PERSONAL DATA PROTECTION COMMISSION

[2019] SGPDPC 2

Case No DP-1702-B0537

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

And

AIG Asia Pacific Insurance Pte Ltd &
Toppan Forms (S) Pte Ltd

… *Organisations*

DECISION

AIG Asia Pacific Insurance Pte Ltd & Toppan Forms (S) Pte Ltd

[2019] SGPDPC 2

Yeong Zee Kin, Deputy Commissioner — Case No DP-1702-B0537

3 January 2019.

Background

1 Today's leading companies are approaching outsourcing in innovative ways to activate, create, integrate and amplify business value. Outsourcing is expected to see growth across all functions, particularly in IT, finance and human resource[1]. This will correspondingly result in an increase in the volume of data processing activities that is outsourced by organisations to data intermediaries.

2 It is, therefore, crucial that data intermediaries and the organisations that engage them understand their respective obligations and those of the other party in this data processing relationship. This matter aims to shed some light in this regard and addresses the following issues:

(a) whether a data intermediary may have control of the personal data that it processes on another organisation's behalf; and

---

[1] See Deloitte's 2016 Global Outsourcing Survey at https://www2.deloitte.com/content/dam/Deloitte/us/Documents/process-and-operations/us-cons-sdt-gos-exec-summary-2016.pdf

(b) if yes, in what circumstances would the data intermediary have such control and whether as a result of this; and

(c) what, if any, are the obligations that the engaging organisation continues to have where the data intermediary is in control of the personal data.

3 On 21 February 2017, AIG Asia Pacific Insurance Pte Ltd ("**AIG**") informed the Personal Data Protection Commission (the "**Commission**") regarding an incident with its printing vendor, Toppan Forms (S) Pte Ltd ("**Toppan**"). Toppan mailed out 87 policy renewal letters ("**Policy Renewal Letters**") addressed to the respective individual AIG policyholders ("**Affected Customers**") enclosing incorrect business reply envelopes (the "**Incident**"). The incorrectly enclosed business reply envelope was addressed to Tan Chong Credit Pte Ltd ("**Tan Chong Credit**") instead of AIG.[2]

4 The Commissioner makes the following findings:

(a) AIG did not breach section 24 of the Personal Data Protection Act 2012 ("**PDPA**"); and

(b) Toppan breached section 24 of the PDPA.

Material Facts

5 AIG is one of the leading general insurance companies in Singapore,.

6 The Incident occurred on or around 10 October 2016, and was discovered by AIG on 2 November 2016 when it contacted an Affected

---

[2] Tan Chong Credit is one of AIG's scheme partners.

Customer to invite him to renew his motor insurance policy. The Affected Customer informed AIG of the incorrectly inserted business reply envelope.

7 The Policy Renewal Letters sent to the Affected Customers enclosed 2 Motor Insurance Renewal Notices. The first notice was to be completed if the Customer wished to also extend the insurance to cover home protection besides the motor insurance. If the Affected Customer only wished to renew the motor insurance, the Customer would only complete the second notice. The Affected Customer was to then return either one of the completed notices to AIG. This could presumably be done either by inserting the completed notice in the enclosed business reply envelope or by way of fax as the Organisation's fax number was provided.

The Commissioner's Findings and Basis for Determination

8 The personal data in each renewal form comprised:

(a) The personal data printed on the first page of both Motor Insurance Renewal Notices which comprised of an Affected Customer's name, address, make of vehicle together with registration number, hire purchase company (if any), motor policy number, premium payable, excess as well as renewal and expiry dates (the "**Printed Personal Data**").

(b) In addition, customers were also required to fill in the second page of the relevant Motor Insurance Renewal Notice to update AIG of the customers' marital status, identification number or passport number, address, contact number etc. and input payment details such as credit card number, card holder's name, and card expiry date (collectively the "**In-filled Personal Data**").

Printed Personal Data and In-filled Personal Data are collectively referred to as "**Personal Data**" in this Decision.

