DECISION OF THE PERSONAL DATA PROTECTION COMMISSION

Case Number: DP-1603-A661

AVIVA LTD (UEN No. 196900499K)

… 1st Respondent

TOH-SHI PRINTING SINGAPORE PTE LTD (UEN No. 198704013N)

… 2nd Respondent

Decision Citation: [2016] SGPDPC 15

GROUNDS OF DECISION

21 September 2016

A. BACKGROUND

1. On 9 March 2016, Aviva Ltd ("**Aviva**") reported to the Personal Data Protection Commission ("**Commission**") an incident involving the disclosure of the personal data belonging to 7,794 Aviva policyholders under the Aviva Public Officers Group Insurance Scheme ("**POGIS**"). It was reported that erroneous annual premium statements for the year 2015 had been sent out to the POGIS policyholders. The Monetary Authority of Singapore was also notified of this incident by Aviva on 10 March 2016.

2. On 10 June 2016, Aviva informed the Commission that while 7,794 POGIS policyholders received erroneous annual premium statements for the year 2015, the personal data of a total of 8,022 individuals, including the POGIS policyholders' dependants, were disclosed in the data breach incident.

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

B. MATERIAL FACTS AND DOCUMENTS

4. Aviva is an insurance company and the appointed insurer for the POGIS. Toh-Shi provides mail out services of all the correspondence for Aviva and data printing services for ad-hoc projects. The mail out and data printing services provided by Toh-Shi to Aviva are governed by a Service Agreement dated 20 December 2012 as amended by a letter from Aviva to Toh-Shi dated 24 April 2014 and an Addendum to the Service

Agreement dated 12 January 2016 (the "**Addendum**" and collectively, the "**Toh-Shi Service Agreement**").

5. The Toh-Shi Service Agreement provides that, among other things, Toh-Shi shall (i) comply with the Personal Data Protection Act 2012 ("**PDPA**") and all subsidiary legislation related thereto; and (ii) have in place an adequate security plan containing Toh-Shi's security policies, procedures and controls in respect of protecting the confidentiality and security of Aviva's information in connection with the provision of the Services.

6. During investigations, Aviva represented to the Commission that it has put in place the following security arrangements:

   (a) a Standard Operating Procedure ("**SOP**") whereby Toh-Shi provides sample cases to Aviva for verification and Aviva is required to sign-off on the sampled cases and give the go-ahead before Toh-Shi can commence printing the finalised documents;

   (b) annual inspections and review of Aviva's arrangement with Toh-Shi are conducted to ensure that Toh-Shi is adhering to its security procedures in handling data, such as data encryption to protect customer data, as well as conducting data sample checks to ensure data consistency and integrity; and

   (c) annual on-site inspections are conducted to verify Toh-Shi's information technology security and business protection measures, and business continuity and disaster recovery capabilities.

7. Similarly, Toh-Shi represented to the Commission that it has a Data Protection Notice (effective 2 July 2014), which sets out the various methods that Toh-Shi has in place to safeguard personal data, and that it has implemented the following security measures and processes:

   (a) Toh-Shi will send user acceptance testing ("**UAT**") samples to Aviva for Aviva's verification and will only send the processed data for printing after Aviva has verified and signed off on the Data Content Form;

   (b) Toh-Shi has quality control ("**QC**") processes in place and conducts sample checks ("**QC Sample Checks**") to ensure the accuracy of the data printed and that the documents printed match the approved UAT samples;

   (c) once the documents are printed, a printout from the mailing machine will record the actual number of letters inserted and this figure will be tallied against the IT report that records the total number of letters computed from the database; and

(d) printing is done in a secured room, with 24/7 CCTV recording. Toh-Shi's data printing supervisor will also observe the operators and ensure that they do not spend more than the required quick glance which may constitute the detailed reading of the printed data but rather, to ensure the correct positioning of the images and clarity.

8. On 8 March 2016, Toh-Shi sent out erroneous annual premium statements ("**Erroneous Statements**") to 7,794 of Aviva's POGIS policy holders ("**Affected POGIS Policyholders**"). The Erroneous Statements contained the following information of another POGIS policy holder ("**2nd Products**"):

(a) the name(s) of the other policy holder's dependant(s);

(b) the sum assured under the other policy holder's policy;

(c) the premium amount under the other policy holder's policy; and

(d) the type of coverage under the other policy holder's policy.

9. On the same day, Aviva informed Toh-Shi that 3 POGIS policyholders had received annual premium statements with 2nd Products that did not belong to them.

10. After the discovery of the data breach, on 10 March 2016, Aviva and Toh-Shi held a recovery management meeting.

11. On 11 March 2016, Toh-Shi reprinted and sent out the 7,794 corrected statements together with an apology letter prepared by Aviva and a S$50 shopping voucher to the Affected POGIS Policyholders. Aviva also gave the Affected POGIS Policyholders a waiver of 1 month's insurance premium as a token for the inconvenience caused.

12. According to the investigations carried out by Toh-Shi, it was found that the data breach incident had occurred due to an error in the sorting process before the printing of the annual premium statements.

