NTUC Income Insurance Co-operative Ltd

[2018] SGPDPC 10

Tan Kiat How, Commissioner— Case No DP-1706-B0894

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

Data Protection – Powers of investigation – General duty on organisations to preserve evidence in an investigation – Commissioner may draw adverse inference against organisation that destroys or deletes relevant documents and records

Data Protection – Powers of investigation – Obligation to retain records relating to an investigation after investigation has been completed pursuant to section 50(4) of the PDPA

3 May 2018

Background

1 This matter deals with a flaw in the design of the Organisation's processes surrounding the printing of various types of letters resulting in the unauthorised disclosure of personal data of 214 of the Organisation's clients (the "**Impacted Clients**").

Material Facts

2 The Organisation is an insurance co-operative that offers various types of insurance plans to its policyholders.

3 On 21 June 2017, a customer (the "**Complainant**") of the Organisation lodged a complaint (the "**Complaint**") with the Personal Data Protection Commission ("**PDPC**") alleging that she received a duplex printed letter from the Organisation correctly addressed to her, but the reverse of which was a letter addressed to another client of the Organisation. Subsequently, on 30 June 2017, the Organisation submitted a voluntary notification of a breach of the Personal Data Protection Act 2012 (the "**PDPA**") which confirmed the Complainant's allegations and provided details surrounding the Complaint.

4 On 5 June 2017, the Organisation printed a batch of 426 letters that were sent out to its clients. These letters were no more than a page long. The vast majority of the 426 letters (the "**Policy Letters**") that the Organisation printed were letters reminding its clients to pay their insurance premium ("**Premium Reminder Letters**"). This batch of letters also included 6 letters ("**Policy Cancellation Letters**") informing the relevant clients of the termination of their insurance policies with the Organisation, and 32 letters recording the relevant clients' non-acceptance of the Organisation's offer of insurance coverage ("**Non-Take Up Letters**"). The personal data ("**Personal Data**") found in these letters are set out in the table below:

Policy Cancellation Letters	**Non-Take Up Letters**	**Premium Reminder Letters**
Name; Full residential address; Type of policy; Policy number; and Endorsement number.	Name; Full residential address; and Type of policy.	Name; Full residential address; Type of policy; Policy number; and Premium amount.

5 The Organisation was informed by some of its clients that, similar to the Complainant, they had each received a Policy Letter addressed to them the reverse of which was a letter addressed to another client (the **"Incident"**).

6 An investigation was carried out under section 50(1) of the PDPA in relation to a breach of section 24 of the PDPA.

The Organisation's process for printing the Policy Letters

7 The Organisation's process for printing the Policy Letters was largely automated. Policy Letters issued by the Organisation to be mailed to its clients would be sent to the system (the "**Printing System**"**)** used by the Organisation's print room operators. The computer files containing these Policy Letters were programmed, before the files were sent to the Printing System, to be printed either in simplex (ie printed on a single side of the paper) or duplex (ie printed on both sides of the paper) according to the type of letters to be printed. The print room operators would initiate the printing of the Policy Letters by releasing the files in the print queue.

8 On 5 June 2017, according to the Organisation one of the three printers in the print room was "overloaded". The Organisation uses the term "overloading" to describe the situation when too many files were automatically sent to one of the printers in the print room. This was a fairly common occurrence and there was a procedure to handle this overloading. The print room operator on duty would have to manually transfer the print files from one printer to another to ensure that the printing load was spread evenly across the three printers. The procedure for the manual transfer of print jobs was as follows:

(a) The print room operator was required to select the specific file to be transferred.

(b) The print room operator would then select the file name and choose the option "forward". A dialog box stating "enable queues" will appear.

(c) The print room operator would then select the particular printer available to receive the file for printing and type in '(dept)_simplex' or '(dept)_duplex' under 'queue name' in the dialog box.

9 As a matter of protocol, the print room operator is required to choose to print the file in the format it was originally sent to the Printing System when he undertakes the manual transfer of the print job from one printer to another. In other words, if a letter sent to the Printing System was to be printed in simplex format, then the print room operator should choose to print the letter in simplex.

10 However, on this occasion the print room operator had mistakenly chosen to print the letters in duplex instead of simplex format. This led to two different Policy Letters addressed to two different policyholders being printed on each sheet of paper that was printed during the print run.

Findings and Assessment

Issue for determination

11 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.

12 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

13 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 Impacted Clients from that information alone. It is also not in dispute that the Personal Data was disclosed mistakenly and without authorisation.

