DECISION OF THE PERSONAL DATA PROTECTION COMMISSION

Case Number: DP-1606-B0061

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

And

DataPost Pte Ltd (UEN 199404610D)

… Organisation

Decision Citation: [2017] SGPDPC 10

GROUNDS OF DECISION

20 June 2017

1. This case arises out of an investigation into DataPost Pte Ltd ("**DPL**"). DPL printed and mailed out financial statements relating to the Overseas-Chinese Banking Corporation Ltd's ("**OCBC**") Supplementary Retirement Scheme ("SRS") to OCBC's customers. One customer ("the recipient"), however, discovered that she had received two additional SRS statements belonging to two other OCBC customers, in addition to her own SRS statement. The following information was disclosed in the SRS statements:

    a. Name;

    b. Address;

    c. Cash balance; and

    d. Types, quantity, and valuation of asset holdings.

2. OCBC alerted the Commission to the incident, and informed the Commission that the recipient had received the additional SRS statements on or about 17 June 2016. The Commission has conducted an investigation into the matter and now sets out its findings.

A. MATERIAL FACTS AND DOCUMENTS

3. DPL's procedure for printing and mailing of the SRS statements was as follows:

   a. The SRS statements are printed on A3 sheets in the format shown below. A sheet may contain either two different statements or two pages of the same statement. In the incident in question, the first sheet, Sheet 1, contained the statements of two different individuals. Sheet 2 also contained the statements of two different individuals.

   A3 size Sheet 1

Statement of Individual 1	Statement of Individual 2

   A3 size Sheet 2

Statement of Individual 3	Statement of Individual 4

   b. An enveloping machine was used to cut the statements and to insert the individual statements into their respective mailer envelopes. For the purpose of this decision, there are two relevant sub-components of the enveloping machine which operations affect the eventual output of the enveloping machine. These are the cutter, which cuts the sheets of paper into A4 pages; and the Optical Mark Recognition ("OMR") reader that reads OMR markings (which are lines resembling barcodes) that are printed on each customer's statements. The OMR reader guides the enveloping machine to insert each customer's statements into the mailer envelope intended for that customer.

   c. The enveloping machine was operated by a single operator. The operator would start each printing run with a test run. If the test

run was successful, the operator would proceed with the printing and enveloping of the entire batch of statements.

d. The design of the machine was such that the first sheet, Sheet 1, had to be loaded directly into the cutter. However, the cutter was located further along in the machine than the OMR reader. Therefore, the first two statements cut from Sheet 1 would always be placed by the machine in the same envelope as the first statement of Sheet 2.

e. As a result of this operational peculiarity, the machine was set to automatically send the first envelope into the reject bin for manual intervention. The operator was supposed to sort out the individual statements in the reject bin by hand and put them into separate envelopes. He was then supposed to leave the sorted statements and envelopes in the reject bin for a quality control ("QC") check by a second level checker.

f. Having passed the second level check, a *third* check for QC was to be conducted by a supervisor. All three levels of checks were supposed to be recorded in a QC form.

g. Correctly filled envelopes were supposed to be deposited by the machine in the main bin. There is a digital counter in the main bin that records the number of envelopes deposited into it. The operator was supposed to record this number in the QC form together with the number of rejected envelopes. The number of "successful" and rejected envelopes, when added up, was supposed to tally with the total expected number of envelopes from the run.

4. The cause of the data breach in this case, according to DPL's internal investigations, was human error by the operator on duty on 4 May 2016. DPL's findings were that the operator manually checked the first envelope generated by the test run, but mistakenly concluded that the three statements contained therein all belonged to the same person. In fact, the statements belonged to three separate individuals, and had been placed in the same envelope due to the operating peculiarity described above.

5. The operator, in the mistaken belief that the three statements belonged to the same individual, removed the envelope from the reject bin and moved it to the main bin. Further, the operator completed the QC form in a way that showed that the number of "successful" and rejected

envelopes tallied with the expected total from the run. As the envelope was no longer in the reject bin, the second and third layers of checks were by-passed, and the envelope was sent out without anyone realising that it contained two extra statements. The manual completion of the QC form by the operator to show that the number of successful and rejected envelopes tallied allowed this to go undetected.

B. COMMISSION'S FINDINGS AND ASSESSMENT

(i) There was an unauthorised disclosure of personal data

6. The information disclosed in the two SRS statements is personal data within the meaning of section 2 of the PDPA. First, the names and addresses of the intended recipients of those two statements were included on the statements themselves. Hence, those individuals could be identified solely from the information disclosed by the statements. Further, the SRS financial information contained therein was clearly their personal data.

7. Given that the disclosure of such information contained was made without the consent of the intended recipients (i.e. the data subjects), and without any authority under the PDPA (or other written law), it was an unauthorised disclosure of personal data for the purposes of the PDPA.

(ii) DPL was a data intermediary and had the obligation to protect personal data under section 24 of the PDPA

8. In relation to the printing and mailing of the statements containing personal data, DPL was "processing" personal data under section 2 of the PDPA. As DPL was processing the personal data on behalf of OCBC, pursuant to their service agreement, DPL is a data intermediary within the meaning of section 2 of the PDPA: see also, *Central Depository (Pte) Limited and Toh-Shi Printing Singapore Pte Ltd* [2016] SGPDPC11 and *Aviva Ltd and Toh-Shi printing Singapore Pte Ltd* [2016] SGPDPC 15.

