due consideration of the Organisation's financial circumstances due to the unprecedented challenges faced by businesses amid the current Covid-19 pandemic, bearing in mind that financial penalties imposed should not be crushing or cause undue hardship on organisations. Although a lower financial penalty has been imposed in this

case, the quantum of financial penalty should be treated as exceptional and should not be taken as setting any precedent for future cases.

11. Taking into account all relevant facts and circumstances, the Deputy Commissioner hereby directs the Organisation to:

(a) Pay a financial penalty of $8,000 in 10 instalments by the due dates as set out below, failing which, the full outstanding amount shall become due and payable immediately and 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:

i. 1st instalment of $800 on 1 January 2021;
ii. 2nd instalment of $800 on 1 February 2021;
iii. 3rd instalment of $800 on 1 March 2021;
iv. 4th instalment of $800 on 1 April 2021;
v. 5th instalment of $800 on 1 May 2021;
vi. 6th instalment of $800 on 1 June 2021;
vii. 7th instalment of $800 on 1 July 2021;
viii. 8th instalment of $800 on 1 August 2021;
ix. 9th instalment of $800 on 1 September 2021; and
x. 10th instalment of $800 on 1 October 2021

12. In view of the remedial actions taken by the Organisation, the Deputy Commissioner will not be issuing any other directions.