13. In accordance with the usual practice, Aviva had sent the statement details in an Excel file to Toh-Shi for processing, which involved populating the relevant fields in the appropriate document templates. Thereafter, the UAT samples were provided to Aviva and Aviva verified and confirmed that the UAT samples were in order and Toh-Shi could proceed with the printing.

14. However, rather than proceed with the printing of the annual premium statements, Toh-Shi performed further processing by sorting the data according to postal code, overseas address and non-deliverable mail before printing. It did so in order to enjoy postage savings. Toh-Shi did not provide any UAT samples of the further sorted data to Aviva for its

verification and confirmation before printing the annual premium statements.

15. Toh-Shi's investigations revealed that the error which resulted in the data breach incident was caused by an incomplete selection of the policyholders' account information in the raw data when Toh-Shi sorted the data further. The annual premium statement can list up to two products depending on the policy that each policyholder is insured. However, due to the incomplete selection of the policyholders' account information by the individual(s) carrying out further sorting, information on the 2nd products were excluded and not sorted with the rest of the information which resulted in the information on the 2nd products being mismatched.

16. While Toh-Shi had conducted QC Sample Checks, Toh-Shi admitted that the QC Sample Checks failed to spot the error as the QC Sample Checks were verified against the erroneously sorted file instead of the source data from Aviva.

C. COMMISSION FINDINGS AND BASIS FOR DETERMINATION

17. The issues to be determined by the Commission are as follows:

    (a) what obligations did Aviva and Toh-Shi each owe under the Personal Data Protection Act 2012 ("**PDPA**") in respect of the personal data of the Affected POGIS Policyholders;

    (b) did Aviva comply with its obligation under Section 24 of the PDPA in respect of the data breach incident that happened; and

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

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

19. Under Section 2(1) of the PDPA, a "data intermediary" is an organisation which processes personal data on behalf of another organisation but does not include an employee of that organisation. Processing personal data on behalf of another organisation refers to the carrying out of any operation or set of operations in relation to the personal data and includes, but is not limited to, the organisation, adaptation or alternation; retrieval; and transmission of the said personal data.

20. Section 4(2) of the PDPA confers an obligation on the data intermediary to comply with the Protection Obligation and the obligation to cease to retain personal data under Sections 24 and 25 of the PDPA respectively.

21. Further, 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.

Relationship between Aviva and Toh-Shi and their obligations under the PDPA

22. Having considered the facts and representations made by Aviva and Toh-Shi, the Commission is satisfied that Toh-Shi was engaged to carry out activities of "processing" personal data on behalf of Aviva as defined in Section 2(1) of the PDPA and was therefore acting as a data intermediary of Aviva.

23. First, while Toh-Shi is not expressly identified as a data intermediary of Aviva in the Toh-Shi Service Agreement, the following extracts from the Toh-Shi Service Agreement show that Aviva had envisaged that Toh-Shi would engage in the "processing" of Aviva policyholder's personal data on its behalf:

    (i) "*[Toh-Shi] shall comply with the [PDPA] and all subsidiary legislation related thereto … with regard to* ***any and all personal data (as defined in the PDPA) that it collects and discloses to and/or receives from Aviva***" [Emphasis added.]: Clause 17.1 of the Toh-Shi Service Agreement as amended by the Addendum; and

    (ii) "*for any* ***personal data that it collects for or receives from Aviva****,* ***[Toh-Shi] shall only process/use such personal data solely for Aviva*** *and in accordance with the instructions/purposes of Aviva or as is necessary for Aviva to fulfil its obligations under the Data Protection Legislation and not disclose such personal data to any other party or insurer …*" [Emphasis added.]: Clause 17.2(c) of the Toh-Shi Service Agreement as amended by the Addendum.

24. Second, as noted at paragraph 13 above, Toh-Shi is responsible for (i) populating in the relevant fields in the appropriate document templates with the raw data received from Aviva, and (ii) printing, enveloping and dispatching by post of the finalised annual premium statements on behalf of Aviva.

25. Therefore, the Commission finds that Toh-Shi is a data intermediary of Aviva for the purposes of the PDPA. Pursuant to Section 4(2) and Section 4(3) of the PDPA, both Aviva and Toh-Shi have an obligation to make reasonable security arrangements to protect the personal data of the Aviva policyholders.

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

26. Based on the Commission's investigation into the matter, it is satisfied that Aviva has met its Protection Obligation under Section 24 of the PDPA as it has made reasonable security arrangements to protect the personal data in its possession or under its control.

27. As noted at paragraphs 6 and 7 above, the Toh-Shi Service Agreement required Toh-Shi to put in place adequate security policies, procedures and controls to protect the confidentiality and security of the Aviva policyholders. The Commission is also satisfied that Aviva has demonstrated that it has undertaken an appropriate level of due diligence to assure itself that its data intermediary, Toh-Shi, is capable of complying with the PDPA. Having done so, it was reasonable for Aviva to have expected Toh-Shi to take the necessary actions to protect the Affected POGIS Policyholders' personal data. Additionally, Aviva had no direct part to play in the actual breach itself, given that the data breach was mainly caused by Toh-Shi's staff failing to comply with its own security measures and procedures, as will be elaborated upon below.

