PERSONAL DATA PROTECTION COMMISSION

Case No. DP-2101-B7826

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

And

Specialized Asia Pacific Pte Ltd

SUMMARY OF THE DECISION

1. On 29 January 2021, Specialized Asia Pacific Pte Ltd. (the "**Organisation**") informed the Personal Data Protection Commission of a data security incident involving the Specialized Cadence application (the "**Application**") that it developed, operated and maintained.

2. The Organisation's developing staff did not realize that the online development tool, which was used to develop the Application, had a default privacy setting that made all data created by users or developers "visible", even though this had been stated in the tool's privacy rules. This default setting allowed the Application's network traffic to be intercepted and accessed using third-party security testing software that can be acquired online. A member of the public had therefore been able to intercept and access the personal data of the Application's users by using a free version of such software (the "**Incident**"). However, the risk of unauthorised access had been limited to parties who knew how to use such security testing software to obtain access. This factored in the enforcement outcome below (see paragraph 6 below).

3. The undetected default privacy setting of "visible" put the personal data of 2,445 individuals at risk of unauthorised access. The data affected included names, addresses, dates of birth, telephone numbers, email addresses and gender.

4. Remediation by the Organisation encompassed turning off all access and use of the Application by all external parties, including users, and changing the privacy setting from "visible" to "hidden". The Organisation also engaged a third-party IT security firm to

test and address any security and privacy issues relating to the Application, commenced discussions with its IT application designers and employees involved to adopt 'privacy-by-design' in future applications development.

5. The Protection Obligation in section 24 of the Personal Data Protection Act 2012 requires that organisations understand the privacy policies and security features of all online tools or software they choose to employ. This was established in published cases such as *Re GMM Technoworld Pte. Ltd.* [2016] SGDPDPC 18. Organisations employing online tools or other online software must set or reconfigure privacy policies and security features to protect the personal data of application or website users. It would not be a discharge of the Protection Obligation for an organisation to simply adopt, vis-à-vis users, the same default privacy policies of online tools or software that do not protect the personal data of users.

6. The Deputy Commissioner for Personal Data Protection therefore found the Organisation in breach of the Protection Obligation under Section 24 of the Personal Data Protection Act 2012. Upon consideration of the facts, including the limited exposure of the affected data to those who knew how to use the above-mentioned third party software to access such information via the default privacy setting, and the Organisation's commitment to improve its processes, a Warning was issued to the Organisation.

The following are the provisions 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 unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks.