PERSONAL DATA PROTECTION COMMISSION

[2018] SGPDPC 8

Case No DP-1707-B0901

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

And

AIG Asia Pacific Insurance Pte. Ltd.

… *Organisation*

DECISION

AIG Asia Pacific Insurance Pte. Ltd.

Tan Kiat How, Commissioner — Case No DP-1707-B0901

3 May 2018

Background

1 On 30 June 2017, the Personal Data Protection Commission (the "**Commission**") received a data breach notification from the Organisation, AIG Asia Pacific Insurance Pte. Ltd (the "**Organisation**" or "**AIG**"), informing the Commission that:

(a) the personal data of some of the Organisation's policyholders (for its Individual Personal Accident product) had been compromised and disclosed to an unauthorised party (the "**Unauthorised Disclosure**"); and

(b) the Unauthorised Disclosure had occurred because the Organisation had stipulated an incorrect facsimile number on the policy renewal notices issued to its policyholders, which had caused its policyholders to fax their renewal notices to a third party, Tokyu Hands Singapore Pte. Ltd. ("**Tokyu Hands**") instead of the Organisation.

2 On account of the notification made, the Commissioner commenced an investigation under section 50 of the Personal Data Protection Act 2012 (the "**PDPA**") to ascertain whether the Organisation had breached its obligations under the PDPA. The Commissioner's findings and decision are set out below.

Material Facts

3 The Organisation is a general insurance company, and among the largest general insurance companies in Singapore.

4 The Organisation implemented a new electronic policy administration system on 29 November 2016. This system was responsible for generating forms including for its Individual Personal Accident product. These forms included the quote application form, endorsement quote form, policy schedule, endorsement schedule and renewal notice.

5 The form which is the subject of the data breach notification is the renewal notice. The renewal notice is a form that is generated by the Organisation and sent to a policyholder to notify the policyholder on policy renewal and to facilitate the policyholder renewing his or her policy. The policyholder can renew his or her policy by endorsing the renewal notice and returning it to the Organisation.

6 The renewal notice generated by the Organisation contains personal data of the policyholder including the policyholder's name, address and policy details as well as, depending on the policy, personal data of the policyholder's family members (the "**Personal Data**"). The renewal notice also contains a section which allows policyholders to provide their updated personal data such as updated address, email address and/or telephone numbers to the Organisation as well as their payment details.

7 From 29 November 2016 (when the new system was implemented) and until 19 May 2017, an incorrect facsimile number was indicated on all the forms generated by the system for the Individual Personal Accident product, including the renewal notice. This incorrect facsimile number was provided by a member

of the Organisation's staff during the development of template forms for the system. This incorrect facsimile number was formerly in use by the Organisation prior to 11 March 2011 but is now in use by Tokyu Hands.

8 As a result of the incorrect facsimile number, policyholders who were sending and returning their renewal notices to the Organisation during this period by facsimile had their renewal notices sent to Tokyu Hands instead of the Organisation.

9 The incorrect facsimile number was (fortuitously) corrected when the Organisation conducted a standardisation exercise on its system to ensure that the same contact information was provided across the Organisation's different forms for different products. Even then, the Organisation did not realise that there had been an error in the facsimile previously provided. It was only on 29 May 2017 that the Organisation became aware of the error after receiving notice from Tokyu Hands that it had been receiving the renewal notices intended for the Organisation.

10 The Organisation informed the Commission that Tokyu Hands had received approximately 1 to 5 facsimiles weekly that were intended for the Organisation. In other words, for the period from 29 November 2016 to 29 May 2017, between 25 to 125 renewal notices intended for the Organisation could have been sent to Tokyu Hands. It also appears that the majority of these renewal notices had been sent by the Organisation's own agents (on behalf of its policyholders).

