Ang Rui Song

[2017] SGPDPC 13

Tan Kiat How, Commissioner — Case No DP-1610-B0257

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

14 August 2017.

Background

1 This is a case of a Financial Consultant (an "**Organisation**" under the Personal Data Protection Act 2012, and hereinafter, the "**Respondent**") who improperly disposed of his clients' insurance policy related documents, which contained sensitive personal data ("**Prudential folders**"). The documents were discovered by the Complainant at a rubbish bin of a residential estate.

2 Following an investigation into the matter, the Commissioner found that the Financial Consultant is in breach of Section 24 of the Personal Data Protection Act 2012 ("**PDPA**"). The Commissioner's findings of this matter are set out below.

Material Facts and Documents

3 The Respondent was a Financial Consultant with Prudential Assurance Company (Pte) Ltd ("**Prudential**"). The terms of his engagement as a Financial Consultant was such that the Respondent was an independent contractor and not an employee of Prudential. During his engagement as a Financial Consultant, the Respondent came into possession of his clients' Prudential folders. However, at the time that the Respondent disposed of these documents, he was no longer with the organisation.

4 On 10 October 2016, the Commissioner was informed by the Complainant that the Prudential folders had been disposed of by leaving beside the rubbish bin at level 2 of the multi-storey car-park at Blk 821A Jurong West Street 81. Upon further inspection, the Complainant found that the Prudential folders contained 13 Certificates of Life Assurance issued by the Organisation, and bore the names of 12 individuals, in addition to 2 letters addressed to 2 of the aforementioned individuals.

5 The folders contained information on 12 of the Organisation's policy-holders. Taken collectively, the information identified the individual policy-holders, which included the following pieces of personal data:

(a) Name of policy holder;

(b) NRIC Number;

(c) Benefits;

(d) Sum assured;

(e) Cover Start Date;

(f) Cover Expiry Date; and

(g) Premium.

The full list of information is set out in the Schedule of this Grounds of Decision.

6 The 2 letters were addressed to 2 of the 12 policy-holders mentioned above, and contained the following personal data:

(a) Name of Policy Owner;

(b) Address;

(c) Policy Number; and

(d) Name of Life Assured (same as the Policy Owner).

7 During investigations, the Respondent confirmed that he had disposed of the folders containing the abovementioned personal data at the location where they were found by the Complainant. The disposal was made under the instructions of the Complainant's clients. However, he claimed that he had disposed of them in the bin, and not by leaving them beside the rubbish bin. The Complainant also claimed that he had placed the documents in a plastic bag before disposal.

The Commissioner's Findings and Basis for Determination

The Respondent's obligation to protect personal data under Section 24 of the PDPA

8 As a preliminary issue, the Commissioner had considered the following question: was the Respondent acting as an "organisation" for the purposes of

the PDPA in respect of the personal data contained in the Prudential folders? If so, then, as an "organisation", he has an obligation to protect the personal data under Section 24 of the PDPA.

9 The definition of "organisation" under the PDPA expressly includes "any individual" and would apply to an individual such as the Respondent.

10 At the time the Respondent joined Prudential, he was, according to his contract, acting as an independent contractor of Prudential, and not as an employee. In dealing with his clients' personal data, he had control and autonomy over the management of the personal data. For example, he had control over how the policy folders were stored and kept in his care, and the provision and receipt of the policy documents from his clients. Accordingly, the Respondent was an "organisation" under the PDPA, and had an obligation under Section 24 of the PDPA to protect the personal data he had collected.

