PERSONAL DATA PROTECTION COMMISSION

Case No. DP-2101-B7725

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

And

GeniusU Pte. Ltd.

SUMMARY OF THE DECISION

1. On 12 January 2021, GeniusU Pte. Ltd. (the "**Organisation**") notified the Personal Data Protection Commission (the "**Commission**") of unauthorized access and exfiltration of a staging application database (the "**Database**") holding personal data (the "**Incident**").

2. The personal data of approximately 1.26 million users were affected. The datasets affected comprised first and last name, email address, location and last sign-in IP address.

3. The Organisation's internal investigations revealed that the likely cause of the Incident was compromise of one of its developer's password, either because the developer used a weak password for his GitHub account or the password for his GitHub account had been compromised. This allowed the threat actor to enter

the Organisation's GitHub environment. As the Organisation had stored the login credentials to the Database in the codebase in its GitHub environment, the threat actor was able to gain access to and exfiltrate personal data stored in the Database.

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

   a. Rotated the credentials of the Database;

   b. Removed all hard-coded credentials from the codebase;

   c. Purged all existing website sessions;

   d. Removed all personal data from non-production environment servers,

   e. Implemented multi-factor authentication on all work-related accounts;

   f. Implemented a standardised cyber security policy and related procedures for all staff; and

   g. Notified users and the GDPR data authority (Ireland) of the Incident.

5. The Commission accepted the Organisation's request for this matter to be handled under the Commission's expedited breach decision procedure. This meant that the Organisation had voluntarily provided and unequivocally admitted

to the facts set out in this decision. The Organisation also admitted that it was in breach of section 24 of the Personal Data Protection Act (the "**PDPA**").

6. Based on its admissions, the Organisation had breached the Protection Obligation by:

   a. Storing credentials for the Database in the codebase in its GitHub environment. This meant that once the threat actor was able to access the GitHub environment, he was able to discover the credentials to access personal data stored in the Database; and

   b. Storing actual personal data in the Database that was in a non-production (testing) environment, which are usually not as secure as production environments. Actual personal data should not be stored in testing environments, which are known to be less secure.

7. In the circumstances, the Organisation is found to be in breach of section 24 of the PDPA.

8. Having considered the circumstances set out above and the factors listed at section 48J(6) of the PDPA and 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 prompt remedial actions undertaken by the Organisation, the Organisation is given a notice to pay a financial penalty of $35,000.

9. The Organisation must make payment of the financial penalty within 30 days from the notice accompanying date this decision, 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 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.

The following is the provision of the Personal Data Protection Act 2012 cited in the above summary:

Protection of personal data

24. An organisation shall protect personal data in its possession or under its control by making reasonable security arrangements to prevent –

(a) unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks; and
(b) the loss of any storage medium or device on which personal data is stored.