PERSONAL DATA PROTECTION COMMISSION

[2018] SGPDPC 28

Case No DP-1711-B1367

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

And

Institute of Singapore Chartered
Accountants

… *Organisation*

DECISION

Institute of Singapore Chartered Accountants

[2018] SGPDPC 28

Tan Kiat How, Commissioner — Case No DP-1711-B1367

13 December 2018.

Background

1 Technology has transformed the way we communicate. Today, we live in a world of tweets and texts, email and instant messaging. This case shows that when sending documents containing a significant volume of personal data by email, it is important for organisations to have in place reasonable security arrangements to protect these documents from unauthorised access by unintended recipients.

2 On 27 November 2017, the Personal Data Protection Commission (the "**Commission**") received notification from the Institute of Singapore Chartered Accountants ("**ISCA**") that one of its employees inadvertently sent an email attaching a Microsoft Excel document containing personal data of 1,906 individuals (the "**Excel File**") to an unintended recipient (the "**Incident**").

3 Following an investigation into the matter, the Commissioner found ISCA in breach of section 24 of Personal Data Protection Act 2012 ("**PDPA**").

Material Facts

4 Established in 1963, ISCA is the national professional body for accountants in Singapore with about 32,000 members. ISCA is the

Administrator of the Singapore Chartered Accountant Qualification and the designated body to confer the "Chartered Accountant of Singapore" designation.

5 On or about 23 November 2017, as part of business operations, 2 ISCA employees (the "**First Employee**" and the "**Second Employee**", collectively the "**Employees**") were unable to open the Excel File (stored on ISCA's internal shared drive) as it appeared to be corrupted. The Employees sought the assistance of ISCA's IT department. Arising from this, ISCA's IT Support Specialist sent an email to the System/Network Engineer from the ICT department to recover the Excel File from the backup server, and to send the recovered Excel File to the Employees.

6 On 24 November 2017, the System/Network Engineer created an email to send the recovered Excel File as an attachment to the Employees (the "**Subject Email**"). As the earlier email from the IT Support Specialist did not include the Employees in the addressee list, the System/Network Engineer had to specifically insert the Employees in the recipient section of the Subject Email. Due to the auto-complete feature in Microsoft Outlook's email software, the System/Network Engineer inadvertently selected an accounts manager (the "**Unintended Recipient**")[1] in a listed telecommunications service provider ("**Telco**") instead of the First Employee as they both had the same first name. The Subject Email containing the Excel File was therefore sent to the IT Support Specialist, the Second Employee and the Unintended Recipient. The Excel File was not encrypted with a password.

---

[1] The Unintended Recipient was the designated accounts manager to communicate with ISCA on services provided by the Telco to ISCA.

7 The Excel File listed 1,906 candidates in the ISCA Professional Examination programme. The personal data[2] of the candidates which were disclosed include the following:

(a) NRIC numbers;

(b) Passport numbers;

(c) Name;

(d) Date of Birth;

(e) Postal Address;

(f) Email Address;

(g) Mobile Phone Numbers;

(h) Employment history records;

(i) Qualification records;

(j) Exam results; and

(k) Appeal status of their candidature.

(collectively, the "**Subject Data**")

8 The Second Employee discovered the mistake within 10 minutes of the Subject Email being sent, and reported it to the Manager, Info-communications and Technology Management, who was also one of ISCA's data protection officers (the "**Manager ICT**").

9 ISCA took the following remedial action:

---

[2] Each of the 1,906 candidates did not have the same types of data disclosed in the Excel File. Some candidates had more data in the Excel File than others.

(a) On 24 November 2017 at around 3.24pm, the System/Network Engineer emailed the Unintended Recipient to inform her to disregard the Subject Email. At around 3.44pm, the Unintended Recipient replied the System Network Engineer to inform ISCA that she had deleted the Subject Email without opening the Excel File.