14 Based on the investigations carried out, the Commissioner found 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 did not implement any measures to prevent the Incident

15 According to the Organisation, the print room operator was required to conduct a visual check ("**visual check**") of 10% of printed letters for the quality of print and alignment. The print room operator was also required to reconcile (the "**Reconciliation**") the number of letters printed as shown on the electronic counter of the individual printers with the number of letters sent for printing as displayed on the Printing System. The quantity of the printouts would be recorded in a printout log book (the "**Log Book**"). No other checks or security arrangements were implemented with respect to the printing process to prevent the unauthorised disclosure of personal data.

16 The Commissioner was of the view that the visual check and Reconciliation were not designed to adequately address the protection of personal data.

17 Such checks were to be undertaken by the same print room operator who printed the letters. As has been traversed in other cases, it is not advisable for an organisation to rely on a member of its staff checking his own work to ensure that he has undertaken a task properly to meet the Organisation's protection obligation under section 24 of the PDPA: see *Re Aviva Ltd* [2017] SGPDPC 14 at [28]; *Re Furnituremart.sg* [2017] SGPDPC 7 at [20] - [21].

18 Further, these checks had little to do with protecting personal data. The visual check was a check to ensure that the print on the letters were legible and not faded or smudged and that the letter was correctly aligned such that words were not missing or cut off. The Organisation did not require the print room operator or any other staff to check that the information on both sides of duplex printed letters were meant for the same individual. There was also no requirement to check that Policy Letters were printed in the correct format, either simplex or duplex, as it was originally sent to the Printing System when a manual transfer of print jobs was undertaken.

19 The Reconciliation check would not catch an error in the choice of print format as the reconciliation was based on the number of letters which were sent to be printed against the number of pages printed as shown on the electronic counter of the printers. The number of pages printed would not change whether or not the letters were printed in the simplex or duplex format, it will merely show the number of pages printed in total. If 5 letters sent to the Printing System were printed, the electronic counter on the printer would show that 5 pages were printed, whether or not the letters were printed in the simplex or duplex format.

20 While investigations showed that a check was implemented at the enveloping stage, this check also did not address situations such as this Incident. At the enveloping stage, letters would be inserted into a mail insertion machine

for enveloping by one of the Organisation's mail insertion operators. The mail insertion operator was required to reconcile the number of sealed envelopes with the number of sheets of paper printed by the print room operator. If instead, the mail insertion operator was required to reconcile the number of sealed envelopes with the number of letters sent for printing, the Incident would likely have been prevented. As it stands, however, this final check also did not address situations such as this Incident.

21 Given that the Personal Data includes insurance data of the Complainant and other policyholders, the Commissioner would also highlight that information such as the type of insurance policy and insurance premium amounts have been determined in the past to be sensitive personal data: *Re Aviva Ltd & anor* [2016] SGPDPC 15 at [38(b)]. The Commissioner has in the past expressly stated his view that an Organisation should accord a higher standard of protection to sensitive personal data: *Re Aviva Ltd* [2017] SGPDPC 14 at [18] – [19]. In this case, the standard of protection provided was not even sufficient for non-sensitive personal data.

22 In the circumstances, taking the printing and enveloping process as a whole, the Commissioner finds that the Organisation did not implement reasonable security arrangements to prevent the unauthorised disclosure of the Personal Data.

Organisations are required to preserve documents and records relating to an investigation

23 Before moving on to the remediation action taken by the Organisation and to the directions in this matter, the Commissioner takes this opportunity to remind the Organisation and organisations in general about their duty to

preserve evidence, including but not limited to documents and records, in relation to an investigation by the PDPC.

24 This issue arises in this case because the Organisation was unable to provide copies of the Log Book when asked pursuant to the investigations powers set out in the Ninth Schedule of the PDPA; the Organisation alleged that the copies were destroyed, in line with the Organisation's three-month retention period for such records. Notably, the destruction of copies of the Log Book took place *after* the commencement of investigations.

25 The Commissioner does not look favourably on the destruction or deletion of potentially relevant documents and records and may impose tough sanctions on any organisation that is found to have destroyed or deleted such documents or records.

26 Analogous to the preservation of evidence in civil proceedings, the Commissioner will consider, in deciding on the necessary and appropriate sanctions to be imposed, amongst other things, whether the deletion or destruction of the documents or records was deliberate (which includes negligent or reckless conduct resulting in destruction) and to what extent did the deletion or destruction of the records or documents prejudice a fair investigation into a potential breach of the PDPA.[1] In summary, the approach of the Commission will be to first consider whether a fair investigation into a potential breach of the PDPA is possible. If investigations may still proceed, particularly in reliance on evidence that may still substantially be obtained from other sources, the Commission may draw adverse inferences against the organisation

---

[1] *K Solutions Pte Ltd v. National University of Singapore* [2009] 4 SLR(R) 254 at [125].

