Aviva Ltd

[2018] SGPDPC 4

Tan Kiat How, Commissioner— Case No DP-1706-B0860

Data Protection – Protection obligation – Disclosure of personal data – Insufficient administrative security arrangements

Data Protection – Personal data – Disclosure of financial and medical data – Stronger controls needed to protect sensitive personal data

19 April 2018

Background

1 The Organisation mistakenly sent out by post underwriting letters meant for 3 different clients (the "**Impacted Clients**") to another client (the "**Recipient Client**"). The facts of this matter are uncomplicated and the application of the law is straightforward. Of note, however, is that this incident is disappointingly similar to a prior incident involving the Organisation (see *Re Aviva Ltd* [2017] SGPDPC 14 ("***Re Aviva Ltd* [2017]**")), for which the Organisation was found to be in breach of section 24 of the Personal Data Protection Act ("**PDPA**") and fined $6,000.

Material Facts

2 The Organisation is a multinational insurance company that offers various types of insurance plans to its policyholders.

3 On 8 June 2017, the Monetary Authority of Singapore ("**MAS**") informed the Organisation that it had received a complaint on the unauthorised disclosure (the **"Incident**") as set out at paragraph 1 above. The Organisation was unaware of the Incident prior to the notification from MAS. The Organisation in turn notified the Personal Data Protection Commission ("**Commission**") on 15 June 2017. An investigation was carried out under section 50(1) of the PDPA in relation to a breach of section 24 of the PDPA.

4 The Incident occurred during the enveloping of underwriting letters issued through the Organisation's underwriting department (the "**Department**") to individual clients who signed up for group insurance policies. Staff in the Department print out underwriting letters to be issued to the Organisation's clients. Each staff will then place the relevant underwriting letter into the case file of each individual client and place the file onto a tray for an administrative staff to pick it up. The relevant administrative staff is to pick up the case files from the trays, remove the underwriting letter, fold it, and seal the underwriting letter in an envelope. The envelope is then placed in the mail basket to be delivered to a postal services company.

5 On the day of the Incident, 1 February 2017, the Department processed about 90 distinct underwriting letters. These underwriting letters were issued to individual clients who had requested for an increase in insurance coverage to update them on the status of their requests. The personal data disclosed in each underwriting letter included an individual's full name, residential address, medical conditions and the sum assured (the "**Personal Data**").

6 One of the administrative staff (the "**Admin Staff**") folded 4 underwriting letters, each of which were addressed to a unique individual client, at the same time. However, the Admin Staff forgot that the letters were meant

to be sent to different individuals and enclosed all 4 letters in a single envelope. As a result, the 4 underwriting letters were sent to the Recipient Client and the personal data of the 3 Impacted Clients were disclosed to the Recipient Client when the envelope was opened.

Findings and Assessment

Issue for determination

7 The issue to be determined is whether the Organisation had, pursuant to section 24 of the PDPA, put in place reasonable security arrangements to protect the Personal Data from unauthorised disclosure.

8 Section 24 requires an organisation to 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.

Whether the Organisation was in breach of section 24 of the PDPA

The Personal Data were disclosed without authorisation

9 It is not disputed that the Personal Data fell within the definition of "personal data" under section 2 of the PDPA as it was possible to identify the 3 Impacted Clients from that information alone.

10 It is also not in dispute that the Personal Data were disclosed mistakenly; the disclosure was therefore without authorisation.

11 Based on the investigations carried out, the Commissioner finds that the unauthorised disclosure of the Personal Data was a result of a breach of the

Organisation's obligation to make reasonable security arrangements for the protection of the Personal Data. The reasons for this finding are set out below.

The Organisation relied solely on the administrative staff to perform their duties diligently

12 Upon investigation, it was discovered that there were no processes or safeguards put in place to prevent the Incident. Just as in *Re Aviva Ltd* [2017], the Organisation merely relied on the administrative staff to perform their duties diligently.

