SLF Green Maid Agency

[2018] SGPDPC 27

Yeong Zee Kin, Deputy Commissioner — Case No DP-1806-B2265

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

13 December 2018.

Background

1 This case arose out of the common practice of reusing scrap or discarded paper where the reverse side of the paper can still be used. This is highly commendable and environmentally-friendly, but organisations must take care to ensure that there is no personal data on the scrap or discarded paper set aside for such re-use. An employee of SLF Green Maid Agency (the "**Organisation**") wrote information for the Complainant on a piece of paper which contained personal data of other individuals on the reverse side and gave the paper to the Complainant. This happened on two separate occasions. The key issue is whether this disclosure of personal data by the Organisation amounts to a breach of section 24 of the Personal Data Protection Act 2012 ("**PDPA**").

Material Facts

2 On 8 April 2018, the Complainant visited the Organisation's office to enquire about engaging a foreign domestic worker. An employee of the

Organisation assisted her and over the course of these enquiries, the employee handed the Complainant some paper on which he wrote information related to her query. The Complainant discovered that the reverse side of the paper contained personal data of other individuals. The Complainant informed the employee that the paper that was used should not have been given to the Complainant.

3 On 24 April 2018, the Complainant returned to the Organisation's office and was served by the same employee. Again, over the course of the queries, she was provided information hand written on used paper. Similarly, the reverse side of the paper contained personal data of other individuals.

4 Over the two occasions, the following personal data was disclosed to the Complainant:

(a) On the first occasion, the used side of the paper contained a photocopy of the front and back of an individual's NRIC.

(b) On the second occasion, the used side of the paper was a letter detailing a family's personal circumstances, explaining why a foreign domestic worker was required by them. The letter also contained four individuals' names and two of their FIN numbers. In an accompanying portion of a contract, the same four individuals' passport numbers and passport expiry dates were found; and

(c) the same portion of a contract contained five other individuals' names and NRIC numbers, with some accompanying signatures.

Did the Organisation breach section 24 of the PDPA

5 Section 24 of the PDPA stipulates 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. It is undisputed that the personal data listed in paragraph **Error! Reference source not found.** was disclosed without authorisation. The totality of the circumstances led me to conclude that the unauthorised disclosure stemmed from the Organisation's lack of reasonable security arrangements to prevent such disclosure. I set out the factors leading to this conclusion below.

6 Organisations that re-use scrap paper should put in place reasonable security measures to prevent scrap paper containing personal data from being re-used or given to other clients. The security arrangements will have to involve at least two aspects:

(a) Implementing a system of processes backed up by policies, and

(b) Training of staff to be aware of the risks and to be alert to spot them.

7 In this case, investigations did not turn up any process or system within the organisation for segregating scrap paper containing personal data from the pile(s) of scrap paper that can be re-used by staff.

8 Neither were there any policies. In fact, the Organisation admitted that they did not have a detailed policy with respect to personal data protection nor did they provide staff with any formalised training on personal data. Instead, the Organisation relied on the management's verbal directions to screen through all

discarded paper and to destroy any paper that contained personal data; and that only paper which did not contain personal data was to be re-used. The Organisation intimated, in written responses during investigations, that the following instructions were given to employees:

> "Physical Office Manning- Office should be manned continuously by staff during operating hour. In occasion that staff is alone in office and the need to leave the office, say go to the toilet, office should be locked. Do not leave office open but unattended.
>
> Management of Client's data- Clients (Employer/customer and FDW) data should not be used or discussed loosely. Not even between staff and staff. Management insists that no loose talk on sensitive data like how rich is an employer and personal income, where employer stays, etc... Only on a need to know and authorized to know basis.
>
> Clients/FDW's document. Individual client/FDW's document are filed and serialized. Files are safe keep in cabinet within the office space which is locked after office hour.
>
> Access to Personal Computer. Instruction to all staff is that "outsider" person who is not authorized is not allowed to "touch" our personal computer. Ever happened before that a staff let a customer use her personal computer to check certain thing from website was reprimanded."

