PERSONAL DATA PROTECTION COMMISSION

Case No. DP-2004-B6193

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

And

Vimalakirti Buddhist Centre

SUMMARY OF THE DECISION

1. On 14 April 2020, Vimalakirti Buddhist Centre (the "**Organisation**") notified the Personal Data Protection Commission (the "**Commission**") of a ransomware infection that had rendered its data management system inaccessible by the Organisation (the "**Incident**").

2. The Organisation subsequently requested for this matter to be handled under the Commission's expedited breach decision procedure. In this regard, the Organisation voluntarily provided and unequivocally admitted to the facts set out in this decision. It also admitted that it was in breach of section 24 of the Personal Dara Protection Act (the "**PDPA**").

3. The Incident occurred on or about 31 March 2020. Personal data of approximately 4,500 members and 4,000 non-members (total 8,500 individuals) were encrypted by the ransomware. The personal data encrypted included the name, address, contact number, NRIC number, date of birth and donation details of the individuals.

4. The Organisation admitted it did not give due attention to personal data protection, and had neglected to implement both procedural and technical security arrangements to protect the personal data in its possession and control. Consequently, it did not have the relevant security software and/or protocols in place to prevent the ransomware from entering its data management system.

5. In the circumstances, the Deputy Commissioner for Personal Data Protection finds the Organisation in breach of the Protection Obligation under section 24 of the Personal Data Protection Act 2012 (the "**PDPA**").

6. Following the incident, the Organisation set up a new server with backup from 21 October 2019. For the data collected by the Organisation from 22 October 2019 to the Incident, the Organisation had retrieved the data from physical file records and restored them in the new server. It also installed a firewall to filter network traffic to and from the new server, and cleaned, restored and reinstalled all computers

connected to its data management system. Additionally, the Organisation committed to engage consultants to help produce a data protection manual and train its staff in cyber hygiene and incident response.

7. The Deputy Commissioner for Personal Data Protection notes that the Organisation had admitted to a breach of Protection Obligation under the PDPA, cooperated with the Commission's investigation and taken prompt remedial action. There was no evidence that the personal data affected in the Incident had been misused in any form. In addition, the Organisation had a backup copy of the encrypted data and did not lose any data as a result of the Incident. Accordingly, the practice of having data backup(s) should be encouraged to prevent organisations from losing data in the event of ransomware.

8. On account of the above, the Deputy Commissioner for Personal Data Protection directs the Organisation to pay a financial penalty of $5,000 within 30 days from the date of this direction (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).

9. In view of the remedial actions taken by the Organisation, the Commission will not be issuing any other directions.