PERSONAL DATA PROTECTION COMMISSION

[2019] SGPDPC 20

Case No DP-1801-B1530

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

And

AIA Singapore Private Limited

… *Organisation*

DECISION

AIA Singapore Private Limited

[2019] SGPDPC 20

Tan Kiat How, Commissioner — Case No DP-1801-B1530

20 June 2019

Background

1 On 5 January 2018, the Organisation notified the Personal Data Protection Commission (the "**Commission**") of the potential unauthorised disclosure (the "**Incident**") of individuals' personal data contained in 244 letters sent to two individuals due to an error with its letter generation system. In particular, 245 letters meant for various customers that the Organisation generated on 22 December 2017 and 27 December 2017 were sent to two customers as follows:

(a) 179 letters were sent to the first customer ("**Customer X**"), of which 178 letters were received by him (with one having gone missing in transit); and

(b) 66 letters were sent to, and received by, the second customer ("**Customer Y**"). Customer Y was the intended recipient of only one of these letters.

2 Following an investigation into the matter by the Commission, the Commissioner found the Organisation in breach of section 24 of Personal Data Protection Act 2012 ("**PDPA**") for the reasons set out below.

Material Facts

3 The Incident arose from an error in the Organisation's "Integral Life System" (the "**System**") which was used to automatically generate certain types of letters to its customers. The error was introduced into the System as a result of the Organisation deploying a software fix (the "**Fix**") on 21 December 2017 to rectify an earlier error (the "**First System Error**"). The First System Error resulted in the Organisation sending duplicate letters to customers who had provided the Organisation with only a foreign despatch address (ie they had not provided any local despatch address in Singapore).

4 Unfortunately, the Fix inadvertently introduced a logic error[1] which caused the System to extract and reflect the wrong local despatch addresses on the affected letters. This logic error manifested itself when the System generated "HealthShield Non-Integrated for Foreigners Policy" letters ("**Type A letter**") and letters which were not Type A letters ("**non-Type A letter**") in a batch; the local despatch address of the non-Type A letters generated immediately after a Type A letter incorrectly reflected the local despatch address of that Type A letter (the "**Error**"). A more detailed description of this Error is provided below:

(a) When the System generates Type A letters (ie Letters 1 and 2 in Table 1 below), the Type A letters accurately reflect the local and/or foreign despatch address of the intended recipients.

(b) If the System then generates non-Type A letters (ie Letters 3, 4 and 5 in Table 1) immediately after a Type A letter, the non-

[1] A logic error is a glitch in a computer programme that causes it to operate incorrectly and produce unintended output or other behaviour, but not to crash.

Type A letters *wrongly* reflect the local despatch address of the *recipient of the last Type A letter* (ie Letter 2 in Table 1), but accurately reflect their foreign despatch address (if any) (*eg* Letters 4 and 5 in Table 1).

(c) If the System generates Type A letters after a non-Type A letter (ie Letter 6 in Table 1), the Type A letters accurately reflect the local and/or foreign despatch address of the intended recipients.

5 Table 1 below illustrates the effects of the Error:

Table 1: Illustration of Error

Letter Number, in sequential order	**Letter Type**	**System Policy Record**		**Despatch Address generated in the letters**		**Outcome**
		Local Address	**Foreign Address**	**Local Address**	**Foreign Address**	
1	Type A	Tampines	-	Tampines	-	
2	Type A	Ang Mo Kio	India	Ang Mo Kio	India	
3	Non-Type A	Bedok	-	Ang Mo Kio	-	Letters 3 to 5 were sent to the local despatch address reflected in Letter 2 above.
4	Non-Type A	Ubi	USA	Ang Mo Kio	USA	
5	Non-Type A	-	Australia	Ang Mo Kio	Australia	
6	Type A	Eunos	-	Eunos	-	
7	Type A	East Coast	France	East Coast	France	
8	Type A	-	Vietnam	-	Vietnam	

6 In this case, the letters generated were therefore all addressed to their intended recipients but 179 letters reflected the local despatch address of Customer X and 66 letters reflected the local despatch address of Customer Y. This is because Customers X and Y were in the position of the recipient of the last Type A letter (*eg* Letter 2 in Table 1) before the batch of non-Type A letters were generated.

