Matthew Chiong Partnership

[2019] SGPDPC 7

Tan Kiat How, Commissioner — Case No DP-1709-B1138

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

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

3 June 2019.

Background

1 An administrative staff of Matthew Chiong Partnership (the "**Organisation**") mistakenly sent out email correspondences meant for a client (the "**Complainant**") to an incorrect email address on two separate occasions. Additionally, a third email correspondence was mistakenly sent by the Managing Partner and Data Protection Officer of the Organisation (the "**Managing Partner**") to the Complainant with an attachment which mistakenly contained the names of two other clients of the Organisation. The Commissioner found the Organisation to be in breach of its Protection Obligation and Openness Obligation under the Personal Data Protection Act 2012 ("**PDPA**"). The Commissioner's findings and grounds of decisions are set out below.

Material Facts

2 The Organisation is a Singapore-registered law firm which provides estate planning services and handles property transactions for its clients.

3 On 28 August 2017, an administrative staff from the Organisation sent an email ("**Email 1**") to two individuals informing them that the legal documents for their property refinancing had been prepared and were ready for signature. One of the email addresses was incorrect as the administrative staff made an error in the email address – as an example and only for illustration purposes, by typing AAA@yahoo.com instead of ZAAA@yahoo.com. The incorrect email address was a valid email address as the Complainant had sent a test email to that email address after Email 1 was sent and did not receive a mail delivery failed message. This mistake was identified by the sister of the Complainant ("**Sister**"), one of the intended recipients, who informed the Complainant. Once the Complainant informed the administrative staff, the administrative staff re-sent the email to the Complainant. Email 1 disclosed information including the email address of the Sister, the residential address of Complainant and Sister, and the name of the bank in relation to the Complainant and Sister's mortgage of their property.

4 The second incident occurred on 15 September 2017 when the same administrative staff sent an email ("**Email 2**"), enclosing a letter addressed to a bank from the Organisation and a redemption statement issued by the bank, to the same incorrect email address. Email 2 disclosed information including the full names, NRIC numbers, residential address, financial data such as the mortgage account information (consisting the name of bank, account holders' full names, loan account number, file reference number, name of security, and redemption statement of account for the month of September 2017) of the

Complainant and her Sister. Following the two incidents, the Managing Partner apologised to the Complainant and Sister and offered: (i) a full refund of legal costs; and (ii) to absorb all the disbursements incurred in handling the property transaction.

5 Subsequently, on 29 September 2017, the Managing Partner sent an email ("**Email 3**") to the Complainant and Sister enclosing two attachments: (i) a Letter of Approval from the Central Provident Fund ("**CPF**") Board; and (ii) a blank Authorisation Use of CPF for Purchase of Private Property form. The Complainant noticed that there were two different documents contained within the Letter of Approval, and one of the pages reflected the full names of two other individuals ("**Other Clients**"), who were clients of the Organisation, and who were unrelated to the Complainant's property transaction and unknown to the Complainant and Sister.

6 The table below sets out the three emails sent (collectively, the "**Emails**") and the enclosed attachments (collectively, the "**Attachments**") along with a description of the corresponding information that was disclosed without authorisation.

	Type of Document	**Information Disclosed**
Email 1	Correspondence	• The Sister's email address; • the Complainant's and Sister's residential address; and • the name of the bank in relation to the mortgage of the property.
Email 2	1. A letter addressed to a bank from the Organisation	• The Complainant's and Sister's full names; • the Complainant's and Sister's NRIC numbers;

	2. A redemption statement issued by the bank	• the Complainant's and Sister's residential address; and • financial data such as the mortgage account information which consists of the name of the bank, account holders' full names, loan account number, repayment information, and information relating to the collateral for the loan.
Email 3	1. A Letter of Approval from CPF Board 2. A blank Authorisation Use of CPF for Purchase of Private Property Form	• The full names of Other Clients who were other clients of the Organisation, within 2 pages of documents which formed part of a larger 10-page legal document relating to the Other Clients.

