PERSONAL DATA PROTECTION COMMISSION

Case No. DP-2010-B7196

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

And

St. Joseph's Institution International Ltd.

SUMMARY OF THE DECISION

1. On 16 October 2020, St Joseph's Institution International Ltd. (the "**Organisation**") informed the Personal Data Protection Commission that a file listing the personal data of 3155 parents and students ("**the File**") was found on a website called VirusTotal (the "**Incident**").

2. The Incident occurred on or around 13 October 2020 when a staff of the Organisation downloaded and deployed a Google Chrome browser extension developed by VirusTotal for additional security scanning. Unknown to the staff, apart from security scanning, the extension also forwarded scanned samples to premium members of VirusTotal (the "**3rd Parties**") for security analysis and research. This use of samples was made known in VirusTotal's privacy policy covering the use of the extension.

3. As a result of the Incident, the personal data of 3155 individuals including both parents and students were put at risk of unauthorised access. The personal data affected included the names of parents and students, parents' email addresses, students' date of birth, students' classes, students' year and grades.

4. Users of the VirusTotal Chrome extension would have to agree to VirusTotal's Privacy Policy, which provides that once files are uploaded to the VirusTotal website for scanning, copies of these files will be kept by VirusTotal and shared with their subscribers for research purposes. The risk of such file sharing and in turn disclosure of personal data to 3rd Parties ought to have been known to the said staff of the Organisation, but was overlooked due to oversight. Such oversight could have been prevented if the Organisation had sufficiently robust processes for assessing such risks prior to deploying downloaded software, including Chrome Extensions. However, the Organisation lacked such processes.

5. Nevertheless, the Organisation took prompt action to mitigate the effects of the breach by contacting VirusTotal immediately to remove the File and notified all affected individuals. While personal data was disclosed, it was limited to premium members of VirusTotal for research purposes only.

6. On the facts, the Deputy Commissioner for Personal Data Protection found the Organisation in breach of the Protection Obligation under section 24 of the Personal Data Protection Act 2012. However, in consideration of the limited risk of personal data being disclosed, and the Organisation's commitment to improve its processes, a Warning was issued to the Organisation.

7. The Commission reminds all organisations that they must have sufficiently robust processes to obtain a functional understanding of software to be deployed, in order to assess the security risks to personal data in their possession or control. Failure to do so would be breach of the Protection Obligation.