(b) On 25 November 2017, the Manager ICT sent a further email to the Unintended Recipient to require that all copies of the Subject Email and Excel File are permanently deleted. Through emails dated 27 and 28 November 2017, the Unintended Recipient confirmed that the Subject Email and Excel File have been permanently deleted.

(c) The Unintended Recipient signed a Declaration confirming that:

(i) The Subject Email and Excel file was promptly deleted upon the Unintended Recipient being notified by ISCA of the Subject Email being sent by mistake;

(ii) The Excel File was not opened by the Unintended Recipient nor anyone else; and

(iii) The Unintended Recipient's employer does not possess the Subject Email and Excel File and no copies remain in its mail servers, backups or systems.

(d) On 29 November 2017, ISCA notified all 1,906 candidates of the Incident by email and/or SMS.

The Commissioner's Findings and Basis for Determination

10 It is not disputed that the Subject Data is "personal data" as defined in section 2(1) of the PDPA. There is also no dispute that the PDPA applies to ISCA as it falls within PDPA's definition of "organisation".

11 The issue to be determined by the Commissioner in this case is whether ISCA had complied with its obligations under section 24 of the PDPA.

Whether ISCA complied with its obligations under section 24 of the PDPA

12 Section 24 of the PDPA provides that an organisation shall protect personal data in its possession or under its control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks.

13 It is not disputed that ISCA had possession and/or control of the Subject Data in the Excel file stored on ISCA's internal shared drive and backup server.

ISCA's security arrangements to protect electronic documents containing personal data

14 As part of ISCA's business operations, its employees are required to access a significant number of its members' personal data contained in electronic files (e.g. the Excel File contained 1,906 individuals' Subject Data). The Subject Data in ISCA's possession and/or control included personal data which has a higher expectation of confidentiality (e.g employment history records, qualification records, exam results and appeal status) and could be potentially embarrassing if disclosed to unauthorised recipients.

15 In this regard, ISCA has a general policy that applies to the whole organisation with respect to the protection of personal data of its members. This "Information Sensitivity Policy" is intended to guide employees on protecting information at varying sensitivity levels, including during electronic distribution. According to ISCA, the Subject Data in the Excel File would fall under the "More Sensitive" category. For electronic distribution of documents in this category, there are *"no restrictions to approved recipients within ISCA, but should be encrypted or sent via a private link to approved recipients outside of ISCA premises".*

16 ISCA also has targeted policies and standard operation procedures ("SOPs") for specific departments and/or operational activities that deal with personal data. The policies/SOPs that require electronic documents containing personal data to be protected are:

(a) "Data Management for CPE Programmes Policies and Procedures" applies to employees dealing with continuing professional education. It requires encryption for excel reports generated that contains personal data.

(b) "Data Management" applies to the Member Services and Marketing department of ISCA. It requires internal reports generated by the department that contain personal data to be "*encrypted with password*".

(c) The SOP entitled "Student Data Management" attached 2 emails in relation to the protecting files that contain personal data which stated:

(i) "*Please ensure that your files are password-protected especially if they contain personal data such as name, NRIC number, address, phone number and email address*"; and

(ii) "For electronic transmission (i.e. email, thumbdrives etc) of personal data, please ensure the files are encrypted".

17 However, none of ISCA's security arrangements at [15] and [16] required password based encryption for the Excel File in the circumstances leading up to the Incident.

(a) ISCA's Information Sensitivity Policy did not apply because the System/Network Engineer intended to send the Excel File by email to authorised recipients within ISCA only.

(b) ISCA conceded that none of the policies/SOPs at [16] applied to the System/Network Engineer who was in ISCA's ICT department.

18 The Commissioner found that ISCA failed to put in place reasonable security arrangements to protect the Subject Data in the Excel File during email transmission for the following reasons:

(a) The volume (1,906 members) and type (data with a higher expectation of confidentiality) of Subject Data in the Excel File warranted direct protection. In this regard, ISCA should have had a policy/SOP that applied to all employees requiring password based encryption for the Excel File in respect of both external and internal emails. This would be a reasonable security arrangement to protect the Subject Data against unauthorised access in the event the Subject Email was sent to any unintended recipient.

