PERSONAL DATA PROTECTION COMMISSION

Case No. DP-2103-B7984

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

And

ChampionTutor Inc. (Private Limited)

SUMMARY OF THE DECISION

1. On 24 February 2021, the Personal Data Protection Commission (the "**Commission**") received information that ChampionTutor Inc. (Private Limited)'s (the "**Organisation**") database, containing personal data of individuals, was being sold on dark web (the "**Incident**").

2. The Organisation was not aware of the Incident until it was notified by the Commission. The cause of the Incident was suspected to be SQL injection of the Organisation's website. The Organisation knew about this SQL injection vulnerability when it conducted a penetration test in December 2020. The Organisation had instructed its developer, based in India, to fix the vulnerability. However, the developer did not act on the request and this vulnerability was left unfixed until the Incident happened.

3. As a result, the personal data of 4,625 students were affected. The personal data included name, email address, contact number and address.

4. The Organisation took the following remedial measures after the Incident:

   a. Engaged a new team of developers to fix all the SQL injection vulnerabilities;

   b. Parameterised SQL statements by disallowing data-directed context changes to prevent SQL injection attacks from resurfacing; and

   c. Is in the process of revamping the entire website source codes to reduce possible vulnerabilities.

5. The Organisation admitted to having breached the Protection Obligation under section 24 of the Personal Data Protection Act (the "**PDPA**"), and requested for the matter to be dealt with in accordance with the Commission's Expedited Decision Procedure.

6. The Organisation admitted it was aware of the SQL injection vulnerability in December 2020. Yet, the Organisation failed to take active steps to fix the vulnerability even when its developer was not responsive, purportedly due to the COVID-19 pandemic, and the Organisation left the vulnerability unresolved until the Incident happened.

7. In the circumstances, the Organisation is found to have breached section 24 of the PDPA.

8. On 14 July 2021, the Organisation was notified of the Commission's intention to impose a financial penalty based on the Commission's consideration of the factors listed under section 48J(6) of the PDPA, and the circumstances of this case, in particular (i) the Organisation's upfront voluntary admission of liability which significantly reduced the time and resources required for investigations; and (ii) the prompt remedial actions undertaken by the Organisation. The Organisation was invited to make representations.

9. Having considered the Organisation's representations dated 28 July 2021, the Deputy Commissioner hereby directs the Organisation to pay a financial penalty of $10,000 in 12 instalments by the due dates as set out in the accompanying notice, 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.

10. In view of the remedial actions taken by the Organisation, the Commission will not issue any directions under section 48I of the PDPA.