28. Therefore, the Commission does not find Aviva to be in breach of Section 24 of the PDPA.

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

29. Having considered the facts and representations made by Toh-Shi and Aviva, the Commission is of the view that Toh-Shi had failed to make reasonable security measures to protect the personal data it processed on behalf of Aviva.

30. As stated at paragraph 7 above, the Commission notes that Toh-Shi did have in place some security arrangements and procedures to safeguard the personal data that Toh-Shi processes on behalf of Aviva.

31. However, despite the fact that Toh-Shi had implemented security arrangements and procedures, Toh-Shi does not dispute that the data breach incident occurred as a result of:

    (a) an error that occurred when Toh-Shi carried out further sorting of the data that had already been verified and confirmed by Aviva (viz sorting by postal code, overseas address and non-deliverable mails);

    (b) Toh-Shi's deviation from the SOP when it did not provide the UAT samples of the data that had undergone further sorting to Aviva for verification and confirmation before printing the finalised annual premium statements; and

(c) mistakes by the individual(s) conducting the QC Sample Checks in failing to verify the data that had undergone further sorting against the source data file provided by Aviva (but against the erroneously sorted file prepared by Toh-Shi).

32. Toh-Shi also represented that it has taken the following remedial steps following the data breach incident:

(a) remind and re-train its staff to be more vigilant in processing the customer's data;

(b) ensure that Toh-Shi staff follow the customer's SOPs including any new SOPs to enhance data processing and not deviate from it unless it has been approved by the customer; and

(c) remind Toh-Shi staff that all final products must be approved by the customer before mailing out and not to alter the data after Toh-Shi has obtained the customer's confirmation.

33. Notwithstanding the security measures and procedures implemented by Toh-Shi to protect the very sensitive financial data it processed on behalf of Aviva, the Commission notes that Toh-Shi itself admitted that the data breach incident was caused by errors that occurred because its staff had failed to comply with the company's own security measures and procedures.

34. In the Commission's view, the error in the further sorting process could have been avoided and the data breach incident could have been prevented if:

(a) Toh-Shi had provided samples to Aviva for further verification after sorting; and

(b) Toh-Shi had conducted its QC Sample Checks on the further sorted data against the original source data from Aviva.

35. As such, in view of all of the relevant facts and circumstances, the Commission is not satisfied that Toh-Shi has made reasonable security arrangements to prevent authorised access, collection, use, disclosure, copying, modification, disposal or similar risks in compliance with the Protection Obligation under Section 24 of the PDPA.

D. ENFORCEMENT ACTION TAKEN AGAINST TOH-SHI

36. Having completed its investigation and assessment of this matter, the Commission finds that Aviva 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.

37. In exercise of the power conferred upon the Commission pursuant to Section 29 of the PDPA, the Commission directs that a financial penalty of S$25,000 be imposed on Toh-Shi.

38. In assessing the breach and the directions to be imposed, the Commission took into account the following factors:

(a) a large number of individuals (totalling 8,022, including the Affected POGIS Policyholders' dependants whose personal data were disclosed in the data breach incident) were affected by the data breach;

(b) the personal data disclosed in the data breach, namely, the names of the policyholder's dependants or beneficiaries, the sum insured under the insurance policy, the premium amount and type of coverage, are of a sensitive nature, not merely from a financial perspective but can also be socially embarrassing;

(c) this is the second time in a short span of approximately one year that Toh-Shi has committed a breach of Section 24 of the PDPA and both of the data breach incidents involve similar fact patterns and causes:

(i) in Toh-Shi's first breach of Section 24 of the PDPA[1] in June 2015, erroneous account statements were sent to 195 Central Depository ("**CDP**") account holders ("**First Breach**"). The Commission found that the cause of the First Breach was due to errors made by Toh-Shi staff during the printing process, such as a misalignment of the pages during the sorting process which led to errors in the compilation of multi-page CDP statement. A financial penalty of S$5,000 was imposed on Toh-Shi in the First Breach; and

(ii) despite the fact that Toh-Shi had taken steps to improve on the security of its system following the First Breach, a similar error in the sorting process has recurred in the present case within a year of the First Breach, which suggests that there is still a weakness in Toh-Shi's internal work processes;

(d) the data breach could have been avoided if Toh-Shi had followed the established SOP. Since Toh-Shi had performed additional sorting, the QC Sample Checks ought to have been carried out again;

(e) prompt notice was given to the Commission of the data breach incident; and

[1] The Commission's decision against Central Depository (Pte) Limited and Toh-Shi Printing Singapore Pte Ltd [2016] SGPDPC 11.

(f) Toh-Shi was cooperative during the investigation and took prompt remedial and preventive actions.

39. 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.

LEONG KENG THAI
CHAIRMAN
PERSONAL DATA PROTECTION COMMISSION