11 The renewal notice with the incorrect facsimile number had been in circulation for a period of six months. In this regard, even after the notices were corrected, Tokyu Hands continued to receive renewal notices intended for the

Organisation by facsimile, with 11 such notices received between 30 May 2017 and 25 July 2017. Such risk would of course reduce with the passage of time. In this regard, the Organisation had in its representations, by way of its letter of 5 April 2018, confirmed that any outstanding renewal notices have by now lapsed and, as such, it is unlikely that any further renewal notices would be faxed to the wrong number. Given the process put in place between the Organisation and Tokyu Hands to contain the breach, any possibility of further renewal notices being faxed to Tokyu Hands was not considered in determining the quantum of financial penalty to be imposed. Nonetheless, there was no reduction of the financial penalty on the basis of the Organisation's confirmation that that the renewal notices have since lapsed.

12 In addition to correcting the facsimile number, the Organisation has since taken additional steps to address the data breach and the impact on affected policyholders:

(a) the Organisation has sought and obtained confirmation from Tokyu Hands that it has either destroyed or returned to the Organisation, all renewal notices received by Tokyu Hands, and that no copies of such notices have been retained;

(b) the Organisation has made arrangements to contact Tokyu Hands on a bi-weekly basis, and to collect any renewal notices that may have been sent to Tokyu Hands;

(c) the Organisation had on 1 June 2017, communicated to all its producers and agents, the correct facsimile number to be used;

(d) the Organisation is (or will be) undertaking a thorough review of all other forms used in its system to ensure that the contact and facsimile numbers are correct; and

(e) the Organisation has taken steps to reverse any negative impact on the policies of policyholders who had sent their renewal notices to Tokyu Hands instead of the Organisation (e.g. lapsed policies due to late renewal submissions have been backdated and renewed).

13 The Organisation has also put in place measures to reduce the risks of a similar incident by:

(a) requiring its managers to verify the accuracy of contact information collated by its staff; and

(b) including in the user acceptance testing process for its systems, a step to confirm that documents sent using the contact details provided by the Organisation is received by the intended recipient.

Commissioner's Findings and Basis for Determination

Issues to be determined

14 An investigation was conducted into the unauthorised disclosure. The issue in the present case is whether the Organisation had breached section 24 of the PDPA in providing an erroneous facsimile number on the renewal notices to which policyholders were to fax the duly completed renewal notices, resulting in the notices (and the personal data contained therein) being sent to an unauthorised third party.

15 There is no question or dispute that the data in the renewal notice is "personal data" as defined under the PDPA. The data concerned comprised of names, addresses, policy details, payment details and contact details of policyholders. There is also no question or dispute that the PDPA applies to the Organisation as it falls within the PDPA's definition of "organisation".

The Organisation was in control or possession of the Personal Data

16 Taking the formulation of the elements of a breach of section 24 of the PDPA from *Re Hazel Florists & Gifts Pte Ltd* [2017] SGPDPC 9 at [8], the next question to be asked is whether the Personal Data is in possession or control of the Organisation such that the obligation to make reasonable security arrangements attaches in respect of the Personal Data.

17 The Organisation was in *possession* of the Personal Data for the following reasons. First, it had the Personal Data of each of the affected individuals on record as each of them had an existing relationship with the Organisation. Second, it generated the renewal notices with the Personal Data pre-filled such that the individual need only sign the renewal notice and return it by facsimile transmission. It is only where there had been changes to the Personal Data on record that the individual had to provide updated information.

18 The Organisation was also in *control* of the Personal Data. 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, used or disclosed.

19 In this regard, the Hong Kong Administrative Appeals Board, in the case of *Shi Tao v. The Privacy Commissioner for Personal Data* (Administrative

Appeal No. 16 of 2007), agreed with the view of the Hong Kong Privacy Commissioner for Personal Data that control "can either mean the physical act of collecting, holding, processing or using the personal data or it can mean the ability of determining the purpose for which or the manner in which the data are to be collected, held, processed or used". Further, the UK Information Commissioner's Office ("**ICO**"), in its guidance[1] on the difference between data controllers and data processors stated that "[t]he data controller determines the purposes for which and the manner in which personal data is processed. It can do this either on its own or jointly or in common with other organisations. This means that the data controller exercises overall control over the 'why' and the 'how' of a data processing activity".

