SAFRA National Service Association
[2019] SGPDPC 45

Yeong Zee Kin, Deputy Commissioner — Case No DP-1809-B2711

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

16 December 2019

Facts of the Case

1 On 13 September 2018, the Personal Data Protection Commission (the "**Commission**") received a voluntary breach notification from SAFRA National Service Association (the "**Organisation**"). An employee of the Organisation (the "**Employee**") who had sent out two separate batches of e-mails attaching an Excel spreadsheet (the "**Spreadsheet**") containing the personal data of certain members of the Organisation's shooting club (the "**SSC**") to other members (the "**Incident**").

2 According to the Employee, his job scope included sending mass e-mails to SSC members. He has been sending such e-mails since September 2016 at least once a month. According to him, he was not aware of any SOPs for sending of such mass emails. The Employee claims that his supervisor had instructed him verbally on the process. First, prepare proposed e-mail, and attach a spreadsheet containing intended recipients' e-mail addresses extracted from another internal system. Next, send this draft email from his individual work e-mail account to the official SSC e-mail account. Thereafter, copy the intended recipients' emails addresses into the draft email, and delete the attached spreadsheet, before sending out the mass email. This is the process that the Employee has been following whenever he sends mass e-mails to SSC members, as was the case during the Incident.

3 The Organisation claims that it was not aware of this process for mass e-mails. However, its staff were briefed on the practice of using the bcc function when sending mass e-mails and were verbally instructed to "*check and ensure that no unnecessary information or document (including those which contain personal data) has been enclosed before sending an email to members*".

4 The Incident occurred on 9 September 2018. The Employee followed this procedure to publicise an upcoming event. After copying the e-mail addresses from the Spreadsheet and pasting it in the bcc field of the e-mail, the Employee tried to delete the Spreadsheet. He was prompted by the webmail that "*the attachment could not be removed and to try again*". This was the first time he encountered such an error message. The Employee claims that upon trying to delete the Spreadsheet again, "*the Spreadsheet disappeared from the email draft*" and he proceeded to send the first batch of mass e-mails. The same thing happened for the second batch of mass e-mails sent by the Employee. According to the Employee, he was notified by an SSC member right after sending the second batch of mass e-mails that the Spreadsheet had been attached to the mass e-mails. Upon checking the "Sent Items" folder on the SSC e-mail account, he realised that the Spreadsheet was attached in the sent e-mails.

5 The Incident resulted in the Spreadsheet containing the personal data of 780 SSC members being sent to 491 SSC members. The types of personal data in the Spreadsheet (the "**Personal Data**") included the following:

(a) Name;

(b) NRIC number;

(c) Date of birth;

(d) Address;

(e) Telephone number; and

(f) E-mail address.

6 Upon being notified of the Incident, the Organisation took the following remedial actions:

(a) Completed the masking of members' NRIC number in its internal systems and reports, which it was in the process of undertaking;

(b) Circulated the Commission's guidelines on Personal Data Protection Act 2012 (the "**PDPA**") with reminders to be mindful when handling personal data;

(c) Notified all affected SSC members about the Incident via e-mail and SMS, and provided an e-mail address and phone number for members to contact for any queries on the Incident;

(d) Put up an announcement on the Organisation's website regarding the Incident;

(e) Set up an incident response team and incident management hotline and prepared an FAQ for its frontline staff; and

(f) Followed up with phone calls to the SSC members who received the Spreadsheet to delete the attachment.

Findings and Basis for Determination

7 Section 24 of the PDPA requires an organisation to 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 ("**Protection Obligation**").

8 As a preliminary point, the Organisation alleges that it had replicated the steps taken by the Employee to confirm whether or not the Employee's version of events was accurate. The Organisation claimed that, in replicating these steps, it had similarly encountered the issue as set out in paragraph 4 above. When the Commission requested for evidence of the tests conducted, the Organisation provided some screenshots of emails with attachments, and stated that the test results were not saved, although *"[the investigation team] had witnessed [the test] but no screen shot or video recording was made".* However, these screenshots were inconclusive in demonstrating that the Organisation managed to replicate the issues. As part of its investigations, the Commission contacted the Organisation's webmail software service provider who informed that it had not encountered such an issue nor had it encountered or received any enquiry on such an issue from users of its webmail software at the material time. On a balance of probabilities, based on a review of the evidence before me, I am unconvinced that there was a software glitch. It is more likely that the Employee had simply failed to delete the attached Spreadsheet prior to sending the emails out.

