Aviva Ltd

[2017] SGPDPC 14

Tan Kiat How, Commissioner— Case No DP-1611-B0323

Data Protection – Protection obligation – Access to personal data – Insufficient technical security arrangements

11 October 2017

Background

1 Can an organisation fulfil its obligation to protect personal data by relying solely on its employees to perform their duties diligently? That is ultimately the question which the Commissioner had to determine in this matter.

2 The complaint which arose in this matter was that Aviva Ltd ("the **Organisation**") had disclosed personal data without authorisation because it had mistakenly mailed to one of its policyholders (the "**First Policyholder**") insurance documents which were meant for another policyholder (the "**Second Policyholder**"). A family member of the First Policyholder lodged a complaint on 8 November 2016 and the office of the Commissioner proceeded to investigate the matter. The Commissioner's findings and the grounds of decision are set out below.

Material Facts

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

4 On 1 November 2016, the Organisation was alerted to the data breach (the "**Incident**") by a complaint from a family member of the First Policyholder. It undertook an internal investigation into the source of the data breach, which was traced to its Processing Department. By way of background, the Organisation's Processing Department is in charge of, amongst other things, preparing follow-up letters that need to be sent to the Organisation's policyholders. This is done whenever the Organisation requires further administrative details or personal particulars from the policyholders as part of administering its insurance policies. In the event that there are any additional documents to be sent to a specific policyholder, e.g. application forms or product summaries, staff (the "**processing staff**") in the Processing Department would enclose the additional documents with the follow-up letter and place these in the same envelope. For each day of operation, there would be a total of four processing staff handling approximately 16 follow-up letters together with the enclosed additional documents.

5 The Organisation's investigations revealed that the Incident occurred when one of the processing staff erroneously enclosed the Second Policyholder's documents to follow-up letters addressed to the First Policyholder. This led to the First Policyholder receiving two envelopes from the Organisation. The first envelope ("**Envelope 1**") contained three documents; two documents were correctly addressed to the First Policyholder, but the third document was meant for the Second

Policyholder. The second envelope ("**Envelope 2**") contained two documents; the first document was correct but the second document was an application form meant for the Second Policyholder.

6 The table below lists the documents contained in Envelopes 1 and 2 along with a description of the corresponding personal data ("**Personal Data**") that was disclosed without authorisation.

	Type of Documents	**Personal Data Disclosed**
Envelope 1	1. First Policyholder's MyShield "Request for further requirement(s)" letter 2. First Policyholder's MyShield Application Form 3. Second Policyholder's MyShield "Request for further requirement(s)" letter	Second Policyholder: name, address, policy plan type Second Policyholder's dependant: full name
Envelope 2	1. First Policyholder's MyHealthPlus "Request for further requirement(s)" letter 2. Second Policyholder's MyShield Application Form	Second Policyholder: name, address, policy plan type, NRIC number, CPF account number, nationality, contact number, date of birth, gender, marital status, occupation, name of employer Second Policyholder's dependant: full name, ID type, FIN, nationality, date of birth, gender, marital status, relationship to Second Policyholder

7 The Organisation confirmed that at the time of the Incident, the team leader ("**Team Leader**") of the Processing Department did not perform any random checks on the work of the processing staff carrying out the enveloping process. In fact, the Organisation did not have in place any checks on the enveloping work of the processing staff at any time prior to the dispatch of the letters to policyholders.

8 Following its internal investigation, the Organisation revised its procedures for the enveloping process to include random checks by the Team Leader on any two of the envelopes processed during each day of operation.

Findings and Assessment

Issue for determination

9 The issue to be determined is whether the Organisation had, pursuant to section 24 of the Personal Data Protection Act 2012 ("**PDPA**"), put in place reasonable security arrangements to protect the Personal Data from unauthorised disclosure.

10 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 was disclosed without authorisation

11 It is not disputed that the information contained in Envelopes 1 and 2, which included details such as full name, NRIC number/FIN, CPF account number, nationality, contact number, date of birth, gender, marital status, occupation and name of employer, falls within the definition of "personal data" under section 2 of the PDPA as it was possible to identify the two individuals (i.e. the Second Policyholder and the Second Policyholder's dependant) from that information alone.