7 After the 245 letters were generated, they were converted into PDF format and sent to the Organisation's vendor, DataPost Pte Ltd ("**DataPost**"), for printing, enveloping and despatch. These letters comprised four Integrated Shield Plan premium notice reminder letters, 237 Integrated Shield Plan premium notice letters, three change of payor letters and one modified terms of coverage letter. These letters were sent to Customers X and Y between 28 December 2017 and 2 January 2018.

8 As a result of the Error, the following types of personal data for each category of letters were potentially compromised:

(a) in respect of the modified terms of coverage letters, and Integrated Shield Plan premium notice letters and premium notice reminder letters:

(i) the policyholder or insured person's full name;
(ii) the policyholder or insured person's policy number;
(iii) the policyholder or insured person's type and name of policy;
(iv) the policyholder or insured person's policy premium due date; and

(v) the policyholder or insured person's premium amount.

(b) in respect of the change of payor letters:

(i) the intended recipient's full name;
(ii) the intended recipient's policy number;
(iii) the intended recipient's type and name of policy;
(iv) the intended recipient's policy anniversary date;
(v) the insured person's full name, which differs from the intended recipient as the latter was paying the premiums on behalf of the insured; and
(vi) the intended recipient's premium amount.

9 On 30 December 2017, the Organisation learnt about the Incident from a social media post by Customer X and discovered the Error. It took the following remedial actions to mitigate the damage caused and to prevent the recurrence of similar incidents:

(a) immediately implemented a software fix to resolve the Error in the System;

(b) conducted and completed a scan of the System to check that all Singapore despatch addresses for letters sent to the Organisation's customers in 2017 were accurate;

(c) implemented a function in the System to enable it to perform, and generate daily reports for the purposes of, the following:

(i) checking and validating that the despatch addresses printed on the automatically generated letters match the records of the intended recipients, as found in the System's database; and

(ii) flagging out non-conforming cases to automatically stop such letters from being transmitted to DataPost for printing;

(d) took steps to retrieve the 244 letters which were sent to the wrong addresses and successfully retrieved 243 unopened letters. One letter was never received by Customer X and was determined to have been lost in transit; and

(e) printed and re-sent the affected letters to the customers concerned and extended their deadline to respond to the matters contained therein.

Findings and Basis for Determination

10 The main issue for determination is whether the Organisation breached section 24 of the PDPA. Section 24 of the PDPA requires an organisation to protect personal data in its possession or under its control by taking reasonable security steps or arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks.

11 As a preliminary point, the Organisation had engaged DataPost to assist with the printing, enveloping and despatch of the letters on the Organisation's behalf. According to the agreement between the Organisation and DataPost, and

as admitted by the Organisation in its responses to the Commission's queries, the scope of DataPost's engagement did not include checking the substantive contents of the letters it printed, enveloped and despatched on behalf of the Organisation; DataPost was only required to conduct sampling checks of the printouts in relation to the quality of presentation and alignment. Accordingly, the Incident did not relate to the scope of DataPost's engagement under its agreement with the Organisation.

12 Before examining the arrangements put in place by the Organisation, it should be noted that the personal data involved in this case includes insurance data, a category of personal data that is considered to be of a sensitive nature. It has been stated in previous decisions[2] that personal data of a sensitive nature should be safeguarded by a higher level of protection. To reiterate *Re Aviva Ltd* [2018] SGPDPC 4 at [17]:

> "All forms or categories of personal data are not equal; organisations need to take into account the sensitivity of the personal data that they handle. In this regard, the Commissioner repeats the explanation in *Re Aviva Ltd* [2017] (at [18]) on the higher standards of protection that should be implemented for sensitive personal data:
>
> > The Advisory Guidelines on Key Concepts in the PDPA states that an organisation should "implement robust policies and procedures for ensuring appropriate levels of security for personal data of varying levels of sensitivity". This means that ***a higher standard of protection is required for more sensitive personal data. More sensitive personal data, such as***

[2] See, for example, *Re AIG Asia Pacific Insurance Pte Ltd & Toppan Forms (S) Pte Ltd* [2019] SGPDPC 2, *Re NTUC Income Insurance Co-operative Ltd* [2018] SGPDPC 10, *Re AIG Asia Pacific Insurance Pte Ltd* [2018] SGPDPC 8, *Re Aviva Ltd* [2018] SGPDPC 4, and *Re Aviva Ltd* [2017] SGPDPC 14.

