DECISION OF THE PERSONAL DATA PROTECTION COMMISSION

Case Number: DP-1506-A456

CENTRAL DEPOSITORY (PTE) LIMITED (UEN. 198003912M)

... 1st Respondent

TOH-SHI PRINTING SINGAPORE PTE LTD (UEN. 198704013N)

... 2nd Respondent

Decision Citation: [2016] SGPDPC 11

GROUNDS OF DECISION

21 July 2016

A. BACKGROUND

1. On 11 June 2015, the Central Depository Pte Limited ("**CDP**"), reported to the Personal Data Protection Commission ("**Commission**") of an incident of a data breach involving its customers' personal data. It was reported that six CDP account holders had received CDP account ("**CDP account**") statements for the month of May 2015 containing account information of other account holders. On the same day, Singapore Exchange Limited ("**SGX**") issued a news release to inform and apologise for the incident.

2. Following the reporting of the incident, the Commission undertook an investigation into the matter. The Commission had determined that the two respondents in the matter were CDP and Toh-Shi Printing Singapore Pte Ltd ("**Toh-Shi**") respectively. The Commission's decision on the matter and grounds of decision are set out below.

B. MATERIAL FACTS AND DOCUMENTS

3. CDP is a wholly-owned subsidiary of SGX, and provides clearing, settlement and depository facilities in the Singapore securities market. Toh-Shi is the external vendor of CDP in charge of printing the CDP account statements for CDP.

4. The printing services provided by Toh-Shi are governed by a contract between parties dated 1 March 2013 (the Document Management Service Agreement ("**DMSA**")). The DMSA required, amongst other things, for Toh-Shi to protect the confidentiality of the CDP account holders' personal data and to put in place the necessary measures to protect the data.

5. Following the discovery of the data breach and Toh-Shi alerting the Commission of the breach, on 15 June 2015, CDP reissued the corrected CDP statements for the month of May 2015 with an apology letter to the 195 affected account holders. On 17 June 2015, SGX started to contact the affected account holders to assist with any queries or concerns, and to give them an option to change their CDP account numbers. From what the Commission understands, none of the account holders requested to change their account numbers.

6. On 26 June 2015, SGX conducted its own internal investigation into the incident and provided the SGX Regulatory Breach Report to the Commission.

7. Based on the investigations that were carried out, SGX found that the data breach incident occurred due to a misalignment of the pages during the sorting process which led to errors in the compilation of multi-page CDP statements such that the first page of the statement of one account holder was compiled with the second and subsequent pages of another account holder. The erroneous pages were initially spotted and marked out by Toh-Shi's Print System Operator ("**PSO**"). He subsequently informed the Fan Fold Operator ("**FFO**") of the markings; who was to discard the erroneous statements and to replace them with the correct statements from the printed roll. However, the FFO had mistakenly discarded the correct statements and despatched the erroneous statements for postage instead. This led to the erroneous statements being mailed to the account holders.

8. According to SGX's own internal investigation, 92 out of the 195 affected CDP account holders had received the second page belonging to another account holder containing one or more of the following information:

   (a) account information (i.e. name, address and account number);

   (b) securities holdings;

   (c) transaction summary; and/or

   (d) payment summary.

9. The remaining 103 affected CDP account holders received the second page containing account information of another account holder and general CDP information, with no details on securities holdings, transactions or payments.

C. COMMISSION FINDINGS AND BASIS FOR DETERMINATION

10. The issues in this case to be determined are as follow:

    (a) What obligations did CDP and Toh-Shi each owe under the Personal Data Protection Act 2012 ("**PDPA**") in respect of the personal data of the CDP account holders?

(b) Did CDP comply with its obligation under Section 24 of the PDPA in respect of the data breach incident that happened?

(c) Did Toh-Shi comply with its obligation under Section 24 of the PDPA in respect of the data breach incident that happened?

Relevant provisions under the PDPA

11. Section 24 of the PDPA provides 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.

12. Section 4(2) of the PDPA provides that Parts III to VI (except for Section 24 of the PDPA (protection of personal data) and Section 25 of the PDPA (retention of personal data)) shall not impose any obligation on a data intermediary in respect of its processing of personal data on behalf of and for the purposes of another organisation pursuant to a contract which is evidenced or made in writing.