The Commissioner's Findings and Assessments

Main Issues for Determination

7 The issues to be determined in the present case are as follows:

(a) whether the information disclosed by the Emails and Attachments constituted personal data within the meaning of the PDPA;

(b) whether the Organisation had implemented reasonable security arrangements to protect the personal data in its possession or under its control, as required pursuant to section 24 of the PDPA; and

(c) whether the Organisation had put in place policies and practices relating to personal data, as required pursuant to section 12 of the PDPA.

Issue (a): Whether the information disclosed by the Emails and Attachments constituted personal data

(i) The information disclosed in the Emails and Attachments were personal data

8 Section 2(1) of the PDPA defines personal data as data, whether true or not, about an individual who can be identified from either that data, or from that data and other information to which the organisation has or is likely to have access. Given that the full names, residential address, NRIC numbers, email addresses and financial data of the Complainant and Sister were disclosed, it would have been possible to identify the Complainant and Sister from the information contained in the Emails and Attachments. Taking just the email address of the Complainant as an example, given that it contained the partial name of the Complainant, it in itself would potentially allow a third party to identify the Complainant. The disclosure of the full names of the Other Clients in Email 3 would also have allowed a third party to identify these individuals. Accordingly, the information contained in each of the Emails and Attachments or collectively, amounted to personal data within the meaning of section 2(1) of the PDPA.

(ii) The personal data contained in Emails and Attachments were sensitive in nature

9 The earlier decisions of the Commissioner have identified that certain information by reason of the context of their disclosure or by their very nature would be considered as personal data that is sensitive.[1] These include but are

1 See *Re Credit Counselling Singapore* [2017] SGPDPC 18 at [11].

(*cont'd on next page*)

not limited to NRIC/Passport numbers[2], financial data such as bank account details containing the name of the bank, the bank account number and the account holder's name[3], and insurance policy data such as the premium amount and type of coverage[4].

10 As set out in the table at paragraph 6, the following personal data had been disclosed: the bank name, the NRIC numbers of the Complainant and Sister, loan account number of the bank, repayment information and collateral information. The disclosure of such information could have led to harm to the Complainant and Sister as such financial information could have exposed the Complainant and Sister to the risk of fraud and identity theft. As such, the personal data of the Complainant and Sister which had been disclosed, when taken as a whole, constituted sensitive personal data.

11 Since the Organisation is in the business of providing legal services, and handles large volumes of personal data on a day to day basis, the Organisation and its staff members should be vigilant in its handling of personal data. The fact that the same administrative staff managed to send the emails to the incorrect email address on two separate occasions within a period under one month – ie between 28 August and 15 September 2017 – despite being told of the mistake demonstrated that a culture of care and responsibility towards the handling of the personal data had not been sufficiently ingrained within the Organisation.

---

2 *Re JP Pepperdine Group Pte. Ltd.* [2017] SGPDPC 2 at [22]; and *Re Singapore Telecommunications Limited and another* [2017] SGPDPC 4 at [26].

3 *Re AIA Singapore Private Limited* [2016] SGPDPC 10 at [19].

4 *Re Aviva Ltd and another* [2016] SGPDPC 15 at [38].

Issue (b): Whether the Organisation has complied with its Protection Obligation under Section 24 of the PDPA

(i) Personal data of a sensitive nature is subjected to a higher standard of protection

12 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 (the "**Protection Obligation**").

13 In *Re Credit Counselling Singapore* [2017] SGPDPC 18 ("***Re Credit Counselling Singapore***")[5] and *Re Aviva Ltd* [2017] SGPDPC 14 ("***Re Aviva Ltd* [2017]**")[6], the Commissioner opined that organisations are required to take extra precautions and ensure that higher standards of protection are accorded to sensitive personal data due to the actual or potential harm, and the severity of such harm arising from the unauthorised disclosure of such data. This point was again emphasised in the recent decision of *Re Aviva Ltd* [2018] SGPDPC 4 where sensitive personal data was disclosed due to a lack of safeguards put in place to protect against the unauthorised disclosure of personal data in the organisation's enveloping process. The PDPC's Advisory Guidelines on Key Concepts in the Personal Data Protection Act urge organisations to "*implement robust policies and procedures for ensuring appropriate levels of security for personal data of varying levels of sensitivity*".[7]

---

5 *Re Credit Counselling Singapore* [2017] SGPDPC 18 at [25] and [26].

