DECISION OF THE PERSONAL DATA PROTECTION COMMISSION

Case Number: DP-1509-A533

AIA Singapore Private Limited (U.E.N. 201106386R)

... Respondent

Decision Citation: [2016] SGPDPC 10

GROUNDS OF DECISION

22 June 2016

A. BACKGROUND

1. On 18 September 2015, the Personal Data Protection Commission ("**Commission**") received a complaint from [Redacted] ("**Complainant**"), alleging that the Respondent had made an unauthorised disclosure of his personal data, in particular, his bank account details, to Chiropractic First CFG (TP) Pte Ltd ("**CFG**") in respect of the Complainant's claim under an insurance policy.

2. The Commission investigated into the alleged unauthorised disclosure made, and its findings are set out below.

B. MATERIAL FACTS AND DOCUMENTS

3. The Respondent is an insurance company. The Complainant holds an insurance policy with the Respondent. Previously, in signing up for the insurance policy with the Respondent, the Complainant provided information of himself in the application form ("**Application Form**"), including, his name, address, NRIC number, contact details, occupation and various other personal particulars ("**Personal Particulars**").

4. In the declaration portion of the Application Form, the Complainant agreed, amongst other things, to the Respondent: (a) releasing to any medical source or insurance office any relevant information concerning the Complainant at any time; and (b) using and/or disclosing any information to independent third parties with regard to any matters pertaining to the application/policy.

5. On 24 May 2015, the Complainant made a claim for insurance under the policy with the Respondent. In raising the claim, the Complainant had to fill in an Accident & Hospitalisation Claim Form ("**A&H Form**") to be submitted to the Respondent. In the A&H Form, the Complainant had to provide, amongst other

things, his policy details, his Personal Particulars, and his bank account information "*for direct crediting of claims*". For the bank account information, the Complainant provided the name of the bank, branch of the bank, the bank account number and the account holder's name ("**Bank Account Details**").

6. In the authorisation and declaration portion of the A&H Form, the Complainant had agreed, amongst other things, to the Respondent disclosing the personal data of the Complainant for purposes described in the "AIA Personal Data Policy".

7. The AIA Personal Data Policy ("**Policy**") produced by the Respondent sets out the following scope of consent:

   (a) The persons who may be provided with the insured's personal data. Specifically, it states that the Respondent may disclose personal data to "*medical sources and insurance organisations*".

   (b) The types of personal data that may be collected, used or disclosed, including the insured's "*personal particulars such as NRIC numbers, passport numbers, contact details, addresses, date of birth, occupation, photographs and marital status*" or "*your financial information such as income, bank account numbers, CPF statements, bank statements…*".

   (c) The purposes for which personal data may be collected, used or disclosed. In particular, it lists the purpose to "*assess, process, administer, implement and effect the requests or transactions*" or "*assessing, processing, settling, authenticating and investigating claims*".

8. Pursuant to the Complainant's claim, the Respondent had communicated with the Complainant's chiropractor, CFG, to obtain further medical information about the Complainant. In its communication, the Respondent disclosed pages 1 and 3 of the A&H Form to CFG, which disclosed, amongst other things, the Complainant's Bank Account Details.

9. According to the Respondent, there were a number of reasons why it was permitted or authorised to disclose the personal data of the Complainant to CFG. Briefly, the Respondent claimed that:

   (a) The Complainant had provided consent for his personal data to be disclosed to CFG, pursuant to, the A&H Form read with the AIA Personal Data Policy.

   (b) The disclosure was necessary to; (i) facilitate the speedy processing of the claim; (ii) assure CFG that the Respondent's request for disclosure is based on a claim from CFG's patient / the Respondent's policy holder, and (iii) assure CFG that all required consents had been obtained to allow CFG to respond to the Respondent's requested information.

(c) CFG would be obliged to handle the information that the Respondent had provided in a manner that ensures its confidentiality.

(d) The disclosure was consistent with Section 20(2) of the Personal Data Protection Act 2012 ("**PDPA**") which states that an organisation, on or before disclosing personal data about an individual from another organisation without the consent of the individual, shall provide that other organisation with sufficient information regarding the purpose of the collection to allow that other organisation to determine whether the disclosure would be in accordance with the PDPA.