20 It is clear that the Organisation which collected, processed and used the Personal Data for the purposes of providing its clients with insurance services was in control of the Personal Data. The Organisation determined what personal data it required to provide its services and the purposes for, and the manner in, which the Personal Data was collected, processed, used and disclosed. This is not in dispute. In particular, the Organisation was in a position to decide, and did in fact do so, that as a matter of providing a better experience to its customers when renewing their policies, it pre-filled the renewal notices with each customer's Personal Data on record. This clearly demonstrates the Organisation's control of the Personal Data.

---

1 U.K., ICO, Data controllers and data processors: what the difference is and what the governance implications are (6 May 2014) <https://ico.org.uk/media/for-organisations/documents/1546/data-controllers-and-data-processors-dp-guidance.pdf> at [15].

21 Given that AIG is an organisation within the definition of the PDPA and that it is in possession and control of the Personal Data, section 24 of the PDPA applies to it in respect of the Personal Data.

22 However, before assessing whether the Organisation had made reasonable security arrangements to protect the Personal Data, the Commissioner, for completeness, assessed whether the Organisation was in control of the payment details and updated contact details which were entered into the renewal notice by, or on behalf of, the individual policyholders after the renewal notices left the Organisation's actual possession.

23 In this regard, in *Re The Cellar Door Pte Ltd and another* [2016] SGPDPC 22, it was found that there is a distinction between the possession and control of personal data and that an organisation that does not possess personal data may still be in control of the personal data (albeit in that case, the personal data was processed by a data intermediary on behalf of the organisation).

24 In the present case, the Organisation designed the renewal notice, pre-filled in the forms with relevant data including the Personal Data and stipulated the fields in the renewal notice which the individual policyholders were supposed to fill up, including the payment details and the updated contact details. The Organisation also devised the process for which policyholders may renew their insurance policies by faxing the duly completed renewal notice to the facsimile number it provided. Therefore, the Organisation was solely responsible for determining the purposes for which the payment details and updated contact details were collected, processed and used and directing the manner and mode of transmitting the renewal notice (and the Personal Data contained therein). Therefore, insofar as the policyholders were transmitting the renewal notices (and their personal data) in accordance with the Organisation's

instructions, such Personal Data was within the Organisation's control at the material time (i.e. when the personal data was filled in and faxed to the erroneous facsimile number).

25 The Commissioner therefore finds that the Organisation was in possession and control of the Personal Data (including the payment details and the updated contact details where such data was filled in by policyholders) within the meaning of section 24 of the PDPA.

26 The final issue that remains is whether the Organisation had taken reasonable security arrangements to protect the Personal Data concerned, when the Personal Data was in the Organisation's possession and control.

Whether reasonable security arrangements taken by the Organisation

27 The fact that personal data had been disclosed to an unauthorised party by an error or flaw in an organisation's systems and processes does not automatically mean that the organisation is liable under section 24 of the PDPA for failing to take reasonable security arrangements to protect personal data.

28 For the purposes of section 24, the Commissioner has to consider what security arrangements (if any) an organisation had implemented to prevent such unauthorised disclosure, and whether those arrangements are reasonable.

29 In this case, the Organisation failed to stipulate the correct facsimile number to which the duly completed renewal notices were to be sent. Such a failure would necessarily (and did) result in the notices being sent and disclosed to an unauthorised third party to whom the incorrect facsimile number belongs. The issue is therefore whether the Organisation had taken reasonable

arrangements to prevent an unauthorised disclosure of the Personal Data through the stipulation of an incorrect facsimile number.

30 The investigations found that the Organisation did not have any security arrangements to prevent such unauthorised disclosure. In particular, the Organisation did not have any arrangement or process to verify the accuracy of facsimile numbers uploaded or in use by its systems (and in the forms generated by its system). The Organisation clarified in its representations that it relied on the facsimile numbers provided by the relevant departments within the Organisation when entering the numbers into the new system and verifying that the numbers keyed in matched the numbers provided by the relevant departments. There was, however, no check to verify that the facsimile numbers were up to date. When the system was developed and tested, the scope of the testing only involved a verification that the facsimile number in the template forms (which was then incorrect) corresponded with the forms generated by the system. Also, the user acceptance testing process did not provide for the tester to send a test fax to the facsimile number to verify that the document was received.