6 *Re Aviva Ltd* [2017] SGPDPC 14 at [17] and [18].

7 PDPC, Advisory Guidelines on Key Concepts in the Personal Data Protection Act (revised on 27 July 2017) at [17.3].

(*cont'd on next page*)

14 Further, the Commissioner in *Re Credit Counselling Singapore* advised that suitable checks and controls be implemented before emails containing sensitive personal data are sent.[8] These may range from process-based supervision to technological controls like using the "mail-merge" function in Outlook. Credit Counselling Singapore had, after the data breach, automated the process of sending emails using mail-merge software. The Organisation in this case should similarly consider putting in place a similar technological solution since it has to churn out standard form emails regularly.

15 However, the Commissioner "*is not suggesting that organisations would need, for example, to have the added layer of supervision in all cases where emails containing personal data are being sent out … organisations are to put in place security arrangements that are commensurate with the sensitivity of the data in question – a balance of considerations*."[9] The PDPC's guide to preventing accidental disclosure when processing and sending personal data encourages organisations to have a process to double check and verify: (i) the recipients' email addresses; (ii) whether the right attachments containing the correct personal data are attached; and (iii) whether the attachments are for the intended recipients before sending the emails out.[10] Therefore, implementing additional checks and controls when handling sensitive personal data is not a mandatory requirement but one that should be adopted where appropriate. Ultimately, the facts of the case and the type of personal data being handled will influence whether or not the current checks and controls implemented in the particular organisation are sufficient.

---

8 *Re Credit Counselling Singapore* [2017] SGPDPC 18 at [29].

9 *Re Credit Counselling Singapore* [2017] SGPDPC 18 at [30].

10 PDPC, Guide to Preventing Accidental Disclosure When Processing and Sending Personal Data (20 January 2017) at [2.1]

(ii) The Organisation failed to implement adequate security arrangements which led to the unauthorised disclosure of personal data

16 The Organisation explained that the unauthorised disclosure in the Emails were caused by human error and failure to conduct thorough checks of the recipients' email addresses and the content of the attachments before sending out the email to the recipients. For Email 1 and Email 2, the administrative staff had entered an incorrect email address which the Organisation claims has never occurred when she had sent out electronic communications on previous occasions. For Email 3, the Letter of Approval was printed on recycled paper and scanned by an employee of the Organisation. However, the employee had scanned the Letter of Approval using the double-sided scanning mode which was the previous setting left on the scanner. As a result, a page containing the names of the Other Clients who were also clients of the Organisation was scanned together with the Letter of Approval.

17 The excuse that this was a one-off mistake by the employees and the Managing Partner of the Organisation, and not due to any lack of or failure to implement reasonable security arrangements pursuant to section 24 PDPA was duly considered by the Commissioner. This was an alternative position previously considered by the Commissioner in *Re Furnituremart.sg* [2017] SGPDPC 7 ("***Re Furnituremart.sg***").[11] The Commissioner in *Re Furnituremart.sg* ultimately concluded that the organisation lacked the necessary policies and practices to protect personal data.[12] Similarly, the Commissioner also takes the view in this case that the Organisation failed to

11 *Re Furnituremart.sg* [2017] SGPDPC 7 at [11].

12 *Re Furnituremart.sg* [2017] SGPDPC 7 at [17].

implement reasonable security arrangements, and the incident could not be considered as a one-off inadvertent disclosure.

18 As a starting position, under section 53(1) of the PDPA, is that the Organisation is liable for the acts and conduct of its employees in relation to the unauthorised disclosure of the personal data. In response to the Commissioner's request of the details of the Organisation's security arrangements, the Organisation stated that: (i) all employees were briefed on the need to keep private and confidential personal data of their clients on a regular basis; and (ii) all employees were advised to cut and paste email addresses of clients from a legitimate source of information or click the "Reply" function to the email sent from a client rather than typing in the email addresses. However, the Organisation was unable to provide any evidence of such briefings to its employees.