9 It is not disputed that the Personal Data in the renewal forms constitutes "personal data" as defined in section 2(1) of the PDPA.

10 There is also no dispute that the PDPA applies to AIG and Toppan as they both fall within PDPA's definition of "organisation".

11 The issues to be determined by the Commissioner in this case are as follows:

(a) Whether Toppan was a data intermediary for AIG;

(b) Whether AIG had complied with its obligations under section 24 of the PDPA; and

(c) Whether Toppan had complied with its obligations under section 24 of the PDPA.

Toppan was a data intermediary

12 Toppan, pursuant to an agreement dated 1 March 2006 and supplemented by Addendum No. 1 dated 24 June 2014 (collectively the "**Agreement**"), agreed to provide printing, collation and delivery services for AIG. This would have included printing the Policy Renewal Letters and the Motor Insurance Renewal Notices which included the Printed Personal Data. To perform this work, Toppan would have had to record, hold and retrieve the Printed Personal Data, thereby processing personal data on behalf of AIG. Toppan would also have caused the Affected Customers to transmit the Personal

Data through the customers use of the business reply envelopes Toppan had enclosed with the Policy Renewal Letters to return the notices.

13 In the circumstances, the Commissioner finds that Toppan was engaged to carry out activities of "processing" personal data on behalf of AIG as defined in section 2(1) of the PDPA. Toppan was therefore acting as a data intermediary of AIG.

Elements of Section 24 under the PDPA

14 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.

15 The obligation to make reasonable security arrangements does not attach unless the organisation is in possession or control of personal data.

AIG and Toppan had possession of the Printed Personal Data

16 AIG was in possession of the Printed Personal Data. First, AIG had the Printed Personal Data of each of the Affected Customers on record as each of them had an existing relationship with AIG. Second, it was AIG who provided Toppan with the Printed Personal Data.

17 Toppan was in possession of the Printed Personal Data from the moment it received the data from AIG.

The meaning of "control" in the PDPA

18 While there is no definition of "control" in the PDPA, the meaning of control in the context of data protection is generally understood to cover the ability, right or authority to determine (i) the purposes for; and/or (ii) the manner in which, personal data is processed, collected, use or disclosed.[3]

19 The organisation which engages a data intermediary to process personal data on its behalf (in this case AIG) will always have overall control of the purposes for which, and manner in which, personal data is processed, collected, used or disclosed.

20 A data intermediary is unlikely to have control over the purposes for which personal data is processed, collected, used or disclosed. If a data intermediary has control over the purposes for the collection, use or disclosure of the personal data, it is likely to be processing personal data on its own behalf rather than on behalf of another organisation.

21 A data intermediary, however, may be in control over the manner in which personal data is processed, collected, used or disclosed from a practical perspective, especially where the data intermediary is in the best position to determine the specific manner in which the personal data is processed, collected used or disclosed and the organisation defers to the data intermediary on how best to process, collect, use or disclose the personal data because of the data intermediary's expertise in the processing of personal data.

---

[3] See *AIG Asia Pacific Insurance Pte Ltd* [2018] SGPDPC 8 at [18].

22 In the current business environment, where the outsourcing of data processing is increasingly prevalent and has led to a well-developed business process outsourcing industry, the reality is that these data intermediaries have specialised knowledge and skills and tools including in the area of data processing, that the organisations which engage them may not have. The fact is that organisations no longer engage data intermediaries just to bring costs down but increasingly because of their expertise and resources available in specific areas including in the handling personal data. In these circumstances, such data intermediaries are likely to be in the best position to advice or determine the manner in which personal data is processed, collected, used or disclosed and the relevant security measures to be implemented to protect personal data it is processing.

23 In addition, section 4(2) read together with section 24 of the PDPA supports the view that a data intermediary may be in control of personal data. Pursuant to section 4(2), data intermediaries are subject to section 24 of the PDPA, which obliges the data intermediary to "*protect personal data in its possession or under its control*…". A data intermediary may, therefore, be in possession of, and/or in control of, personal data.

