PERSONAL DATA PROTECTION COMMISSION

Case No. DP-2007-B6563

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

And

BLS International Services Singapore Pte. Ltd.

SUMMARY OF THE DECISION

1. BLS International Services Singapore Pte. Ltd. (the "**Organisation**") provides government-to-citizen services for the High Commission of India in Singapore, such as visa and consular services.

2. On 7 July 2020, the Personal Data Protection Commission (the "**Commission**") received information that the URLs of the printable version of appointment booking confirmation webpages could be manipulated to access other individuals' personal data (the "**Incident**"). The personal data comprised the individual's name, passport number, contact number, email address, type of service request, booking date/time, appointment date/time, and number of booking applications.

3. 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**").

4. Investigations revealed that on 8 June 2020, which was about a month prior to the Incident, the Organisation had implemented a new booking system for the High Commission of India. Under this new booking system, users who submitted a booking for an appointment at the High Commission of India would be provided with an URL, which led to a printable version of the booking confirmation. In designing the booking system, the Organisation had intended for the URLs to be encrypted. This would have made it more difficult for people to manipulate the URL. However, the encryption was not done properly due to a coding error. Although the Organisation had conducted some testing on the new booking system, the testing was not extensive enough to detect the error.

5. Upon realising the occurrence of the Incident from the Commission on 16 July 2020, the Organisation took immediate action to investigate and subsequently identified the coding error. On the same day, the Organisation made changes to the booking system. It stopped providing users with an URL to a printable version of their booking confirmation. Instead, the booking confirmation would be sent to the user's email account.

6. The Organisation's records showed that a total of 3,357 individuals used the new booking system from 8 June 2020 to 16 July 2020. This meant that the personal data of 3,357 individuals was at risk of exposure by URL manipulation.

7. The Deputy Commissioner for Personal Data Protection found that the Organisation was in breach of the Protection Obligation under section 24 of the Personal Data Protection Act 2012 for failing to conduct adequate testing of the booking system before it went "live". Depending on how the URL encryption was implemented, URL encryption could had been a reasonable security measure for the personal data type the Organisation was collecting. However, because the Organisation had not conducted adequate testing of the booking system before it went "live", the Organisation did not detect the coding error, thereby resulting in the Incident.

8. After considering the circumstances of the case, including: (i) the Organisation's upfront voluntary admission of liability which significantly reduced the time and resources required for investigations; and (ii) the Organisation's prompt remedial actions, the Deputy Commissioner for Personal Data Protection directs that the Organisation pays a financial penalty of $5,000 for the breach.

9. The Organisation 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.

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