13 Random checks on the enveloping carried out by the administrative staff were not conducted. This was despite the fact that a total of 4 permanent staff and 2 temporary staff were tasked to carry out the enveloping of such underwriting letters. It is surprising that none of the 4 permanent staff were tasked with a supervisory role to conduct random checks. In fact, the Organisation did not have in place any checks on the enveloping work of the administrative staff at any time prior to the dispatch of the letters to individual clients.

14 The Organisation did not even have a process to check if the number of letters sent out corresponded with the number of underwriting letters scheduled to be sent out on the day. This would have been the most basic check and would likely have prevented the Incident, but even this was not conducted. To be clear, it is unlikely that such a basic arrangement on its own would suffice for the purposes of complying with section 24; such an arrangement would still leave potential foreseeable errors (eg one of the pages of a letter being mistakenly included in an envelope to be sent to another individual) unaddressed. It would, however, have been better than nothing.

15 As it was made clear in *Re Aviva Ltd* [2017], relying solely on employees to perform their tasks diligently is not a sufficiently reasonable security arrangement and is a breach of the Organisation's obligation under section 24.

Personal data of a sensitive nature should be safeguarded by a higher level of protection

16 The personal data found in the underwriting letters included data of a sensitive nature such as financial and medical data (*Re Aviva Ltd* [2017] at [17]).

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 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".

The Organisation encountered a similar incident due to the lack of security arrangements surrounding its enveloping process but failed to take any heed from the prior incident

18 The Organisation's failure to implement any reasonable security arrangements in respect of the enveloping process here is perplexing given the occurrence of a previous incident (the "**Prior Incident**") suffered by the

Organisation and which, as mentioned above, is the subject of the decision in *Re Aviva Ltd* [2017].

19 In the Prior Incident, the Organisation had mistakenly mailed insurance documents which were meant for one policyholder to another policyholder. Just as in the present case, the Organisation relied solely on its administrative staff to perform their duties diligently and had not implemented any security arrangements to prevent the disclosure of personal data arising from the enveloping process.

20 As set out in *Re Aviva Ltd* [2017] (at [37]), the Organisation implemented the following checks as of 3 December 2016 within its processing department to mitigate against enveloping errors:

(a) a random check amounting to a sample size of about 10% would be conducted; and

(b) if an error is detected, the team leader would conduct a 100% audit of the work of the staff who had erred for a period of 1 week.

21 The investigations show that the above checks were not implemented across all departments within the Organisation. Notably, the Department involved in the present case (ie underwriting department) was not amongst those departments in which the above checks were implemented.

22 If the Organisation did not appreciate the fact that a lack of security arrangements in the enveloping process would potentially lead to an unauthorised disclosure of Personal Data before the occurrence of the Prior Incident, it should have become acutely aware of this potential after the Prior

Incident was reported or at least by the time it had concluded its internal investigations on 3 December 2016.

23 The Organisation had about 2 months (from 3 December 2016 to 1 February 2017, *ie* the time of the Incident) to implement some form of security arrangement to prevent the unauthorised disclosure of personal data arising out of mistakes in the enveloping process across its departments. This was, however, not done. In fact, even till as late as 8 June 2017, when MAS notified the Organisation of the Incident, no security arrangements were implemented to prevent such incidents. Clearly the checks which were implemented in respect of the Prior Incident were not complex and could have been rolled out to the rest of the departments within the Organisation which also handled enveloping in a short span of time. In fact, the Organisation had been able to implement some checks as security arrangements (as set out below at paragraphs 26(d) and 26(e) in respect of the enveloping of underwriting letters by 15 June 2017 (within 7 days after it became aware of the Incident).

24 Whether or not the checks (described below at paragraph 26), would have prevented the Incident from occurring is beside the point. What is egregious in this case is that the Organisation failed to put in place any security arrangements in the Department, as it was obliged to under the PDPA, to counter the potential of an unauthorised disclosure of personal data through mistakes in the enveloping process even though a similar incident involving an enveloping process within the Organisation had taken place about 2 months prior to the Incident. By 3 December 2016, the Organisation knew about the process gaps and the need for safeguards arising from its internal investigations into the Prior Incident. Even as it was implementing the recommended safeguards, the Organisation failed to conduct a more thorough review of its internal departments in order to identify more completely those departments that are

subject to the same vulnerabilities and risk similar failures as the Prior Incident. It cannot be gainsaid that the Organisation's failure to include the Department in its remedial plans arising from the Prior Incident contributed to the present incident.