(i) ISCA's Information Sensitivity Policy at [15] was not a sufficient security arrangement as it only required password based encryption for external emails.

(ii) ISCA's "Student Data Management" SOP at [16(c)] recognised that the Subject Data in the Excel File required direct protection. Under this SOP, the Employees who had requested the Excel File would have had to ensure that the Excel File is encrypted with a password for electronic transmission. However, as discussed at [17(b)], this SOP did not apply to the System/Network Engineer. At the material time, ISCA did not have a specific policy/SOP for the ICT department in respect of its operational activities that deal with personal data.

(iii) According to ISCA, the System/Network Engineer did not open the Excel File when recovering it from ISCA's backup server. He was therefore not aware that the Excel File did not have password based encryption. This excuse is not credible for the reason that when the Employees requested for the restoration of an Excel file from the backup server, one would have expected that the least that would have been done was for the System/Network Engineer to open the file to be sure that it had been properly restored and thus usable by the Employees. It is more likely that the System/Network Engineer had opened the file but it had not occurred to him that it was a spreadsheet containing voluminous personal data. In any event, the lack of policy/SOP for the ICT department and the gap in the extant Information Sensitivity Policy meant that the System/Network Engineer would not have been required to password protect the restored Excel file.

(b) ISCA conducted PDPA training for its employees. In this regard, data protection training only has an impact on the proper implementation of an organisation's data protection policies and practices. It does not replace the requirement for an organisation to have the necessary data protection policies in respect of its operational/business activities that deal with personal data. In the present case, ISCA did not have any policy/SOP that if properly implemented, would have been a reasonable security arrangement to protect the Excel File during internal email transmission.

19 For the reasons above, the Commissioner finds ISCA in breach of section 24 of the PDPA.

Representations by ISCA

20 ISCA made representations following the issuance of a preliminary Decision to ISCA. The representations did not go to the merits of the matter but were mainly related to the timelines for ISCA to comply with the Commissioner's directions. The Commissioner has considered the representations made and has made adjustments to the timelines in the final set of directions below.

The Commissioner's Directions

21 Given the Commissioner's findings that ISCA is in breach of section 24 of the PDPA, the Commissioner is empowered under section 29 of the PDPA to issue ISCA such directions as it deems fit to ensure compliance with the PDPA. This may include directing ISCA to pay a financial penalty of such amount not exceeding S$1 million.

22 In assessing the breach and determining the directions, if any, to be imposed on ISCA in this case, the Commissioner took into account the following mitigating factors:

(a) ISCA notified the Commission of the Incident and was fully cooperative in the investigations;

(b) The unauthorised disclosure was limited to a single Unintended Recipient for a short period of 10 minutes;

(c) ISCA took prompt action to mitigate the impact of the Incident by (i) requesting the Unintended Recipient to permanently delete the Subject Email containing the Excel File; and (ii) notifying all affected individuals of the Incident; and

(d) There was no evidence to suggest any actual loss or damage resulting from the unauthorised disclosure.

23 Having considered all the relevant factors of this case, the Commissioner hereby directs ISCA to do the following:

(a) Within 90 days from the date of the Commissioner's directions, review its policies and security arrangements in respect of electronic transmission of documents containing personal data; and

(b) Pay a financial penalty of S$6,000.00 within 30 days from the date of the Commissioner's direction, failing which, interest at the rate specified in the Rules of Court[3] in respect of judgment debts, shall accrue

[3] Cap 322, R5, 2014 Rev Ed.

and be payable on the outstanding amount of the financial penalty until the financial penalty is paid in full.

YEONG ZEE KIN
DEPUTY COMMISSIONER
FOR COMMISSIONER FOR PERSONAL DATA PROTECTION