31 This failure to undertake any verification is particularly alarming given that the incorrect facsimile number had not been in use by the Organisation for over five years by the time it was uploaded into the system. The incorrect facsimile number was (fortuitously) corrected almost six months after the system was operative, without the Organisation realising that there had been an error. The Commissioner is of the view that merely verifying the facsimile numbers entered into the system against the facsimile numbers provided by the relevant departments was wholly insufficient as a security arrangement and did not warrant a reduction in the penalty imposed. In fact, had the foregoing verification also not been present, the Commissioner may have increased the

penalty imposed, as it would show a very grave lack of basic information security practices.

32 The Commissioner also takes the view that it is only reasonable for a company like the Organisation to have some arrangement to ensure that the contact details they provide for the purposes of receiving personal data are accurate. As a general insurer, the Organisation receives a large volume of documents containing personal data of its many existing and prospective policyholders. It is therefore incumbent on the Organisation to stipulate correct and updated contact details (and ensure that they have done so) to avoid the risk of such personal data being sent to an unauthorised third party instead (as in the present case).

33 One of the considerations that an organisation should factor into its information security arrangements is the monitoring of its systems and processes to detect potential data security breaches (such monitoring to detect data security breaches will be referred to as "**data security monitoring**"). In this regard, the Organisation intimated that it does monitor its renewal business but that its monitoring did not indicate any significant deviation. It is not clear whether the Organisation monitored the number of renewal notices it received by fax (which was the suggestion by the Commissioner) as opposed to the general renewal business (including renewals by other means and not just by way of facsimile). The monitoring of the general renewal business would not constitute data security monitoring; instead this is generally done for business reasons and any data security aspect would be incidental. However, the monitoring of the number of renewal notices received by facsimile, may constitute a data security monitoring measure. To be clear, such a data security monitoring measure would not have prevented the unauthorised disclosure or a finding of breach given the facts of this matter. Any such data security

monitoring measure would, nevertheless, be imperative in containing any unauthorised disclosure. The monitoring of the number of renewal notices received by facsimile would have been a very basic and relatively inexpensive form of data security monitoring and would have, likely, only provided sufficient feedback after a significant period. In the circumstances, and considering all the facts of this case and the Organisation's representations, the Commissioner is of the view that the penalty imposed in this case (set out at paragraph 38 below) is warranted and maintains his decision on the quantum of the penalty.

34 The Organisation has maintained that the data breach arose due to inadvertent human error. As it has been noted on a number of occasions (including in *Re Social Metric Pte Ltd* [2017] SGPDPC 17), inadvertent human error is not a valid reason for an organisation failing to comply with section 24 of the PDPA.

35 Accordingly, the Commissioner finds that the Organisation has breached section 24 of the PDPA.

The Commissioner's Directions

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

37 In assessing the breach and determining the directions to be imposed on the Organisation in this case, the Commissioner considered the following factors:

(a) the Organisation had initiated the data breach notification to the Commission and was cooperative in the investigations;

(b) the Organisation took prompt action (described in paragraphs 12 and 13 above) to mitigate the impact of the data breach and to prevent future breaches of a similar nature from occurring;

(c) the extent of the unauthorised disclosure was limited, and the disclosure was only to a single third party, Tokyu Hands (which has confirmed that it has destroyed or returned the renewal notices received). While the exact number of affected individuals cannot be determined and there remains a possibility that individuals continue to be affected, the Commissioner is satisfied that the Organisation has taken steps to minimise the impact to any affected individual.

38 In consideration of the factors above and the circumstances of the present case, pursuant to section 29(2) of the PDPA, the Commissioner hereby directs that the Organisation pay a financial penalty of S$9,000 within 30 days of the Commissioner's 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.

YEONG ZEE KIN
DEPUTY COMMISSIONER
FOR COMMISSIONER FOR PERSONAL DATA PROTECTION