13. Section 4(3) of the PDPA provides that an organisation shall have the same obligation under the PDPA in respect of the personal data processed on its behalf and for its purposes by a data intermediary as if the personal data were processed by the organisation itself.

The relationship between CDP and Toh-Shi and their respective obligations under the PDPA

14. The Commission notes that Toh-Shi is responsible for printing the account statements of CDP's account holders (containing their personal data) for CDP. This involves CDP providing to Toh-Shi personal particulars and stock holdings of account holders and statement document templates. Toh-Shi has to manage the entire process of merging account statement data with the correct statement document template and printing the final account statement. In this regard, Toh-Shi was carrying out activities of "processing" the personal data on behalf of CDP, as defined by the PDPA. Accordingly, the Commission finds that Toh-Shi was acting as a data intermediary for CDP.

15. Pursuant to Section 4(2) and 4(3) of the PDPA, both CDP and Toh-Shi are obliged under Section 24 of the PDPA to ensure that there are reasonable security arrangements to protect the personal data of CDP's account holders.

16. The Commission now turns to its assessment of whether CDP and Toh-Shi have complied with their obligations under Section 24 of the PDPA respectively.

Whether CDP has complied with its obligations under Section 24 of the PDPA

17. Based on the Commission's investigation into the matter, it is satisfied that CDP had complied with its obligations under Section 24 of the PDPA. In particular, the Commission notes that CDP had in place an agreement obliging Toh-Shi to take

the necessary actions and precautionary measures to protect the CDP account holders' personal data during the printing process. On CDP's part, it was noted that CDP had in place processes for the secure transfer of personal data between CDP and Toh-Shi: CDP ensured that the files containing the CDP account holders' personal data were sent to Toh-Shi via a secured format, i.e. Secured File Transfer Protocol.

18. Accordingly, the Commission does not find CDP in breach of Section 24 of the PDPA.

Whether Toh-Shi has complied with its obligations under Section 24 of the PDPA

19. The Commission notes that the cause of the breach in this case was due to error(s) made by the staff of Toh-Shi during the printing process.

20. In the Commission's assessment, the breach occurred as a result of inadequate operational processes in place to ensure that the letters and personal data were sent to the correct recipient. The Commission notes that in this case the PSO had manually checked that the correct CDP statements were printed and in the event that there was any error, the PSO would mark out the erroneous ones and provide the FFO with both the erroneous and correct CDP statements for sorting. As only one person was involved in the sorting, it resulted in the FFO discarding the correct CDP statements instead of the erroneous one. In the Commission's view, the measures to sort manually by one person were insufficient given the nature of the personal data involved. The human error in this case could have been avoided by putting in place processes or technology solutions that can minimise human error.

21. The Commission notes that following the data breach incident, Toh-Shi had taken steps to improve on the security of the system by implementing (a) additional layers of checks by a Supervisor, Quality Controller and the Manager; (b) barcode system; and (iii) a technology solution to automate the reconciliation of the printed statements to prevent repeat of the incident. In the Commission's view, if there were a better system of checks in place, the data breach incident could have been prevented.

D. ENFORCEMENT ACTION TAKEN AGAINST TOH-SHI

22. Given the above, the Commission finds that CDP is not in breach of Section 24 of the PDPA. However, the Commission finds that Toh-Shi is in breach of Section 24 of the PDPA.

23. In exercise of the power conferred upon the Commission pursuant to Section 29 of the PDPA, the Commission directs that a financial penalty of $5,000 to be meted out against Toh-Shi.

24. In coming to the direction to be given, the Commission has taken into the overall circumstances of the matter, namely:

(a) A considerable number of individuals (totalling 195) were affected by the data breach.

(b) Sensitive financial personal data was involved.

(c) The data breach incident could have been avoided if Toh-Shi had put a better system of checks in place.

(d) Prompt notice was given to the Commission of the data breach incident and that Toh-Shi was cooperative during investigation.

(e) Toh-Shi took prompt remedial and preventive actions following the data breach incident.

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

YEONG ZEE KIN
COMMISSION MEMBER
PERSONAL DATA PROTECTION COMMISSION