11 This obligation stayed with the Respondent (as an "organisation") throughout the time that he was with Prudential, and even after he had left his engagement with Prudential. This is in line with the principles in *Re Chua Yong Boon Justin* [2016] SGPDPC 13, where the Respondent was a registered salesperson who obtained personal data of the Complainant and his wife in the course of his real estate agency work and hence in the course of carrying on his business. Having obtained such personal data in a capacity that is not "personal or domestic", the Personal Data Protection Commission held that the Respondent was not allowed to claim that the subsequent disclosure of the personal data was made in a "personal or domestic capacity", which would have allowed him to dispense with the need to obtain consent under Section 4(1)(a) of the PDPA. In *Re Chua Yong Boon Justin* [2016] SGPDPC 13, the Personal Data Protection Commission held that the Respondent continued to hold such

personal data in the course of his business, and needed to comply with his Consent Obligation when disclosing the personal data. Similarly, in the present case, the Respondent had obtained the personal data during the course of his work as a Financial Consultant and an "organisation" under the PDPA – viz not in a personal or domestic capacity. He therefore had a duty to protect the personal data throughout – whilst with Prudential and after he left Prudential. The Respondent cannot unilaterally change the capacity in which he possesses the personal data, even after he ceased being a financial consultant with Prudential. The Respondent remained obliged to comply with Section 24 of the PDPA at all material times.

12 In respect of the role of Prudential, the Commissioner found Prudential not to be responsible (or liable) for the proper disposal of the policy documents, or the data breach incident that has occurred. Prudential had reasonable policies in place which dealt with proper and secure disposal of clients' policy documents. The pertinent policies required financial advisors to return client data to Prudential when they ceased being financial advisors, or (alternatively) to dispose of personal data properly and securely – for example, by shredding. Prudential had communicated these policies through appropriate channels. Indeed, in accepting the Respondent's resignation, Prudential had issued a letter specifically referring to the need to "return all monies, documents and other effects and property belonging to [Prudential] including such property containing customer information…" (emphasis added).

13 In the Commissioner's view, therefore, it was the Respondent who had full responsibility in the protection and proper disposal of the personal data found in the Prudential folders. We now turn to the analysis of whether the Respondent has complied with this obligation.

Whether the Respondent's manner of disposal of Prudential folders was a breach of Section 24 of the PDPA

14 When it comes to the disposal of documents containing personal data, there is a need to ensure that the disposal is carried out properly and in a secure manner in order to meet the requirements of Section 24. Section 24 requires an organisation to "make reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks". In this case, a reasonable security arrangement meant proper and secure disposal of the Prudential folders, which would prevent any of the risks mentioned.

15 The PDPC's Guide to Disposal of Personal Data on Physical Medium ("**PDPC's Guide to Disposal**") sets out some useful principles undergirding the proper disposal of documents containing personal data in this regard. Some of these principles are relevant to the present case and are set out below. As mentioned in the PDPC's Guide to Disposal, in order to comply with Section 24 of the PDPA, it may not be enough for an organisation to simply discard documents containing personal data in the physical trash bin. This may lead to an incomplete or improper disposal of personal data, which opens up to potential data breaches:

(a) Deleted electronic files or improperly shredded paper may be restored (in full or partially); and

(b) Uncontrolled disposal of paper without destruction may lead to recovery of documents through 'dumpster diving' (eg sifting through physical waste or recycling containers for items that have been discarded, but are still of value or covered by regulation).

16 Instead, for personal data stored on physical media and in paper form, the PDPC's Advisory Guidelines on the Key Concepts in the PDPA, advises organisations to ensure proper disposal of the documents that are no longer needed, through shredding or other appropriate means. This includes one or more of the following processes:

(a) Incineration (or burning): reduces paper to ashes;

(b) Shredding: cuts paper in a way that makes it reasonably difficult, or even impossible to reassemble the pieces in order to reconstruct (a substantial part of) the information, but allows for the paper to be recycled as long as the pieces are not too small; or

(c) Pulping: paper is mixed with water and chemicals to break down the paper fibres before it is processed into recycled paper.

17 The PDPC's Guide to Disposal also cautions that leaving documents containing personal data unattended while they await being discarded or destroyed may provide opportunities for a third party to gain access to the information, eg leaving them at the rear entrance of the office, or at the bottom of the building, for collection by the paper disposal vendor. Generally, if the unauthorised disclosure of the information contained on the paper document could result in significant impact to an individual, organisations should consider shredding the document to cut the paper into separate small pieces, which make it more difficult to reassemble. The more sensitive the information, the higher the level of shredding that needs to be done.