12 It is also not in dispute that the Personal Data of the Second Policyholder and the Second Policyholder's dependant contained in Envelopes 1 and 2 was disclosed mistakenly; the disclosure was therefore without authorisation. For completeness, the Commissioner notes that there was no unauthorised disclosure of the First Policyholder's personal data in the present case.

13 Based on the investigations carried out by the office of the Commissioner, 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.

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

14 The Commissioner assessed that the Personal Data of the Second Policyholder and the Second Policyholder's dependant in

Envelopes 1 and 2 contained sensitive personal data. As detailed in the table at paragraph 6, the following sensitive personal data had been inadvertently disclosed: the Second Policyholder's insurance details, NRIC number, CPF account number, and the name and FIN of the Second Policyholder's dependant.

15 Furthermore, investigations found that Sections G (Underwriting Options) and H (Full Medical Underwriting Only) of the Second Policyholder's MyShield Application Form could have included sensitive medical information provided by the applicant. According to the Organisation, its usual practice was to have the MyShield Application Form filled up, including Sections G and H. However, in the present case, these sections were left blank as the Organisation had not obtained the relevant information. Had Sections G and H been pre-filled, additional sensitive medical information would have been disclosed to the First Policyholder due to the Incident. This was fortuitous for the Organisation and the individuals concerned (i.e. the Second Policyholder and the Second Policyholder's dependant).

16 In addition, Section E (Payment Details) of the Second Policyholder's MyShield Application Form was also left blank. If this section had been pre-filled, further sensitive personal data such as the Second Policyholder's credit card details (credit card number and expiry date) could have also been disclosed to the First Policyholder.

17 Even though there is no special category for sensitive personal data in the PDPA, past decisions and advisory guidelines have highlighted that certain types of personal data would typically be more

sensitive in nature. These include: NRIC/Passport numbers;[1] personal data of a financial nature such as bank account details,[2] Central Depository account details, securities holdings, transaction and payment summaries;[3] names of the policyholder's dependants or beneficiaries, the sum insured under the insurance policy, the premium amount and type of coverage;[4] an individual's personal history involving drug use and infidelity;[5] sensitive medical conditions;[6] and personal data of minors.[7]

18 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*".[8] 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

---

1 *Re JP Pepperdine Group Pte. Ltd.* [2017] SGPDPC 2 at [22]; and *Re Singapore Telecommunications Limited and another* [2017] SGPDPC 4 at [26].

2 *Re AIA Singapore Private Limited* [2016] SGPDPC 10 at [19].

3 *Re Central Depository (Pte) Limited and another* [2016] SGPDPC 11 at [24].

4 *Re Aviva Ltd and another* [2016] SGPDPC 15 at [38].

5 *Re Executive Coach International Pte. Ltd.* [2017] SGPDPC 3 at [9].

6 PDPC, *Advisory Guidelines for the Healthcare Sector* (revised 28 March 2017) at [4.2].

7 PDPC, *Advisory Guidelines on the PDPA for Selected Topics* (revised 28 March 2017) at [8.12].

8 PDPC, *Advisory Guidelines on Key Concepts in the PDPA* (revised 27 July 2016) at [17.3].

(*cont'd on next page*)

expressly states that documents that contain sensitive personal data should be "*processed and sent with particular care*".[9] However, even though the Organisation's processing staff handles sensitive Personal Data of its policyholders in the course of their employment on a daily basis, the Organisation did not ensure that the sensitive Personal Data was accorded a high standard of protection, or that it was processed and mailed with particular care.

