PERSONAL DATA PROTECTION COMMISSION

Case No. DP-1907-B4288

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

And

NTUC Income Insurance Co-Operative Limited

SUMMARY OF THE DECISION

1. The Personal Data Protection Commission (the "Commission") was notified on 17 July 2019 by NTUC Income Insurance Co-Operative Limited's (the "Organisation") of the unintended disclosure of personal data to users making enquiries through its website. The users received automated acknowledgement emails attached with files containing personal data of other individuals (the "Incident").

2. On 10 July 2019, the Organisation enhanced the website's online enquiry application to allow users to upload supporting documents together with their enquiry submissions. When a user A uploaded files, the application assigned a variable that served to identify the files for future retrieval by the same user or by the Organisation. However, due to a coding error, if the next user B did not upload files, the variable generated for the preceding user was applied to the B's submission. As a result, the supporting documents uploaded by A were associated with B's submission.

3. This coding error manifested in the sending of acknowledgement emails, which were intended to include supporting documents submitted by the user. When acknowledgement emails were generated for a user who did not upload files, the coding error caused the files uploaded by a preceding user to be attached. There were 17 users whose uploaded files were sent to 123 other users in this way. The files contained their personal data, such as names, policy numbers, premium amounts, sum assured and period of coverage, email and mailing addresses.

4. The Organisation admitted that the Incident was caused by poor quality codes. The Commission found that such errors should have been detected during the manual code review process that the Organisation had conducted. Further, before the enhancement went "live", the Organisation's tests did not simulate the various scenarios expected whereby some users would upload files while others did not.

5. The Organisation has since sought to improve checks on coding quality by replacing its manual code review process with tools such as Crucible and SonarQube. It also moved to ensure that test scenarios were adequate and that test plans and reviews were in place before changes in its IT applications and systems were allowed to be deployed.

6. In the circumstances, 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 and decided to give a warning to the Organisation. No directions are

required as the Organisation has implemented corrective measures that addressed the gap in its security arrangements.