18 In this case, the Respondent's mode of disposal is wholly inadequate, especially given the type and sensitivity of the personal data found in the

Prudential folders, and based on the circumstances. There are several reasons for the Commissioner's finding in this regard.

19 Based on the Respondent's representations, the documents were simply put in a plastic bag, tied up and placed inside the trash bin. The documents (and their contents) were left in their original readable form, and anyone easily open the plastic bag to access the contents of the documents, especially the sensitive personal data of clients. It is foreseeable that random members of the public may dive into rubbish bins to retrieve disposed items that are recyclable, which is likely to include paper waste.

20 Additionally, with regards to the use of the plastic bag, this did not actually have the effect of securing the documents – just a mere concealment of the documents. While the mere concealment of documents may, in certain contexts, be enough when disposing of documents that contain little or no personal data of individuals, this was not appropriate in the present case.

21 The manner of disposal was inappropriate given the sensitivity of information found in the documents, such as the policy holder's name, NRIC number, premium amounts, name of life assured, benefits and sums assured, and maturity date. Based on what was pronounced earlier at paragraphs 16 to 18 above, the sensitivity of such personal data warrants there to be a greater form of protection in the disposal of these documents. In the Commissioner's view, this can only be achieved by shredding the documents. As to the level of shredding, this should be guided by the level of sensitivity of the personal data

contained in the document.[1] In the present case, the Respondent failed to carry out such shredding of the documents when disposing of these documents.

22 Additionally, Prudential had provided its agents and financial consultants designated "locked console boxes" for the secure shredding of unwanted documents. Prudential had informed its agents and financial consultants of this service and encouraging them to use it by way of a circular that was sent out on 12 January 2016.

23 The Respondent did not use this service for disposing of the policy documents at any point in time. Before leaving Prudential, Prudential had, as part of its standard practice, informed the Respondent to return the documents containing customer data to them, but the Respondent did not do so. When asked why he had not used the locked console boxes provided by Prudential, the Respondent mentioned that the locked console boxes were found in the main office of Prudential, and he was working at the branch office of Prudential. In other words, his excuse was that he seldom went over to the main office and thus it was inconvenient for him to make use of the locked console boxes. The Commissioner does not find this excuse to be acceptable, particularly since this could have been done as part of his end-of-contract administration.

24 Accordingly, the Respondent had available the means of securely disposing of the documents, ie by way of the locked console boxes, shredding or similar means, but he chose not to use such methods of disposal. Instead, he had carried out the disposal in an unsecured manner described above. It would appear that his choice not to use the locked console boxes as provided by

---

[1] See Paragraphs 7.3 to 7.5 of the PDPC's Guide to Disposal

Prudential was borne out of convenience. The fact that Prudential had provided such means of disposing of the documents should have given the Respondent an indication that such documents ought to at least be securely disposed by shredding. However, the Respondent did not adhere to such a standard of disposal of documents.

25 For the reasons above, the Commissioner finds that the Respondent failed to take reasonable security measures to protect the personal data in his possession and/or under his control and is in breach of Section 24 of the PDPA.

Enforcement Action by the Commissioner

26 In exercise of the power conferred upon the Commissioner pursuant to Section 29 of the PDPA, the Commissioner directs that a financial penalty of S$1,000 be imposed on the Organisation.

27 In assessing the breach and the directions to be imposed, the Commissioner took into account the following factors:

(a) the type of personal data contained in the 13 insurance certificates and 2 letters was sensitive data; and

(b) the documents were not disposed of in a high traffic area such as a busy street or a shopping mall.

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

SCHEDULE 1
FULL LIST OF PERSONAL DATA IN THE PRUDENTIAL FOLDERS

1. Name of policy-holder;

2. Client Number;

3. NRIC Number;

4. Age;

5. Date of Certificate;

6. Policy Number

7. Cover Start Date;

8. Maturity Date;

9. First Premium Due Date;

10. Premium Amount Payable;

11. Name of Life Assured (all the 13 certificates listed the names of respective policy-holders as the life assured);

12. Benefits

13. Sum assured;

14. Cover Start Date;

15. Cover Expiry Date;

16. Premium;

17. Last Premium Due.