19 In adopting this view, the Commissioner agrees with the observations made by the Office of the Privacy Commissioner of Canada ("**OPC**") that organisations "*must protect personal information by implementing security safeguards appropriate to the sensitivity of the information*" and that "*more sensitive information should be safeguarded by a higher level of protection*".[10] On the facts, the OPC found that the insurance company which was the subject of the Report lost its policyholders' files containing sensitive personal data as the safeguards for the control and tracking of the insurance files at the time of the data breach incident were inadequate. The personal data leaked included: the individual's name; address; date of birth; height and weight; salary; signature; life insurance amounts (current coverage and requested coverage); medical information (including the information declared on a

---

9 PDPC, *Guide to Preventing Accidental Disclosure When Processing and Sending Personal Data* at [2.2], first bullet point, p. 5.

10 *PIPEDA Report of Findings #2014-003: Insurance company overhauls its security safeguards following privacy breach* <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2014/pipeda-2014-003/>, first and second bullet points in the "Lessons Learned" section at p. 2.

paramedical exam and the results of a medical test); and an underwriter's notes and decision on the application.

The unauthorised disclosure of the Personal Data was the result of the Organisation's failure to make reasonable security arrangements

20 The Organisation represented that the enveloping error committed by its processing staff was an "*isolated incident due to genuine oversight*". However, upon a review of the Organisation's policies and processes, it was discovered that the Incident occurred due to the Organisation's lack of security arrangements in relation to the mailing of follow-up letters to its policyholders. In particular, the Organisation's processing Standard Operating Procedures ("**SOPs**") were ineffective as a safeguard to protect the Personal Data; this was a systemic problem.

i. The Organisation's processing SOPs were ineffective as a safeguard

21 The Commissioner finds that the Organisation's enveloping process as disclosed in the processing SOPs at the time of the Incident did not incorporate reasonable security arrangements for the following reasons.

22 At the time of the Incident, each processing staff handling enveloping would check that he/she has enclosed the correct documents to the follow-up letters. No other staff would be responsible for further checks or ensuring that the correct documents had been enclosed with such letters before the envelopes were sealed and mailed out. When

made aware of any errors by a staff member, the Team Leader would conduct a complete audit on the enveloping output of the staff in question for a period of one week.

23 The Organisation's processing SOPs at the time of the Incident did not include any second-level checks by the Team Leader on any of the follow-up letters that were prepared by the processing staff. This meant that there was no oversight of the enveloping process nor any supervision of the actions of each processing staff. As a matter of fact, the processing staff in charge of preparing and printing the follow-up letters and enclosing the additional documents was the only person checking the contents of the envelopes before they were mailed out to the policyholders.

24 This failure by the Organisation to put in place effective SOPs for the enveloping process was specifically highlighted in the Guide to Preventing Accidental Disclosure When Processing and Sending Personal Data as follows:[11]

> "Organisations that process and send documents or communications containing personal data should ensure that they have policies and procedures in place to prevent the sending of the documents or communications to the wrong recipients.
>
> For example, organisations that prepare account statements (e.g. bank or insurance statements) to be mailed to individuals should take steps to ensure that the statements or the envelopes they are placed in, or the emails they are attached in, are not sent to the wrong

11 PDPC, *Guide to Preventing Accidental Disclosure When Processing and Sending Personal Data* at [1.1]-[1.2].

> recipients by using incorrect postal or email addresses; or enclosing the statement of another individual."
>
> [Emphasis added.]

25 The same guide recommended the establishment of procedures for an organisation's staff to perform, as a best practice, "additional checks" following the processing, printing and sorting of documents to ensure that the destination information matches that of the intended recipient prior to mailing,[12] and that the right document containing the personal data is sent.[13] To be clear, the Commissioner is not setting down any rule that mandates organisations to establish procedures to perform "additional checks" in all cases. While it is recommended as a best practice, organisations should determine and adopt the most reasonable and appropriate policies and procedures given their specific circumstances.

26 In this case, the Commissioner finds that the absence of a second layer of basic checks to ensure that the letters and the enclosed documents were correctly addressed and mailed to the right policyholder pointed to a systemic weakness in the Organisation's processing SOPs and constituted a failure on the part of the Organisation to put in place reasonable security arrangements to protect the Personal Data.

27 The processing SOPs were designed in such a way that the Organisation was entirely reliant on its processing staff to check that the follow-up letters had the correct documents enclosed. Although the

---

12 *Ibid*. at [2.1], second bullet point, p. 4.