25 To be clear, the Commissioner is not making a finding as to the suitability of the above checks as reasonable security arrangements for the work undertaken in the processing and underwriting departments. Neither is the Commissioner recommending that these checks be implemented throughout the Organisation.

Remediation Actions Taken by the Organisation

26 The Commissioner notes that after the data breach incident, the Organisation undertook the following remediation actions:

(a) the Recipient Client was contacted and the Organisation procured the return of the underwriting letters addressed to the Impacted Clients;

(b) the Impacted Clients were notified by the Organisation and were given shopping vouchers as a token of the Organisation's apology;

(c) the Organisation emphasised to the administrative staff the importance of checking that the envelopes do not contain letters addressed to multiple individuals;

(d) the Organisation implemented random sampling checks of 2 envelopes per day and if any enveloping error is detected, a 100% check will be conducted in respect of the enveloping work undertaken by the administrative staff who had erred for one week; and

(e) daily compulsory checks will be conducted to track the number of underwriting letters scheduled to be sent out each day and ensure that it is consistent with the number of envelopes containing these letters to be mailed.

27 As with the Prior Incident, the Commissioner has not reviewed the Organisation's considerations in deciding on the sample size for its random sampling checks and is not providing an opinion on the effectiveness of these random checks. The Commissioner, however, points out that with respect to the follow up letters which were the subject of the Prior Incident, a random check of 2 envelopes per day amounted to a sample size of about 10%. Here, given the quantity of underwriting letters the Organisation processed on the day of the Incident (*ie* 90 letters), the sample size amounts to about 2%.

28 In this regard, the Commissioner reiterates the observation he made in *Re Aviva Ltd* [2017] (at [40] - [41]):

> As a general observation, the Commissioner highlights that organisations should take into account all relevant circumstances and considerations when devising and implementing fresh or enhanced security arrangements in relation to the enveloping process to ensure compliance with section 24 of the PDPA. Such circumstances and considerations include the likelihood of unauthorised access, collection, use, disclosure, copying, modification or disposal of the Personal Data and similar risks in relation to the enveloping process; the sensitivity of the Personal Data and the impact to the individual if an unauthorised person obtained, modified or disposed of the Personal Data; the size of the organisation; and the amount of Personal Data that it is subject to the enveloping process.
>
> The Organisation may also wish to consider a graduated approach to sample checking. For example, the enveloping work of new members of staff and members of staff who have recently made mistakes may be subject to stringent checks while the work of senior members of staff with relatively few records of such mistakes may be subject to more moderate checks. It is not automatous checks that are of utmost importance but the efforts that an organisation puts into the development of

> considered SOPs which focus on the protection of personal data, which in turn contributes to the development of a positive data protection culture amongst its staff.

Directions

29 The Commissioner is empowered under section 29 of the PDPA to give the Organisation such directions as he deems fit to ensure the Organisation's compliance with the PDPA. This may include directing the Organisation to pay a financial penalty of such amount not exceeding S$1 million as the Commissioner thinks fit.

30 In assessing the breach and determining the directions to be imposed on the Organisation in this case, the Commissioner took into account the following aggravating factors:

(a) the Personal Data disclosed, in particular the medical condition and sum assured, were sensitive in nature;

(b) the Organisation is in the business of handling large volumes of personal data, the disclosure of which may cause exceptional damage, injury or hardship to the affected individuals; and

(c) the Organisation had encountered a similar incident prior to this Incident in which its lack of security arrangements surrounding the enveloping process resulted in the unauthorised disclosure of personal data of one of the Organisation's clients to another client due to a mistake by an employee of the Organisation during the enveloping process.

31 The Commissioner also took into account the following mitigating factors:

(a) the Organisation had cooperated fully with investigations and was forthcoming in admitting its mistake;

(b) the Organisation had notified the Impacted Clients of the data breach and offered them an apology and shopping vouchers, and had also made arrangements to retrieve the wrongly delivered documents from the Recipient Client;

(c) the unauthorised disclosure of Personal Data was limited to one individual; and

(d) there was no evidence to suggest that there had been any actual loss or damage resulting from the unauthorised disclosure.