(e) The Complainant was, according to the Respondent, a former Financial Services Consultant "appointed by" the Respondent. He is therefore aware of the claims processing procedure, and would be, at the very least, deemed to have consented to the Respondent's collection, use and disclosure of his personal data for claims processing by reason of his former appointment or engagement.

C. COMMISSION FINDINGS AND ASSESSMENT

10. The issues in this case to be determined are as follow:

(a) Pursuant to Sections 13, 14, 15 and 20 of the PDPA, did the Respondent provide the necessary notification and obtain the necessary consent from the Complainant before disclosing pages 1 and 3 of the A&H Form to CFG, in particular the Complainant's Bank Account Details?

(b) If not, is the Respondent able to rely on any of the exceptions under the PDPA for the disclosure?

(c) Further, can the disclosure of the Bank Account Details contained on page 1 of the A&H Form to CFG be said to be "*for purposes that a reasonable person would consider appropriate in the circumstances*" under Section 18(a) of the PDPA?

Issue a: Notifying the Complainant and obtaining consent for the disclosure of A&H Form

11. The authorisation and declaration sections of the Application Form, A&H Form and the Policy are broadly worded and a plain reading leads to the conclusion that the consent obtained by the Respondent under the Application Form, A&H Form and Policy is wide enough to cover the disclosure made by the Respondent of pages 1 and 3 of the A&H Form to CFG. On this assessment of the relevant clauses produced before the Commission, the Commission finds that Respondent had the Complainant's *consent*, for the purposes of the PDPA, to

disclose the majority of personal data contained in pages 1 and 3 of the A&H Form to CFG, save for the Bank Account Details.

12. With regards to the Bank Account Details, the section of the A&H Form in which the Bank Account Details were to be entered expressly states that the Bank Account Details was for "*direct crediting of claims*". This purpose is at odds with and constrains the otherwise broad consent clauses in the Application Form, A&H Form and the Policy. Specific to this case, it does not extend to permitting the Respondent to disclose the Bank Account Details for the purpose of obtaining a medical report from third parties. This casts doubts as to whether the Complainant had in fact given his consent for such disclosure. On balance, the Commission is unable to draw a firm conclusion on whether the phrase "*direct crediting of claims*" was intended to and did in fact constrain the broad consent previously obtained by the Respondent or that the Complainant had effectively given his consent for the disclosure of his Bank Account Details for the purpose of obtaining a medical report. In the final analysis, the Commission thought it was prudent to decline making a finding of breach on the issue in the absence of clear supporting evidence. Further, the Commission's findings in respect of the issue of whether the disclosure of Bank Account Details accords with Section 18 of the PDPA, as will be examined below, makes it unnecessary to do so.

13. With regard to whether the Respondent had given sufficient *notification* to the Complainant for disclosing the Complainant's personal data for purposes of the Complainant's claim, the Commission is of the view that the A&H Form (and Policy) can possibly operate as prior notification for such a disclosure to be made.

14. In the premises, the Commission finds that Respondent has complied with its obligations under Sections 13, 14, 15 and 20 of the PDPA to provide the necessary notifications and obtain the necessary consent for the disclosure of in respect of the personal data (save for the Bank Account Details) found at pages 1 and 3 of the A&H Form to CFG. In relation to the Bank Account Details, on a balance, the Commission finds that there is insufficient evidence to show that the Respondent had failed to comply with its obligations under Sections 13, 14, 15 and 20 of the PDPA.

Issue b: Applicable exceptions and Section 19 of the PDPA

15. For completeness, the Commission also considered the applicability of Section 19 of the PDPA. Section 19 of the PDPA provides that an organisation may use personal data about an individual collected before the appointed day (ie 2 July 2014) for the purposes for which the personal data was collected unless (a) consent for such use is withdrawn in accordance with Section 16 of the PDPA; or (b) the individual, whether before, on or after the appointed day, has otherwise indicated to the organisation that he does not consent to the use of the personal data.

16. In this case, the Complainant had provided Personal Particulars in the Application Form to sign up for the insurance policy with the Respondent in 2011, and agreed to the terms set out in the Application Form, which provided for the Respondent to use the Complainant's personal data for a variety of purposes mentioned at paragraph 4 above. Since the personal Particulars were provided before the Appointed Day, pursuant to Section 19 of the PDPA, the Respondent was allowed to continue using them based on the terms of the Application Form, which includes disclosing the data to CFG for the purposes of obtaining a medical report for the insurance claim.