13 *Ibid*. at [2.1], fifth bullet point, p. 4.

Organisation claimed that it provided the necessary training and coaching to its processing staff to ensure their proficiency in performing their duties, the high risk of sensitive personal data being disclosed without authorisation was wholly unmitigated and dependent on the infallibility and consistency of the processing staff performing the enveloping work. The fact that the Organisation considered this to be an adequate form of protection is of concern, given that the Organisation is a well-established multinational organisation in the insurance business which handles large amounts of sensitive client personal data on a daily basis.

28 The Commissioner finds that it is insufficient for the Organisation to solely depend on its employees to carry out their duties diligently as a type of safeguard against an unauthorised disclosure of personal data. As observed in *Re Furnituremart.sg* [2017] SGPDPC 7 at [21], it is "*not enough for the Organisation to simply rely on its staff and employees to carry out their duties correctly for the protection of personal data*". In that case, the organisation had represented that if its employees had carried out their job functions properly, by printing and sending the correct invoice to the correct recipient, there would not have been any data protection issue in the first place.[14] Such an argument was soundly rejected.

29 In the present case, investigations found that the processing staff in question had ten years of experience in enveloping work. The fact that this error was made by a highly experienced staff is telling. If a highly

14 *Re Furnituremart.sg* [2017] SGPDPC 7 at [20].

experienced staff made such a mistake, the probability of a less experienced staff committing a similar error is much higher. This adds further weight to the position that any SOPs or work process which solely relies on individual staff being infallible cannot constitute a reasonable security arrangement for the protection of personal data.

30 As such, the Commissioner is of the view that the Organisation failed to make reasonable security arrangements to protect the Personal Data having relied solely on the processing staff to diligently perform his/her functions to prevent the unauthorised disclosure of the Personal Data.

ii. The Organisation's data protection policy provided inadequate protection

31 For completeness, the Commissioner notes that at the material time, the Organisation had in place a general data protection policy ("**PDPA Compliance Policy**"). This was a high-level policy which listed out the nine data protection obligations in the PDPA and the responsibilities of employees. However, the PDPA Compliance Policy merely sets out some dos and don'ts concerning the protection obligation, examples of which follow:

> "Do continue to comply with the various information security policies and standards issued by Aviva.
>
> …
>
> Do not share / disclose individual's personal data to anyone, including other staff, unless it is relevant and necessary for their performance of the duties."

These dos and don'ts did not provide sufficient instructions or guidance for the processing staff concerning their specific duties.

32 Security arrangements may take various forms. Data protection policies and practices developed and implemented by an organisation in accordance with its obligations under section 12 of the PDPA are generally meant to increase awareness and ensure accountability of the organisation's obligations under the PDPA. However, in some cases, such policies may also serve as an administrative security measure to protect personal data.

33 Where a data protection policy is meant to serve as an administrative security measure to protect personal data, organisations should note the importance of providing employees with specific practical guidance on handling personal data in the course of their employment as set out in *Re Hazel Florist & Gifts Pte Ltd* [2017] SGPDPC 9 at [18]:

> "The Commission notes that the Organisation has in place a Data Protection Policy. The Data Protection Policy merely restates the Organisation's data protection obligations in very general terms. The Organisation's Data Protection Policy does not provide the Organisation's employees with specific practical guidance on how to handle personal data in their day-to-day work or how to comply with section 24 of the PDPA. The Commission is, therefore, of the view that the Organisation's Data Protection Policy does not constitute a "security arrangement" under section 24 of the PDPA…"

34 In the present case, the Organisation's PDPA Compliance Policy did not contain any mention of the preparation of the envelopes for the sending of follow-up letters to the Organisation's policyholders, nor any

reference to the checking or verification of the enclosed documents. Whilst there was some attempt to elaborate on the protection obligation through the provision of basic dos and don'ts, the PDPA Compliance Policy did not go further to provide practical guidance on how an employee could comply with section 24 of the PDPA in the course of his/her daily work. Due to this lack of specificity and detail, the Commissioner is not satisfied that the PDPA Compliance Policy constituted a reasonable security arrangement under section 24 of the PDPA.