32 Pursuant to section 29(2) of the PDPA, and the investigation and assessment of this matter having been completed, the Commissioner is satisfied that the Organisation did not make reasonable security arrangements to protect the Personal Data and is in breach of section 24 of the PDPA. Having carefully considered all the relevant factors of this case, the Commissioner hereby directs the Organisation to pay a financial penalty of S$30,000 within 30 days from the date of the directions, failing which interest shall be payable on the outstanding amount of such financial penalty.

Information Provided by the Organisation Subsequent to Receiving the Commissioner's Preliminary Decision

33 The Organisation by way of its letter dated 2 March 2018 provided the Commissioner with certain information subsequent to being informed of the Commissioner's preliminary decision that the Organisation was in breach of section 24 of the PDPA and the intention to impose the financial penalty as set out above at paragraph 32. The Commissioner reviewed the information in the

said letter and has maintained his views on the matter, his decision to impose a financial penalty, as well as the quantum of the financial penalty.

34 The information provided by the Organisation is summarised as follows:

(a) During the material period, there was a surge in the volume of underwriting letters as the Organisation had successfully bid for a large tender. Prior to the material period the Department had to process 40 letters per day; with the increased sales resulting from the successful bid, the Department had to process about 90 underwriting letters per day.

(b) The administrative staff was trained to carry out the staff's duties including training on the importance of handling personal data.

(c) the Organisation was in the process of implementing a barcoding system for their mail to minimise manual intervention.

(d) the Department was aware of the Prior Incident. According to the Organisation, every function (including the Department) across the Organisation handling personal data was advised to take note of the Prior Incident, assess their respective processes and consider implementing necessary controls to prevent similar occurrences with each function considering what practices or controls are appropriate for their processes.

(e) the Department assessed that the risk of unauthorised disclosure as a result of its processes and practices was low given that (i) the Department had not suffered such an incident prior to this; (ii) the staff had been sufficiently trained; (iii) there was verification of the clients' name against an underwriting worksheet before the letters were folded; and (iv) they would be implementing a barcoding system.

(f) reputational damage (if any) on the Impacted Clients would be minimal.

(g) the Organisation took steps to inform the Impacted Clients and apologised for the Incident.

(h) the unauthorised disclosure was limited to one individual.

35 The points summarised above provided an explanation of how the Organisation made its decision and the considerations that it undertook in its risk assessment. The Department made an assessment of the risks and decided not to implement the security measures introduced following the Prior Incident. Clearly, the risk materialised and the Organisation has to be responsible for its consequences.

36 The Organisation's representations concerning its plans to implement a barcode system for processing mail cannot excuse the adoption of the security measures introduced in other parts of the Organisation in the interim since it has continuing obligations to protect its clients' personal data. The future implementation of a barcode system does not address the protection measures that should have been put in place in the interim. It is precisely because of the risk of fluctuating — and in this case, a surge of — workload that interim adoption of the security measures, pending introduction of the barcode system, is necessary.

37 While the Commissioner accepts that personal data protection training which is specific to the administrative staff's role in handling personal data may in certain circumstances be a security measure, it does not detract from the necessity and relevance for operational safeguards in the form of the security measures introduced following the Prior Incident.

38 Pertinently, the Department verified the name of clients against an underwriting worksheet, but this verification was conducted prior to the folding and enveloping of the letters and was not designed to prevent situations similar to both the Incident and Prior Incident where letters were sent to the wrong recipient. More need not be said about the necessity for the Department to have adopted the security measures introduced following the Prior Incident even if to do so was an interim measure pending the implementation of a barcode system.

39 The points set out at paragraphs 34(f), (g) and (h) had been already taken into consideration in assessing the quantum of financial penalty to be imposed.

YEONG ZEE KIN
DEPUTY COMMISSIONER
FOR COMMISSIONER FOR PERSONAL DATA PROTECTION