9. Hence, as provided under section 4(2) of the PDPA, DPL was under an obligation to make reasonable security arrangements to prevent the unauthorised disclosure of personal data under section 24 of the PDPA in respect of the personal data that DPL was processing for OCBC.

(iii) The unauthorised disclosure was the result of a breach of DPL's obligation to make reasonable arrangements for the protection of personal data

10. DPL claims that the unauthorised disclosure was the result of a single instance of human error. DPL provided a written data protection policy to the Commission. This policy states that envelopes in the reject bin should be treated with extra care, and that it was mandatory for such rejected envelopes to be subjected to second and third level checks. Taken together with the steps outlined above, DPL did have in place data protection policies and processes.

11. However, the Commission is of the view that the processes that DPL put in place did not meet the reasonable standards expected of it. There were two main issues in DPL's processes:

    a. It created a significant risk of the first envelope containing the statements of more than one individual (which may subsequently lead to an unauthorised disclosure of personal data); and

    b. It placed too much reliance on the operator to ensure that the first batch of statements were correctly sorted out and separated into the different envelopes, before sending out. Pertinently, DPL's QC checks were over-reliant on the operator strictly adhering to DPL's procedures, and correctly performing each of his functions, in order for such checks to be triggered. A single failure by the operator to comply with the procedure, such as incorrectly filling up the QC form, could lead to the QC checks being by-passed.

12. Given that the first three statements of the print cycle would always be placed in a single envelope by the machine, there was a significant risk of every first envelope containing the statements of two or more individuals. This, in turn, created a risk of the individual's statement being disclosed to another individual. The design and operation of the enveloping machine ensured that this risk arose with each print cycle. In the Commission's view, such risks could be avoided, for example, simply by having Sheet 1 print out blank pages by default, instead of statements containing information of actual customers. That way, the two other statements (of the three statements) in the 1st envelope would be blank statements, and there would be a lower chance of an unauthorised disclosure of a statement to the wrong recipient.

13. It was because of such risks that there needed to be a proper way of checking and ensuring that any additional statements were removed from the envelope. This again was where DPL failed: DPL relied entirely on a single operator for the correction to be made, and it did not have a proper system of checks and supervision over the operator's actions.

14. First, DPL's system of QC checks was inadequate. The operator was able to by-pass both the second or third level checks, since the persons carrying out these checks were only checking envelopes found in the reject bin. The operator was able to remove the envelope from the reject bin and place it in the main bin. This resulted in there being no second or third level checks being carried out on the envelope in this case.

15. Second, there was no independent verification of the accuracy of the QC form filled in by the operator, which meant that the second and third level checkers would not have been aware of the fact that the operator had incorrectly moved an envelope from the reject bin to the main bin, as the numbers in the QC form appeared to tally with the expected total from the run. The second and third level checkers were essentially relying on the numbers provided by the operator in the QC form in order to ascertain whether an error or failure had occurred. Since there was no independent verification, the second and third level checkers could not ascertain if those numbers provided by the operator were actually correct. Accordingly, depending on how the QC form was filled up, the second and third level checks could easily be by-passed just by the QC form showing, on the face of it, that the numbers in the reject bin and main bin had tallied with the expected total from the run. The lack of an independent verification of the QC form, and the manner in which the second and third level checkers could be circumvented from the incorrect filling up of the QC form, was a systemic weakness in DPL's QC process, and a failure to put in place adequate security arrangements to protect personal data.

16. Given the sensitivity of the personal data involved (financial statements), it was incumbent on DPL to ensure that its QC measures could not be so easily bypassed. The data breach could have been avoided if DPL had taken some simple additional precautions, for example:

    a. The second and third level checkers could have been obliged to check the digital counter, to ensure that the QC form filled in by the operator was accurate; and

    b. The operator could have been obliged to always return the first envelope filled by the machine to the reject bin which will ensure that it will be inspected by the second and third level checkers.

17. For the reasons above, the Commission finds that DPL had not put in adequate security arrangements to protect personal data. Accordingly, the Commission finds DPL in breach of section 24 of the PDPA.

C. ENFORCEMENT ACTION BY THE COMMISSION

18. Given that DPL breached its obligation under section 24 of the PDPA, the Commission is empowered under section 29(1) of the PDPA to issue such directions as it thinks fit in the circumstances.

19. The Commission finds that the personal data disclosed, being financial information, was sensitive in nature. This is a significant aggravating factor, warranting a financial penalty as a matter of general deterrence.

20. However, the Commission also notes the following mitigating factors:

    a. The scale of the breach was small. Only personal data belonging to two individuals was disclosed to a single recipient;

    b. There was no evidence to suggest that the data breach caused and actual loss or damage to any person.

21. The Commission has therefore decided to impose a financial penalty of S$3,000/- on DPL.

22. In addition, the Commission also directs DPL to:

    a. Conduct a review of its internal working procedure relating to data printing and enveloping operations, in particular to tighten the application of quality control checks;

    b. Improve the training of all operators and quality checkers involved in its printing and enveloping operations; and

    c. Review its personal data protection policy to determine if it needs to be updated to suit its current operations.

YEONG ZEE KIN
DEPUTY COMMISSIONER
PERSONAL DATA PROTECTION COMMISSION