Information Technology Management Association (Singapore)

[2018] SGPDPC 11

Yeong Zee Kin, Deputy Commissioner — Case No DP-1708-B1019

Data Protection – Protection obligation – Disclosure of personal data – Insufficient security arrangements

Data Protection – Openness obligation – Requirement to develop and implement policies and practices

14 May 2018.

Background

1 On 10 August 2017, the Organisation informed the Commission of its inadvertent disclosure of personal data. The facts disclose a straightforward breach of section 24 of the Personal Data Protection Act 2012 ("**PDPA**").

2 The Organisation engaged a travel service provider to organise a study trip for 49 delegates. On 8 August 2017, the Organisation received an email with two attachments from the travel service provider. One attachment was a list containing full names, gender, nationality, dates of birth and passport numbers of 28 delegates (the "**List**").

3 The Organisation forwarded the email to the 49 delegates on 10 August 2017. The List was inadvertently included in the email. This resulted in the inadvertent disclosure of the personal data in the List.

4 One delegate provided feedback to the Organisation on the List. Upon notification of the error, the Organisation promptly emailed an apology to the 28 delegates. It subsequently contacted all 49 recipients and requested that they delete the copy of the List that they had received.

5 The issues to be determined in this case are:

(a) Whether the Organisation breached section 24 of the PDPA to protect the personal data in the List; and

(b) Whether the Organisation breached section 12(a) of the PDPA to develop and implement policies and practices to comply with the Act.

Did the Organisation breach section 24?

6 An organisation must protect personal data in its possession or under its control under section 24 of the PDPA ("**Protection Obligation**"). In this regard, it must take reasonable steps to prevent unauthorised access, copying, modification, or disposal personal data.

7 The Organisation's core business was running a membership programme. Its functions involved frequent sending of emails including personal data. The Commissioner's Guide to Preventing Accidental Disclosure when Processing and Sending Personal Data (published on 20 January 2017) states that employees should ensure that attachments are checked and verified that they are for the intended recipients. In this case, the Organisation had failed to do so when sending the email containing the List to all 49 recipients. The

result was the personal data in the List being disclosed to delegates who were not intended to receive such data of other delegates. The Organisation was therefore found in breach of section 24 of the PDPA.

Did the Organisation breach section 12(a)?

8 Section 12(a) required the Organisation to develop and implement policies and practices to comply with the PDPA.

9 The Organisation had a Personal Data Protection Statement ("**PDP Statement**"). It outlined how collected personal data might be used. It also stated that access to personal data was limited to employees who needed to process it. Likewise, personal data would be shared on a need-to-know basis. For external communications, personal data would be shared only when there was a "legitimate reason". An employee was assigned to process all personal data handled by the Organisation. The employee had previously attended formal training on the requirements of the PDPA and had been briefed on the Organisation's protection of personal data.

10 It was assessed that the Organisation's PDP Statement complied with the requirement under section 12(a) to develop policies to meet its obligations under the PDPA. Its attempts to limit access to personal data to the employee who had been given PDPA compliance training was assessed to comply with the requirement to implement the policies in its PDP Statement. Finally, the Organisation's efforts to implement its personal data protection polices under section 12(a) were taken as forms of practices on the ground to help employees to manage the risk of unauthorised disclosure of or access to personal data through emails and other external communications.

11 Accordingly, the Organisation was not found in breach of section 12(a) of the PDPA.

Remedial measures taken

12 Following the incident, the Organisation required employees to review all emails and attachments before sending or forwarding. They are also required to check whether personal data is being sent to unintended and/or unauthorised recipients

13 In assessing this case, I took into account the following:

(a) The Organisation's prompt action to inform all 49 delegates to delete the List;

(b) The Organisation's voluntary notification of the incident and cooperation in the investigation; and

(c) The Organisation's remedial measures assessed to be reasonable to address risk of similar incidents.

14 In view of the factors noted above, I decided to issue a warning to the Organisation for the breach of its obligation under section 24 of the PDPA as neither further directions nor a financial penalty is warranted in this case.

YEONG ZEE KIN
DEPUTY COMMISSIONER
PERSONAL DATA PROTECTION COMMISSION