> ***insurance***, medical and financial data, ***should be accorded a commensurate level of protection.*** In addition, the Guide to Preventing Accidental Disclosure When Processing and Sending Personal Data expressly states that documents that contain sensitive personal data should be "processed and sent with particular care"."

[Emphasis added.]

13 In this case, in order to determine whether the Organisation was in breach of section 24, the relevant question is whether it had put in place reasonable security arrangements that would have prevented the Incident. It appears from the Commission's investigations that the Organisation had failed to:

(a) conduct sufficient testing before rolling out the Fix for the First System Error; and

(b) institute sufficient controls or checks to ensure the accuracy of the letters that the System automatically generated.

14 With respect to the failure set out above at paragraph 13(a), the tests which the Organisation conducted after developing the Fix were limited to ensuring that the First System Error was addressed (ie that duplicate letters were not sent to customers who had provided the Organisation with only a foreign despatch address). The scope of these tests was too narrow. Since changes were made to address how the System handled retrieval and insertion of local and foreign addresses, these tests should have been designed to ensure that the Fix did not affect other aspects of the System involving the same functionality.

15 Additionally, the tests were not conducted to mimic real world usage of the System. Firstly, the Organisation conducted its tests by generating one letter at a time. However, the System was ordinarily required to generate letters in batches which included both Type A and non-Type A letters, and the Error in fact only arose when the letters were generated in such batches. If the Organisation had tested the batch processing functionality using test data that approximated real world scenarios, the Error would have likely come to light at that stage.

16 Secondly, the Organisation used a set of test data that was severely flawed. The test data used a single address, 1 Robinson Road, as the local despatch address for all the letters that were generated. The Organisation claimed to have done this in order to prevent the disclosure of production data. There are proven ways to generate dummy or test data that reflects the distribution of the production data without resorting to using a single address, *eg* by swapping[3] the data. Further, this measure would also have prevented them from detecting the Error even if they had tested the generation of letters in batches.

17 With respect to the failure set out above at paragraph 13(b), the Organisation admitted that it did not have in place any process or personnel responsible for checking the contents of the automatically generated letters. The Guide to Preventing Accidental Disclosure When Processing and Sending Personal Data states the following in relation to the use of automated processes:

> "Ensure the accuracy and reliability of the automated processing

[3] The purpose of swapping is to rearrange data in the dataset such that the individual attribute values are still represented in the dataset, but generally, do not correspond to the original records. This technique is also referred to as shuffling and permutation. For more details, please refer to the Commission's Guide to Basic Data Anonymisation Techniques.

> implemented by checking these systems and processes regularly. ***When the data is more sensitive, consider incorporating additional checking mechanisms to cater for unexpected situations and ensure no error arises from the automated processing.***
>
> As good practice, ***establish procedures to include additional checks following the processing, printing and sorting of documents to ensure that the destination information*** (e.g. mailing address, email address or fax number) ***is correct and matches that of the intended recipient(s) prior to sending.***"
>
> [Emphasis added.]

18 Given the sensitive nature of the personal data involved, the Organisation ought to have instituted controls or checks to ensure the accuracy of the addressees of the letters. This is something that the Organisation has since implemented.

19 For the reasons above, the Commissioner found the Organisation in breach of section 24 of the PDPA.

The Commissioner's Directions

20 Having found that the Organisation is in breach of section 24 of the PDPA, the Commissioner is empowered under section 29 of the PDPA to issue the Organisation such directions as he deems fit to ensure compliance with the PDPA.

21 In assessing the breach and determining the directions, if any, to be imposed on the Organisation in this case, the following mitigating factors were taken into consideration:

(a) the Organisation voluntarily notified the Commission of the breach;

(b) the Organisation fully cooperated with the Commission's investigations;

(c) the Organisation took prompt action to mitigate the effects of the breach; and

(d) the Organisation managed to retrieve 243 letters unopened.

22 In consideration of the relevant facts and circumstances of the present case, the Commissioner directs the Organisation to pay a financial penalty of $10,000 within 30 days from the date of this direction, failing which interest, at the rate specified in the Rules of Court in respect of judgment debts, shall accrue and be payable on the outstanding amount of such financial penalty until the financial penalty is paid in full.

23 The Commissioner has not made any further directions for the Organisation given the remediation measures already put in place.

YEONG ZEE KIN
DEPUTY COMMISSIONER
FOR COMMISSIONER FOR PERSONAL DATA PROTECTION