9 To my mind, these instructions were insufficient and failed to establish the practices around the Organisation's policy of using discarded paper that contained personal data.

10 The Organisation intimated that they prominently pasted a set of guidelines on handling personal data and provided a copy of a document entitled "Guidelines to Personal Data Protection" ("**Organisation's "Guidelines"**"). The relevant part of the Organisation's "Guidelines" stated:

> "Proper Housekeeping Other than the document that Staff is working on at any point in time, no other unnecessary document, especially document with personal data should be lying around on the working table or other places."
>
> …

> "Management of waste paper with personal information on it. Waste paper with personal data on them are not to be disposed of in public rubbish bin direct, unless data is permanently masked off by using permanent marker and is torn into small pieces." (emphasis in original)

11 There are a couple of issues with the Organisation's Guidelines. First, they do not address the re-use of discarded paper containing personal data directly. They deal with safekeeping and disposal of waste paper containing personal data. Second, investigations did not uncover any evidence to substantiate that the Organisation's Guidelines were provided to its employees.

12 Turning now to the importance of staff training as a security arrangement. It has been said before in Re: National University of Singapore *[2017] SGPDPC 5* and it bears repeating that training is important to inculcate the right employee culture and establish the right level of sensitivity to personal data amongst staff. The organisation admitted that no training had been provided. The closest form of training in this matter was a verbal exhortation by management to screen scrap paper and to discard (and not to re-use) scrap paper that contained personal data. Clearly, this was insufficient to establish the right level of employee sensitivity to client personal data. These verbal instructions did not appear to have been effective on the employee who served the Complainant as he made the same mistake to the same client twice: he handed over to the Complainant scrap paper containing personal data of other individuals on two separate occasions and had failed to retrieve them even after the employee was informed by the Complainant that he should not re-use paper with personal data.

13 For a company like the Organisation that handles personal data of foreign domestic workers and clients on a daily basis (eg passport and income information), it is necessary for it to put in place a better system of staff training

and awareness given the sensitive nature of personal data that it handles, as well as the volume. Merely disseminating guidelines and verbal instructions is insufficient. As noted in *Re Aviva Ltd*, whilst there is no specific distinction in the PDPA based on the sensitivity of the data, organisations are to ensure that there are appropriate levels of security for data of varying levels of sensitivity: [2018] PDP Digest 245 at [17] - [18]. NRIC and passport numbers and financial information would generally be considered more sensitive: *Re Aviva Ltd* at [17]. Structured and periodic training could have been implemented to protect personal data.

14 I therefore find that the Organisation was in breach of its obligation to protect personal data under section 24 of the PDPA as it did not implement reasonable security arrangements to protect the personal data found in the discarded papers. Since the incident, the Organisation has reminded its staff to comply with internal guidelines on personal data protection and the procedures for destroying documents containing personal data. They have also highlighted to the staff internal penalties for any failure to comply.

Deputy Commissioner's Directions

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

16 Taking into account the limited scope of the unauthorised disclosure, I do not think that a financial penalty is warranted and instead make the following directions:

(a) The Organisation is to conduct a review of its procedures to prevent the use of discarded or unwanted documents containing personal data within 30 days from the date of this Decision;

(b) The Organisation is to develop a training programme to ensure that all of its staff is aware of and will comply with the requirements of the PDPA when handling personal data within 60 days from the date of this Decision;

(c) The Organisation is to require all staff who have not attended data protection training to attend such data protection training in accordance with the training programme set out at (b) above within 30 days of the development of the training programme; and

(d) The Organisation is to inform the Commission of the completion of each of the above within 7 days of implementation.

YEONG ZEE KIN
DEPUTY COMMISSIONER
FOR PERSONAL DATA PROTECTION COMMISSION