DECISION OF THE PERSONAL DATA PROTECTION COMMISSION

Case Number: DP-1504-A390

SINGAPORE COMPUTER SOCIETY (Reg. No. S67SS0039C)
... Respondent

Decision Citation: [2016] SGPDPC 9

GROUNDS OF DECISION

20 April 2016

A. BACKGROUND

1. On 17 March 2015, the Respondent notified the Commission that it inadvertently disclosed certain personal data of individuals attending an event organised by the Respondent to other individuals and had received information about the disclosure from some of the individuals concerned. After being notified of the incident by the Respondent, the Commission undertook an investigation to determine whether there had been a breach of the Personal Data Protection Act 2012 (the "**PDPA**"). The material facts of the case are as follows.

B. MATERIAL FACTS AND DOCUMENTS

2. In April 2015, the Respondent jointly organised and conducted an event with the Infocomm Development of Singapore ("**IDA**") named "IDEAS on Security Analytics". Prior to the event, on 16 March 2015, an employee of the Respondent, [Redacted] (Replaced with Ms L), sent out an email to all individuals who had registered to attend the event ("**registrants**"), which had attached a copy of the registration list for the event. The registration list contained personal data of about 214 registrants (individuals). 11 of the registrants subsequently raised concerns about the unauthorised disclosure of their personal data to the Respondent. The personal data which had been disclosed included information such as the registrants' full names, NRIC numbers, contact numbers, email addresses, organisation and designation information. The Respondent confirmed that it was not acting on behalf of IDA in relation to the collection, use, disclosure or processing of the registrants' personal data.

3. The Respondent acknowledged to the Commission that the registration list was not meant to be disclosed externally and had been inadvertently sent to registrants on 16 March 2015. The Respondent explained that Ms L's supervisor (who was also an employee of the Respondent) had sent her the registration list in an email which included a draft event confirmation email which Ms L was required to send to registrants. Ms L used the "Forward" function in her email application to send the event confirmation email on 16 March 2015 but forgot to remove the attached registration list (which was automatically attached to her email to registrants by her use of the "Forward" function).

4. Upon being notified of the disclosure by some registrants, the Respondent took the immediate step of initiating an email recall at 3 p.m. on 16 March 2015, approximately 40 minutes after the email with the registration list was sent.

5. The Respondent's Data Protection Officer subsequently sent an official email apology to the 11 registrants who had raised concerns to the Respondent over the incident. All 11 registrants accepted the apology and did not pursue the matter further. Neither the Respondent nor the Commission received other complaints relating to this incident.

C. COMMISSION FINDINGS AND BASIS FOR DETERMINATION

Relevant issue(s) in this case

6. This case principally concerns an unauthorised disclosure of personal data by an employee of the Respondent. Under section 24 of the PDPA, an organisation is required to protect personal data in its possession or control by making reasonable security arrangements to prevent unauthorised disclosure, disposal, access, collection, use, or similar risks (amongst others).

7. A secondary issue in this case is that the Respondent did not have the consent of the registrants to disclose their personal data to other registrants (as required under section 13 of the PDPA). However, as the Respondent never intended to make such a disclosure, and hence would not have sought consent from the registrants, the Commission notes that this case is more properly considered from the perspective of the Respondent's obligations under section 24 of the PDPA. Nevertheless, the Commission is not precluding that other cases may require an examination of both sections 13 and 24.

Commission's findings on the relevant issue(s)

8. It is not disputed by the Respondent that its employee, Ms L, had made an unauthorised disclosure of registrants' personal data to other registrants via her email of 16 March 2015. The Commission notes that this unauthorised disclosure arose from a number of factors which reflect poor data handling practices by the Respondent, including the following:

   (a) Ms L's supervisor had sent her the registration list containing registrants' personal data in the same email which contained a draft event confirmation email which Ms L was required to send to registrants. This gave rise to a risk that Ms L may either not realise the registration list was attached or may forget to delete the registration list when she used the "Forward" function in the email application to send the event confirmation email; and

   (b) The registration list sent to Ms L was not protected by a password (or in any other manner which would prevent unintended recipients from opening it and accessing the data contained therein).

9. Under section 53(1) of the PDPA, any act done, or conduct engaged in, by an employee shall be treated for the purposes of the PDPA as acts done, or conduct engaged in, by his employer as well as him. The Respondent is therefore liable for the acts and conduct of its employees in relation to the unauthorised disclosure of registrants' personal data on 16 March 2015.

10. In relation to the personal data which had been disclosed by the Respondent on 16 March 2015, the Commission notes that a significant amount may be business contract information, which is defined in section 2 of the PDPA as "an individual's name, position name or title, business telephone number, business address, business electronic mail address or business fax number and any other similar information about the individual, not provided by the individual solely for his personal purposes". For personal data which is business contract information, section 4(5) of the PDPA provides that Parts III to VI of the PDPA, which includes section 24, does not apply. Nevertheless, as at least some of the personal data disclosed, for example, the NRIC numbers of registrants, was not business contact information, the Respondent was required to protect such personal data in accordance with section 24.

11. Overall, the Commission considers that the Respondent's data handling practices in relation to the sending of the event confirmation email to registrants did not include sufficient security arrangements to the standard required under section 24 of the PDPA. The Commission therefore finds that the Respondent is in breach of section 24 of the PDPA.

A. ACTIONS TAKEN BY THE COMMISSION

12. The Commission is empowered under section 29 of the PDPA to give the Respondent such directions as it deems fit to ensure the Respondent's compliance with the PDPA. This may include directing the Respondent to pay a financial penalty of such amount not exceeding $1 million as the Commission thinks fit.

13. In considering whether a direction should be given to the Respondent in this case, the Commission notes the following:

    (a) A significant part of the personal data disclosed was business contact information;

    (b) The Respondent took prompt action to recall the emails of 16 March 2015 which had the attached registration list, even though this process did not result in a complete recall of all the emails; and

    (c) SCS informed the PDPC of the data breach voluntarily and was cooperative during the investigation.

14. In view of the factors noted above, the Commission has decided not to issue any direction to the Respondent under section 29 of the PDPA. Instead, the

Commission has decided to issue a Warning to the Respondent for the breach of its obligations under section 24 of the PDPA.

15. The Commission emphasises that it takes a very serious view of any instance of non-compliance with the PDPA, and it urges organisations to take the necessary action to ensure that they comply with their obligations under the PDPA. The Commission will not hesitate to take the appropriate enforcement action against the organisation(s) accordingly.

YEONG ZEE KIN
COMMISSION MEMBER
PERSONAL DATA PROTECTION COMMISSION