9 The key issue in this case revolves around the practice adopted by the Organisation for sending mass e-mails. The Organisation's method of drafting the mass e-mail using the

individual work e-mail address of the relevant employee and then sending it to the official SSC e-mail address with the Spreadsheet attached gave rise to the risk of accidental disclosure of the Personal Data in the Spreadsheet. Manual processes such as this give rise to risks of human error. Having in mind that this is a task that the Employee had to perform at least once a month, and the fact that the Organisation had already digitized its membership records, the task could have been partially automated. There are readily available technical solutions like mail-merge functions or the creation of frequently used mailing lists. The Commission's Guide to Preventing Accidental Disclosure When Processing and Sending Personal Data (published 20 January 2017) states (at [2.1]) that organisations may implement automated processing of documents or communications containing personal data (e.g. merging content or populating fields from various sources) to ensure destination information is correct. Organisations are also reminded to ensure the accuracy and reliability of the automated processing implemented by checking these systems and processes regularly.

10 Further, the Guide on Printing Processes for Organisations (published 3 May 2018) also provides guidance (at page 11) on how organisations may use Mail Merge when emailing to ensure the accuracy of the list of intended recipients and the corresponding merged fields in the email.

11 Additionally, the Organisation was unaware of this manual process that its Employee had been using since September 2016 (and potentially earlier, by other employees or by his supervisor) to send out mass e-mails. As stated in [3], the Organisation claimed that it had given certain verbal instructions to its staff on data protection handling practices pertaining to e-mail correspondence. In general, verbal instructions are insufficient as employees would be unable to refer to them in the course of their duties and may very well be unable to recall such instructions after some time. For a regular and perhaps even frequent task like the present monthly mass e-mail to members to publicise upcoming events, the Organisation should have a properly documented process and consider the use of process automation tools.

12 In light of the foregoing, I am satisfied that the Organisation had contravened section 24 of the PDPA.

13 The Organisation informed the Commission after the preliminary Decision in this matter was issued to the Organisation that the following measures have since been put in place:

(a) Mass emails will no longer be sent using the Organisation's generic email account and will only be sent out by a designated Executive or authorised personnel approved by the Club Manager using his or her individual work email account;

(b) The downloading of the list of members from the Organisation's system will be carried out by the Executive personally;

(c) The categories of personal data in the list of members that may be downloaded from the system has been reduced;

(d) The frequency of mass emails to update members on programmes and events will be reduced from monthly to bi-monthly or quarterly;

(e) All new staff will undergo an orientation programme on the operations of the shooting club within the 1st week of joining and only selected staff will be allowed to handle email updates and will also be trained within the 1st week of joining the club;

(f) More stringent access controls to the Organisation's databases have been implemented;

(g) The 1st 5 characters of members' NRIC numbers are masked in the Organisation's internal systems;

(h) The IT Policy has been updated to include guidelines for the protection, encryption and sharing of the Organisation's database. As part of this update, databases are to be encrypted or password protected before they are shared and may only be shared with the written consent of a Head of Department or custodian; and

(i) Training has been provided to staff on data handling.

14 The Organisation also informed that it was in the midst of enhancing its existing system to automate the sending of mass emails. The Organisation asked for an extension of the timeframe for implementation of the second direction set out in the next section. The Deputy Commission has decided to accede to the Organisation's request and has lengthened the timeframe to the period set out below.

The Deputy Commissioner's Directions

15 In determining the directions to be imposed on the Organisation under section 29 of the PDPA, I took into account the following mitigating factors:

(a) the Organisation voluntarily notified the Commission of the Incident;

(b) the Organisation was cooperative and had provided prompt responses to the Commission's requests for information;

(c) the Organisation implemented remedial actions swiftly to address the Incident; and

(d) there was no evidence of any further unauthorised use of the Personal Data in the Spreadsheet.

16 Having carefully considered all the relevant factors of this case, I hereby direct the Organisation:

(a) to pay a financial penalty of $10,000 within 30 days of 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; and

(b) to conduct a review of its email system and processes to put in place process safeguards and written internal standard operating procedures to protect the personal data of its members within 120 days of the date of this direction.

———————————