24 This is consistent with the purpose of the PDPA in recognising both the protection of personal data and the need for organisations to collect, use and disclose personal data for legitimate purposes.[4] A data intermediary that has the relevant expertise, knowledge and/or tools in handling and protecting personal and has been trusted with determining the manner in which personal data is processed is in the best position to protect that personal data; even if the data

[4] Section 3 of the PDPA.

intermediary is not in possession of the personal data it ought to be responsible for the protection of such personal data.

AIG had control of the Personal Data as a whole

25 AIG was in control of the Personal Data as a whole, including the In-filled Personal Data. Similar to *AIG Asia Pacific Insurance Pte Ltd* [2018] SGPDPC 8,[5] in this case, AIG determined what personal data it required to provide its services and the purposes for which the Personal Data was processed, collected, used and disclosed. In particular, AIG was in a position to decide, and did in fact do so, that in order to provide a better experience for customers when renewing their policies, the Printed Personal Data was pre-filled in the opening section of the renewal form. With respect to the In-filled Personal Data, AIG was responsible for determining what personal data was required from its customers and the purposes for which the In-filled Personal Data was processed, collected, used and disclosed. Therefore, in so far as the Affected Customers were returning the completed notices with the Personal Data, such Personal Data was within AIG's control at the material time.

Toppan also had control of the Personal Data as a whole

26 Toppan indicates on its website www.toppanforms.com/eng/about_us.html that the Toppan Forms (Hong Kong) Group (of which Toppan is part of) "has been providing one-stop total information management solutions to help our clients find better ways to handle information asset."

---

[5] See [20] and [24]

27 In fact, Toppan touts its data management expertise in various places on its website stating that

> *"Data Management Services at Toppan Forms is* ***a high security business process outsourcing service specialising in data handling****. ISO 9001:2008 Quality Management Certification and ISO 27001:2005 Information Security Management Systems Certification guarantee that our operations are up to certified international standards. We help you maximize the value of data asset* ***while minimizing handling cost and data leakage risk****.*
>
> *We provide a wide range of data management services from data print and business mailing service to document digitization."(emphasis added)*

28 It is clear from the above that Toppan does not see itself merely as a vendor that prints forms and mails them out but rather a specialised business process outsource service with the value proposition that it not just prints forms but ensure data security. This is consistent with clause 3.3 of Addendum No. 1 dated 24 June 2014, which is part of the Agreement, where in Toppan:

> "*represents and warrants to AIG that it has and will continue to have* ***industry best practice administrative, technical, and physical safeguards*** *in place to ensure the security and confidentiality and protect against the unauthorised or accidental destruction, loss, alternation (sic), use or disclosure of Client Data and other records and Information of AIG's customers or employees, to protect against anticipated threats or hazards to the integrity of such information and records." (emphasis added)*

29 Client Data is defined in the Addendum to mean "*any "personal data" as defined under the Personal Data Protection Act 2012 (Act 26 of 2012), all subsidiary legislation, guidelines, and notices as amended or issued thereunder from time to time"*.

30 Toppan is no ordinary form printing and mailing vendor and instead recognises itself as having expertise in the area of data protection and data security in relation to its form printing and mailing outsourcing services.

31 As explained above, such organisations are likely to have control over the means in which personal data is processed, collected, used or disclosed. In this regard, the investigations revealed that Toppan had control over the systems, processes and practices implemented to process the Personal Data in the notices from the time of receipt of the notices from AIG, to the enveloping of the Policy Renewal Letters, to the mailing out of these letters, and up to the onward transmission of the notices by AIG's customers by way of returning the notices in the business reply envelopes.

32 Toppan was solely responsible for its enveloping process during which business reply envelopes were enclosed with the Policy Renewal Letters, and was, therefore, in control of directing the manner and mode in which Affected Customers returned the completed renewal forms (and the Personal Data contained therein). These processes were not dictated by AIG and AIG did not have input in how these processes were drawn up.