19 In *Re Aviva Ltd* [2017], the Commissioner found that "*it is insufficient for the Organisation to solely depend on its employees to carry out their duties diligently as a type of safeguard against an unauthorised disclosure of personal data*".[13] This case is no different. Therefore, the Commissioner finds that the Organisation's briefing to and/or giving advice to employees was by itself insufficient to prevent the unauthorised disclosure of personal data, particularly given the sensitive nature of the personal data.

20 Further, the nature of the Organisation's services is a relevant factor to be taken into consideration. In *Re Credit Counselling Singapore*, the Commissioner observed that "… *it is foreseeable that there will be risks of*

13 *Re Aviva Ltd* [2017] SGPDPC 14 at [28].

(*cont'd on next page*)

inadvertent disclosure of sensitive personal data" where the organisation "*routinely handles large volumes of sensitive financial personal data of individuals*".[14] In the present case, the Organisation is a law firm and the staff handling conveyancing matters handle sensitive personal data on a day-to-day basis and it was therefore foreseeable that there were risks of inadvertent disclosure of sensitive personal data. Given the nature of the Organisation's work, the Organisation ought to be subject to a higher level of care and responsibility for its clients' personal data.

21 The Commission released a Guide to Data Protection Impact Assessment which is intended to assist organisations interested in conducting data protection risk assessments. The Commissioner encourages the Organisation to carry out a data protection risk assessment on its conveyancing department, which should help to identify and address the specific risks that exists in its operational processes. This will assist the Organisation to put in place effective risk mitigation measures.

22 Given the Commissioner's findings above that the Organisation did not put in place adequate security arrangements to protect the personal data of its clients, it is hereby concluded that the Organisation was in breach of the Protection Obligation under section 24 of the PDPA.

Issue (c): Whether the Organisation has complied with its Openness Obligation under Section 12 of the PDPA

(i) The Organisation did not implement any policies or practices to protect personal data

---

14 *Re Credit Counselling Singapore* [2017] SGPDPC 18 at [32].

23 The investigations revealed that the Organisation did not put any policies or practices in place to protect personal data. In *Re Furnituremart.sg*, the Commissioner decided that "*the lack of a written policy is a big drawback to the protection of personal data … Having a written policy is conducive to the conduct of internal training, which is a necessary component of an internal data protection programme*".[15] The Organisation's claim that internal briefings were conducted to raise staff awareness were unsubstantiated by any supporting evidence. Nevertheless, even if verbal briefings were indeed given, this in itself would not be sufficient for the Organisation to discharge its obligations under section 12 of the PDPA. In general, an organisation should have some form of written policy or practice in place in relation to protecting personal data especially if the process is complex or if the organisation frequently deals with sensitive personal data on a daily basis. A well-drafted written policy has the advantage over verbal instruction of being a resource that can generally be subsequently relied upon to provide clarity about the appropriate procedures and controls to employees and help minimize the chance for any misunderstanding or miscommunication. This may take the form of written standard operating procedures in dealing with personal data which would set out the operational process of how employees should deal with personal data to prevent data protection breaches. For example, a process which implements the suggestion set out at paragraph 15 above may be set out in the form of a standard operating procedure.

---

15 *Re Furnituremart.sg* [2017] SGPDPC 7 at [14].

24 Based on the above, given that the Organisation had not developed and implemented policies and practices that are necessary to protect personal data, it is the conclusion of the Commissioner that the Organisation is in breach of the Openness Obligation under section 12 of the PDPA.

Representations

25 The Organisation, by way of email dated 3 January 2019, requested that the imposition of financial penalty amount be removed or that the amount be reduced. In this regard, the Organisation made the following representations:

(a) the disclosure was not a deliberate act on the part of the Organisation or any of its staff;

(b) the incidents related to one single conveyancing case involving 2 individuals;

(c) the Organisation waived all legal costs and expenses incurred in the matter in which it advised the Complainant;

(d) the information disclosed is generally regarded as sensitive but that it had absolutely no interest to the recipient; and

(e) the unauthorised disclosure was not due to lack of supervision and it was not possible to check all email addresses every time there is an email to be sent out. The staff member who committed the error was 50 years old and probably has long-sightedness. The staff was not in the email thread and so she could not have copied the email address from the header of prior emails to the client. The said staff has since left the Organisation's employment.