17. However, Section 19 of the PDPA does not apply to the Bank Account Details as they were not collected through the Application Form but through the A&H Form on 24 May 2015.

Issue c: Disclosure of personal data was not for purposes reasonable or appropriate in the circumstances

18. Section 18 of the PDPA provides, *inter alia*, that an organisation may collect, use or disclose personal data about an individual only for purposes that a reasonable person would consider appropriate in the circumstances. It should be borne in mind that Section 18 of the PDPA is an independent obligation that organisations would need to comply with even if it had obtained the consent from the relevant individual for the collection, use or disclosure of his or her personal data. This is an important aspect of the PDPA as it is effective in addressing excesses in the collection, use or disclosure of personal data under a broadly-worded consent clause, like in the present case.

19. In this case, the Bank Account Details of the Complainant were found at page 1 of the A&H Form that was disclosed to CFG. In the Commission's view, the disclosure of the Bank Account details by the Respondent was not for "*a purpose that a reasonable person would consider appropriate in the circumstances*" under Section 18 of the PDPA. The disclosure of the Bank Account Details was not relevant or necessary to the request for medical report from CFG. Of the reasons provided by the Respondent (and set out in paragraph 9), the most pertinent one is that of facilitating speedy processing of the claim. It is not obvious how Bank Account Details are relevant to CFG's role in the claim process, nor is it obvious how Bank Account Details will assist CFG in turning out its medical report sooner. In any event, Bank Account Details are necessary for the purpose of effecting payment, which is a function that is logically not within CFG's domain but which falls on the Respondent. Ultimately, the Respondent has not provided any reasonable explanation for why the disclosure of the Bank Account Details needed to be made in the circumstances. In the Commission's view, it was unsatisfactory for the Respondent to disclose sensitive personal data of a financial nature to a third party without good reason or purpose.

20. As discussed above, although the authorisation and declaration portion of the A&H Form provides for a broad-range of actions that may be taken in respect of

the personal data provided, the section of the A&H Form in which the Bank Account Details were to be entered states that the Bank Account Details were for "*direct crediting of claims*". The disclosure made therefore was for a purpose wholly different from this section of the form. Neither can it be said that the purpose of obtaining a medical report is one that is reasonably connected to this antecedent purpose. In the overall circumstances, it was not appropriate for the Respondent to be disclosing the Bank Account Details for a purpose that has no reasonable connection to that which was stated on the A&H Form.

21. In the premises, the Commission finds that the Respondent was in breach of Section 18 of the PDPA for the disclosure of the Complainant's Bank Account Details to CFG.

22. In respect of the other personal data that was provided in pages 1 and 3 of the A&H Form, the Commission is of the view that the disclosure was made reasonably under Section 18 of the PDPA as the Personal Particulars have clear relevance to and will facilitate the process of preparing a medical report.

D. ENFORCEMENT ACTION TAKEN BY THE COMMISSION

23. Given the Commission's findings that the Respondent is in breach of its obligations under Section 18 of the PDPA, the Commission is empowered under section 29 of the PDPA to give the Respondent such directions as it deems fit to ensure compliance with the PDPA. This may include directing the Respondent to pay a financial penalty of such amount not exceeding $1 million as the Commission thinks fit.

24. On a balance, the Commission has decided not to impose a financial penalty on the Respondent in view of the overall circumstances of the matter. Instead, the Commission has decided to issue a warning to the Respondent. In coming to this decision, the Commission has taken into account the following considerations:

    (a) The disclosure was limited to a single third party, CFG, and the personal data, which the unauthorised disclosure was made, although of a sensitive financial nature, was limited to a single data set, ie the Bank Account Details;

    (b) The disclosure had been under circumstances in which CFG knew that the personal data disclosed was to be treated confidentially;

    (c) There was no evidence of actual loss or damage suffered by the Complainant from the disclosure made; and

    (d) The Respondent had undertaken an immediate review of its processes in relation to the disclosure of personal data to parties following the incident.

25. The Commission emphasises that it takes a very serious view of any instance of non-compliance with the PDPA, and it urges organisations to take the necessary action to ensure that they comply with their obligations under the PDPA. The Commission will not hesitate to take the appropriate enforcement action against the organisation(s) accordingly.

LEONG KENG THAI
CHAIRMAN
PERSONAL DATA PROTECTION COMMISSION