33 Given the above, Toppan was, like AIG, also in control of the Personal Data as a whole. This is given Toppan's control over the manner in which the Personal Data was handled and the processes it put in place to print, envelope and mail out the Policy Renewal Letters comprising the Personal Data.

Whether AIG complied with its obligations under section 24 of the PDPA

34 AIG had the same obligation in respect of personal data processed on its behalf and for its purposes by Toppan as if the personal data were processed by AIG itself.[6]

35 Based on the investigations, the Commissioner finds that AIG had complied with its obligations under section 24 of the PDPA.

36 In order to take into account obligations under the PDPA, AIG supplemented its agreement with Toppan dated 1 March 2006 with Addendum No. 1 dated 24 June 2014. Under Clause 3.2 of the Addendum, the covenants made by Toppan with respect to "Client Data"[7] included the following:

> (a) to inform itself regarding, and comply with, AIG's privacy policies and all applicable privacy laws, including the "Privacy Laws"[8];
>
> (b) to maintain adequate administrative, technical and physical safeguards to ensure the security and confidentiality of the "Client Data", protect against any anticipated threats or hazards to the security

---

6 See Section 4(3) of the PDPA.

7 Defined in the Addendum as "*any "personal data" as defined under the Personal Data Protection Act 2012 (Act 26 of 2012), all subsidiary legislation, guidelines, and notices as amended or issued thereunder from time to time and any information regarding AIG's (and/or its Affiliates) clients or prospective clients received by (Toppan) in connection with the performance of its obligations under the Agreement…"*.

8 Defined in the Addendum as "*any Singapore laws, rules or regulations relating to personal information or collection, use, storage, disclosure or transfer of personal information, including the Personal Data Protection Act 2012 (Act 26 of 2012), all subsidiary legislation, guidelines, and notices issued thereunder from time to time, as may be amended from time to time"*.

or integrity of the "Client Data", and protect against unauthorised access to, use of or disclosure of "Client Data".

37 The Incident, as will be explained below, was a result of a gap in Toppan's enveloping process where the necessary checks were not carried out and AIG had no part to play in the actual breach. While this does not automatically excuse AIG from a finding of a section 24 breach the Commissioner is of the view that it would not be reasonable to have required AIG to implement any further security arrangements given the circumstances in this case.

38 Toppan's standard operating procedure, which was updated in January 2017, set out the necessary checks that Toppan had put in place in respect of the printing, enveloping and mailing of the Policy Renewal Letters. This document, if followed, would have prevented the Incident. Of course, AIG could have audited Toppan's enveloping process in a "live" environment to confirm that the relevant checks in respect of ensuring the correct Business Reply Envelope was enclosed were being carried out. However, given Toppan's credibility and expertise in the area of Data Protection Management and data security and Toppan's contractual obligation to maintain industry best practices (as opposed to mere compliance with the PDPA) in implementing security arrangements, any requirement to audit such a seemingly minor part of Toppan's complete process would appear to amount to a requirement for AIG to micromanage its data intermediaries' activities. There may be circumstances where such micromanagement is required, but based on the facts here, this case is not one of those circumstances.

39 Given the circumstances, the Commissioner does not find AIG to be in breach of section 24 of the PDPA.

Whether Toppan complied with its obligations under section 24 of the PDPA

40 As AIG's data intermediary, Toppan had an obligation to put in place reasonable security arrangements to protect the Printed Personal Data and In-filled Personal Data which was in its possession and/or under its control.[9]

41 At the material time, Toppan's standard operating procedure for enveloping was as follows ("**Toppan's Enveloping Process**"):

(a) Step 1 – A supervisor checks for the use of correct stationery including the use of correct business reply envelopes, quantity of letters to be printed and the appearance of the print-out.

(b) Step 2 - The enveloping employee manually envelopes the printed letters according to a check list. The enveloping employee signs off as first checker after checking for correct page sequence and dirty or misaligned prints.