(*cont'd on next page*)

that failed to preserve and produce any piece of evidence to the effect that had the evidence been produced, it would have been adverse to its case (see section 116 of the Evidence Act (Cap. 97)).[2] Adverse inferences may also be drawn against a complainant if the evidence ought to have been preserved and produced by the complainant.

27 Another pertinent factor for consideration is whether the litigation or legal proceedings was anticipated or contemplated by the party that destroyed the document or record. In the case of *K Solutions Pte Ltd v. National University of Singapore* [2009] 4 SLR(R) 254, the appellants had anticipated litigation for some time before its action was filed, and had given instructions to its staff to back up the email in their accounts. The high court did not find it credible that all of the appellant's internal emails had been deleted without backup, and determined that the appellants had deliberately suppressed documents and had lied about it.[3] In contrast, the court in *Tan Chor Chuan v. Tan Yeow Hiang Kenneth* [2004] SGHC 259 dismissed the plaintiff's application for striking out as it did not find anything sinister in the defendant's explanation for the deletion of the email in question – it was the defendant's practice to delete emails from their computer systems regularly to free up memory space; the defendants saw no necessity to archive or keep copies of emails after the EGM; and litigation had not been anticipated at the time. The court determined that the deletion of the email was not an attempt to pervert the course of justice.[4] In *K Solutions*, the

---

2 Section 116 of the Evidence Act (Cap. 97) states: "The court may presume the existence of any fact which it thinks likely to have happened, regard being had to the common course of natural events, human conduct, and public and private business, in their relation to the facts of the particular case".

3 *K Solutions Pte Ltd v. National University of Singapore* [2009] 4 SLR(R) 254 at [131] – [137].

4 *Tan Chor Chuan v. Tan Yeow Hiang Kenneth* [2004] SGHC 259 at [24] – [25].

court exercised its discretion to dismiss the case brought by the party in default. Applying the same principles to investigations conducted by the Commission, the Commissioner may discontinue or refuse to conduct investigations under section 50(3)(e) of the PDPA.

28 The obligation to preserve evidence is taken further by section 50(4) of the PDPA, which imposes an obligation on organisations to retain records relating to an investigation, for one year or such longer period as directed, after the investigation has been completed. This ensures that evidence relevant to any possible application for reconsideration or appeal from an investigation remains available even after investigations are completed.

29 Given the foregoing, the Commissioner takes the view that organisations should have a detailed litigation hold policy in place to ensure that documents and records relating to an investigation or potential investigation of a breach of its obligations under the PDPA are preserved and not deleted, disposed of or destroyed. Organisations should also ensure that relevant procedures and practices are fully implemented to give effect to such a litigation hold policy.

30 In respect of the matter at hand, however, the Commissioner is of the view that the contents of the Log Book, which were meant to have recorded the Reconciliation check by the print room operator, were not required for the Commissioner to make a finding of breach of section 24 given the finding that the Reconciliation was not a security arrangement designed to prevent the Incident. As such, the Commissioner did not impose any sanctions against the Organisation for the failure to preserve copies of the relevant Log Book.

Remediation Actions Taken by the Organisation

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

(a) the manual transfer of print jobs may now only be activated by the supervisors of the print room operators. Once activated, the print room operators may undertake the manual transfer of print jobs under the oversight of the supervisors;

(b) both the print room operators and mail insertion operators are now required to check that the letters are printed in the correct format (ie either in the simplex or duplex formats) by comparing the files sent for printing in the Printing System with the printed letters before enveloping. The checks will be done on 20% of letters printed in a batch on a random basis where no manual transfer of print jobs is undertaken. Where a manual transfer is undertaken, the print room operator and the mail insertion operator are required to check all letters; and

(c) the above measures have been included in the Standard Operating Procedure ("**SOP**") for the print and mail room operations. A briefing was also held for the print and mail room operators to inform them of the changes in the SOP.

Directions

32 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.

33 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:

Aggravating factors

(a) the unauthorised disclosure was systemic in nature;

(b) the Personal Data included sensitive personal data. However, in this regard, the Commissioner took cognisance that the insurance data that was disclosed in this matter was less sensitive than personal data of the type disclosed in *Re Aviva Ltd & anor* [2016] SGPDPC 15 which included the names of beneficiaries and dependants and the sum insured;

Mitigating factors

(c) the Organisation had cooperated fully with investigations;

(d) the Organisation took prompt action to remedy the flaw in the process; and

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

34 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$10,000 within 30 days from the date of the directions, failing which interest shall be payable on the outstanding amount of such financial penalty.

YEONG ZEE KIN
DEPUTY COMMISSIONER
FOR COMMISSIONER FOR PERSONAL DATA PROTECTION