Conclusion of the Commissioner's Findings

35 Considering the level of sensitivity of the personal data that the Organisation handled on a daily basis with regard to follow-up letters and the enclosed documents, the Organisation did not put in place reasonable security arrangements to protect the Personal Data. The absence of any second-level checks in the Organisation's processing SOPs at the material time and the lack of any other form of security arrangement to prevent the erroneous mailing of one policyholder's documents to another amounted to extremely weak internal work process controls and fell far short of the standard of protection required for such sensitive personal data.

36 In consideration of the above, the Commissioner is not satisfied with the Organisation's claim that the unauthorised disclosure was caused by an isolated, one-off case of human error. The Commissioner finds that the Organisation failed to make reasonable security arrangements to protect the Personal Data in its possession or under its control, in breach of section 24 of the PDPA.

Remediation Actions Taken by the Organisation

37 The Commissioner notes that after the data breach incident, the Organisation counselled the staff in question, carried out an audit on the staff's enveloping output for one week, and revised its SOPs to add an additional layer of checks by the Team Leader of the enveloping process. Pursuant to the revised SOPs, the Team Leader would, on each day of operation, randomly check two envelopes whenever there are documents to be enclosed to the follow-up letters to ensure that the personal data of its Policyholders and their dependants are not mistakenly sent to others. Also, the week-long audit by the Team Leader on the processing staff who makes a mistake has now been operationalised as part of the SOPs. The relevant portions from the revised SOPs (which took effect from 3 December 2016) are reproduced below for reference:

> "7. Verification of Data Creation and Processing
>
> Cases created in AS400 will be checked randomly by the respective team leaders.
>
> Each team leader will check 5 cases of data creation per day. The team leader will ensure that he/she checks at least a case for each team member. The cases checked will be updated in an excel spreadsheet in our common drive.
>
> Should there be new team member, his /her mentor will check his/her work thoroughly until he/she is able to deliver the work accurately. This process is independent from the existing staff verification.
>
> Each team leader will check 2 cases of enveloping randomly per day. If error is detected, the team leader will conduct 100% audit on the erred staff enveloping output for a period of one week. The cases checked will be

> updated in the excel spreadsheet in our common drive." [Emphasis added]

38 Given the estimated average work load of 16 follow-up letters per day, a random check of 2 envelopes amounts to a sample size of about 10%.

39 The Commissioner has not reviewed the Organisation's considerations in deciding on the sample size and is not making any opinion on the revised SOPs as it is unnecessary to do so for the purposes of making a breach finding against the Organisation.

40 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.

41 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.

42 With this in mind, it is advisable for the Organisation to monitor the effectiveness of its revised SOPs and to make further revisions as necessary.

43 For completeness, the Commissioner notes that the Organisation also sent an apology letter to the First Policyholder and retrieved the wrongly delivered documents. As for the Second Policyholder, the Organisation sent an apology letter along with shopping vouchers worth S$100.

Directions

44 The Commissioner is empowered under section 29 of the PDPA to give the Organisation such directions as it 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.

45 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 and mitigating factors:

(a) the Personal Data disclosed, especially the Second Policyholder's NRIC number; CPF account number; and the full name and FIN of the Second Policyholder's dependant, was 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;

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

(d) the Organisation had notified the affected victim, i.e. the Second Policyholder, of the data breach incident, and offered an apology and shopping vouchers, and had also made arrangements to retrieve the wrongly delivered documents from the First Policyholder;

(e) the unauthorised disclosure of Personal Data was limited to possibly three individuals, comprising of the First Policyholder and the First Policyholder's nuclear family; and

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

46 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 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$6,000 within 30 days from the date of the directions, failing which interest shall be payable on the outstanding amount of such financial penalty.

47 The Commissioner urges organisations to take the necessary action to ensure that they comply with their obligations under the PDPA. Appropriate enforcement action against non-compliant organisation(s) will be taken.