26 The Commissioner in deciding to impose a financial penalty and on the appropriate quantum of the financial penalty had already taken into consideration the issues raised by the Organisation and as set out at paragraph 25(a) to (c) above.

27 With regard to the issue raised by the Organisation and set out at paragraph 25(d), the Commissioner notes that the Organisation agrees that the information disclosed in these incidents is sensitive.

28 With regard to the issue raised by the Organisation and set out at paragraph 25(e) above, the basis for the finding of a breach of the Organisation's obligation under section 24 of the PDPA was that the Organisation failed to implement reasonable security arrangements. In this regard, the Commissioner does not expect organisations to check the email addresses every time there is an email to be sent out. However, as explained above at paragraph 15, the Organisation ought to have implemented a considered process to verify that emails are correctly addressed to the intended recipient – the Organisation did not adduce any evidence of such a considered process. Nevertheless, the Commissioner has decided on compassionate grounds to reduce the quantum of the financial penalty set out in the preliminary decision issued to the Organisation, given that the staff who committed the error was advanced in age and long-sighted.

The Commissioner's Directions

29 The Commissioner is empowered under section 29 of the PDPA to issue directions as it thinks fit in the circumstances. This may include directing the Organisation to pay a financial penalty of such amount not exceeding S$ 1 million as the Commissioner thinks fit.

30 In assessing the breach and determining the directions to be imposed on the Organisation in this case, the Commissioner took into account the Organisation's dilatory conduct during investigations. It had been neither cooperative nor forthcoming in its responses to the Notice to Require Production of Documents and Information ("**NTP**") issued by the Commissioner as part of its investigations. The Organisation took a month to respond to the first NTP and second NTP despite being sent reminders by the Commissioner on several occasions:

(a) The first NTP was sent on 12 December 2017 with a deadline to respond by 22 December 2017. The Organisation failed to meet the deadline and only on 2 January 2018, more than a week after the expiry of the deadline, did the Organisation write requesting for an extension of time to respond. The extension sought was up to 4 January 2018. The Organisation was granted an extension of time to respond by 10 January 2018. The organisation finally responded on 11 January 2018.

(b) The 2nd NTP was sent on 22 January 2018 requiring the Organisation to respond by 1 February 2018. The Organisation again failed to meet the deadline and did not even request for an extension of time to respond. The investigating officer had to call the Organisation on 6 February 2018 to ask the Organisation why it had failed to respond to the 2nd NTP within the deadline. During this conversation, the Organisation requested for an extension of time of the deadline. The investigating officer informed the Organisation that she would issue a reminder with a deadline to respond by 15 February 2018. The reminder was issued on 7 February 2018. The Organisation failed to comply with this new deadline. In fact, no correspondence from the Organisation was received even by 20 February 2018. On 20 February, the investigating

officer called the Organisation as a further reminder. Only after this did the Organisation respond to the 2nd NTP on 23 February 2018.

31 Having considered all the relevant factors of this case, the Commissioner hereby directs the Organisation to pay a financial penalty of S$8,000 within 30 days from the date of the Commissioner's direction, failing which, interest, at the rate specified in the Rules of Court in respect of judgment debts, shall be payable on the outstanding amount of such financial penalty.

32 In addition, the Commissioner hereby issues the following directions to the Organisation:

(a) to implement a data protection policy and internal guidelines or standard operating procedures to comply with the obligations under the PDPA;

(b) for all employees of the Organisation handling personal data to attend a training course on the obligations under the PDPA and the Organisation's data protection policies; and

(c) to complete the above directions within 60 days from the date of this decision and inform the office of the Commissioner of the completion thereof within one week of implementation.

YEONG ZEE KIN
DEPUTY COMMISSIONER
FOR PERSONAL DATA PROTECTION