(c) Step 3 - The supervisor conducts a quality control check by ensuring addressee's name and address are visible in the envelope window and that the number of letters enveloped tallies with the checklist. The envelope content is not checked. The supervisor signs off as second checker.

(d) Step 4 - A manager does a sampling check on content. The manager must check content of the first 5, the last 5 and another 5 randomly chosen envelopes. The manager then signs off.

---

[9] See Section 4(2) of the PDPA

(e) Step 5 - The packing employee tallies the number of envelopes with the checklist before sealing and sending the envelopes for mailing.

42 The investigations found that Toppan's enveloping employee inserted the incorrect business reply envelope because it looked similar to the correct reply envelope and failed to submit the unsealed envelopes for the supervisor and manager to conduct their respective checks. Also, Toppan's staff who packed the envelopes for mailing did not check for signatures of the supervisor and manager before sealing and mailing the enveloped Policy Renewal Letters.

43 Toppan's Enveloping Process fell far short of the standard protection required for the processing of the Personal Data, and amounted to weak internal work process controls:

(a) The enveloping employee was able to by-pass the relevant checks during the Enveloping Process undetected;

(b) No specific instruction was given to the enveloping employee to check that the correct business reply envelope is inserted; and

(c) The packing employee was not instructed to check for signatures of the supervisor and manager before sealing and mailing the enveloped Policy Renewal Letters.

44 Toppan was processing a significant volume of personal data on behalf of one of the leading general insurance companies in Singapore. It was therefore incumbent on Toppan to put in place reasonable security arrangements to protect this personal data. In this regard, Toppan was fully aware of its obligations, and had in fact made specific warranties to implement industry best

practice security arrangements with respect to its processing of Personal Data as discussed at [28] above.

45 The data breach could have been avoided if simple additional steps had been included in Toppan's Enveloping Process, for example:

(a) Toppan could have required notification to the assigned supervisor and manager before the start of each enveloping job. This would have made it less likely for their respective sampling checks to have been by-passed, as happened in the Incident;

(b) Toppan could have required its packers to have sight of the signatures of the supervisor and manager before sealing and mailing the enveloped Policy Renewal Letters; and

(c) As part of the job instructions for each enveloping job, Toppan could have required its employee to check that the correct business reply envelope is inserted.

46 For the reasons above, the Commissioner finds Toppan in breach of section 24 of the PDPA.

Remedial Action taken by Toppan

47 Toppan took the following remedial actions after it was notified of the Incident:

(a) The random sampling size for content checks was increased to 30%;

(b) The packers are required to inform the manager or supervisor if signatures of the relevant supervisor and manager are not on the accompanying checklist;

(c) The relevant supervisor and manager are required to track the number of enveloping jobs. They are also required to ensure all enveloping jobs are checked and signed off by them before the batch is sent to the packers;

(d) Employees are to be reminded during daily meetings and monthly Work Improvement Meetings to strictly follow the standard operating procedure for enveloping works; and

(e) A stern warning given to the employee responsible for the Incident.

The Commissioner's Directions

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

49 In assessing the breach and determining the directions, if any, to be imposed on Toppan in this case, the Commissioner also took into account the following mitigating factors:

(a) Toppan cooperated fully with the investigations;

(b) Toppan took prompt remedial action to prevent future breaches of a similar nature from recurring; and

(c) The impact of the data breach was limited. Only 1 Affected Customer used the incorrectly inserted business reply envelope.

50 Having considered all the relevant factors of this case, the Commissioner hereby directs Toppan to pay a financial penalty of S$5000.00 within 30 days from the date of the Commissioner's direction, failing which, interest at the rate specified in the Rules of Court[10] in respect of judgment debts, shall accrue and be payable on the outstanding amount of the financial penalty until the financial penalty is paid in full.

YEONG ZEE KIN
DEPUTY COMMISSIONER
FOR COMMISSIONER FOR PERSONAL DATA PROTECTION

---

[10] Cap 322, R5, 2014 Rev Ed.