

PERSONAL DATA PROTECTION COMMISSION

Case No. DP-2010-B7132

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

And

Chapel of Christ the Redeemer

SUMMARY OF THE DECISION

1. On 6 October 2020, Chapel of Christ the Redeemer (the “**Organisation**”) informed the Personal Data Protection Commission (the “**Commission**”) that a file (the “**File**”) containing personal data of 815 members’ name, NRIC, address, date of birth, marital status, email address, mobile and residential phone number was inadvertently disclosed online.
2. Investigations revealed that a staff had accidentally uploaded the File (which was supposed to be an internal document) onto the sub-directory on 24 November 2019. The Organisation only discovered the matter on 8 September 2020 when a member of the Organisation performed a Google search of another member’s name and found a Google search result of the File.

3. The Organisation admitted that there were no access controls to the sub-directory prior to the incident as the sub-directory was intended to be accessible to public. As a result, the File was indexed by search engines and showed up in online search results. The Organisation also admitted that at the time of the incident, the Organisation had not developed any internal policies and practices to ensure compliance with the Personal Data Protection Act 2012 (the “**PDPA**”). In particular, there was no system of checks for the uploading of files on the Organisation’s website.
4. Fortuitously, it appeared that the access to the File was minimal – based on Google Analytics Report, save for the Organisation’s member who discovered the File on the internet on 8 September 2020, there was only one other access to the File on 9 December 2019, and the access only lasted for approximately 1 minute.
5. Following the incident, the Organisation disabled the search engine indexing to the sub-directory, password-protected all files with members’ data, and implemented a weekly check of all files uploaded onto the website to detect any accidental uploading of incorrect files; and a policy to delete files that are on the website for more than three months. The Organisation has also informed the Commission that it intends to engage a consultant to conduct PDPA training for its staff, as well as to review the data protection processes within the Organisation to ensure compliance with the PDPA.
6. In view of the facts stated at [3] above, the Deputy Commissioner for Personal Data Protection found the Organisation in breach of section 12 of the PDPA (the obligation to

develop and implement data protection policies and practices), and section 24 of the PDPA (the obligation to protect personal data in an organisation's possession or under its control by making reasonable security arrangements).

7. In determining the directions to be imposed on the Organisation under section 29 of the PDPA, the following factors were taken into account:

(a) The Organisations had voluntarily notified the Commission of the incident, fully cooperated with the Commission's investigations and implemented prompt remedial measures to address the breach; and

(b) There was minimal access to the File and no evidence that the personal data had been misused.

8. In the circumstances, the Deputy Commissioner would not be imposing any financial penalty on the Organisation. However, in light of the Organisation's lack of the necessary data protection policies and practices, the Deputy Commissioner hereby directs the Organisation to:

(a) Develop and implement internal data protection policies and practices to comply with the provisions of the Act within 90 days from the date of the direction, and

(b) Inform the Commission within 1 week of implementation of the above.