PERSONAL DATA PROTECTION COMMISSION

[2023] SGPDPC 11

Case No. DP-2111-B9135

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

And

Koh Wei Ming @ Muhammad Amin Koh (trading as Mobile Chat)

… *Organisation*

DECISION

Koh Wei Ming @ Muhammad Amin Koh (trading as Mobile Chat)

Lew Chuen Hong, Commissioner — Case No. DP-2111-B9135

17 October 2023

Introduction

1 Between the period February 2020 – September 2021, the Personal Data Protection Commission ("the **Commission**") received 1,391 complaints from members of the public who received marketing messages, despite their numbers being registered with the Do Not Call Register ("**DNC Register**").[1] The messages were traced to 95 prepaid SIM cards purchased from one Koh Wei Ming @ Muhammad Amin Koh ("**KWM**"), the sole proprietor of Mobile Chat ("**the Organisation**").

2 The Commission commenced investigations to determine KWM's compliance with the Personal Data Protection Act 2012 ("**PDPA**") and for suspected breaches of the same.

Facts of the Case

3 The Organisation is in the business of the sale and servicing of mobile phones, as well as the sale of prepaid SIM cards and mobile phone accessories. It has operated since 2015 from a shop located in Geylang. As a retailer of M1 SIM cards,

[1] Under Section 43 of the PDPA, a person is not allowed to send specified messages to a Singapore telephone number registered with the DNC register unless the person has, at the time where he sends the specified message, valid confirmation that the Singapore telephone number is not listed in the DNC register.

KWM was provided a terminal device by M1 installed at the Organisation's premises for the purposes of SIM card registration (the "**M1 Terminal Device**"). The M1 Terminal Device was used for registration of SIM cards prior to December 2021. SIM card registration had to be carried out in accordance with the conditions of M1's telecommunications licence granted under Section 5 of the Telecommunications Act (Chapter 323).[2] The typical SIM card registration process would be as follows:

(a) First, the customer's identity document (e.g. identity card, passport, work pass etc.) would be scanned using the M1 Terminal Device, which is connected directly to M1's registration system. The system would capture the customer's personal data, and state whether the customer had reached the permitted limit of 3 prepaid SIM cards.

(b) Next, the barcode of the SIM card(s) would be scanned so that they could be tagged to the registered customer.

(c) Finally, a mobile application would be used to load credit value to the prepaid SIM card(s) to activate them for usage. This was done in the Organisation's premises. M1's policy was for each prepaid M1 SIM card to have a zero-initial balance, and for retailers to load some or all of the money paid by the customer.

4 The Commission's investigations revealed that KWM exploited the above registration process in order to use his customers' personal data without consent to

[2] The version of the Telecommunications Act 1999 which was in force at the time

register for additional prepaid M1 SIM cards that his customers did not intend to purchase. To do so, KWM would employ one of two methods:

(a) **Method 1 (Duplicate Scanning)** – After scanning a customer's identity documents via the M1 Terminal Device to register the SIM card they wished to purchase, KWM would scan the identity documents a second time to register a second SIM card to the same customer without their knowledge. KWM would then hand over only one SIM card to the customer, and keep the other to sell to unauthorised purchasers.

(b) **Method 2 (Incomplete Transactions)** – Occasionally, customers who had completed the registration process would not want to continue with their purchase after learning that the credit value of the SIM card would have to be separately loaded. At this juncture, instead of cancelling or reversing the registration process, KWM would keep the SIM card(s) and activate them without the customer's knowledge, and thereafter offer them for sale to other unauthorised purchasers.

5 During investigations, KWM admitted that the purpose of the above two methods was to earn extra money from the unauthorised sale of the preregistered SIM cards. In his 4 years of selling such SIM cards to anonymous purchasers, KWM estimated that he made a profit of approximately $35,000 (i.e. around 250 illicit SIM cards per year at a profit of $35 per card).

6 The affected personal data collected and used by KWM to register the illicit SIM cards include the following personal data of 73 individuals (used to register 95 SIM cards):

(a) The customers' names;

(b) The customers' addresses; and

(c) The customers' NRIC / FIN / passport numbers.

7 However, it is likely that the personal data of many more individuals (approximately 1,000) was affected, based on KWM's admission that he sold an average of 250 prepaid SIM cards annually over 4 years.

Findings and Basis for Determination

8 Section 2(1) of the PDPA defines an "*organisation*" to include "*any individual, company, association or body of persons, corporate or unincorporated*". The Organisation is a sole proprietorship and has no separate legal personality from KWM. Further, KWM was acting in a business capacity in selling the illicit SIM cards to make a profit, and not a domestic capacity (which ordinarily would have excluded him from being bound by the PDPA).[3] Accordingly, KWM (trading as the Organisation) is an organisation for the purposes of the PDPA.

[3] See also *Re Sharon Assya Qadriyah Tang* [2018] SGPDPC 1 at [9] – [10] and *Re Neo Yong Xiang (trading as Yoshi Mobile)* [2021] PDPC 12 at [8]

9 Based on the circumstances set out above, the Commission's investigation centred on whether KWM had breached:

(a) The Consent Obligation under section 13 of the PDPA; and

(b) The Purpose Limitation Obligation under section 18 of the PDPA.

The Consent Obligation under section 13 of the PDPA

10 Under Section 13 of the PDPA, organisations are prohibited from collecting, using or disclosing an individual's personal data unless the individual gives, or is deemed to have given, his consent, unless otherwise authorised under the PDPA or any other written law (the "**Consent Obligation**").

11 KWM breached the Consent Obligation by using his customers' personal data without their consent:

(a) In the case of Method 1 (Duplicate Scanning), KWM's customers consented to the collection and use of their personal data only for the purpose of registering the number of SIM card(s) they had requested. They did not provide consent to KWM to use their personal data for any other purpose, including the registration of additional SIM cards.

(b) In the case of Method 2 (Incomplete Transactions), the customers had withdrawn their consent to the use of their personal data at the point where they found that the credit value of the SIM card would have to be separately loaded. The correct action for KWM to take would have been to cancel the SIM card registration and not use the customers' personal data any further. Instead,

KWM proceeded to keep the registered SIM card and activated them separately, thereby continuing with the use of customers' personal data for purposes they had not consented to.

12 In the premises, KWM breached the Consent Obligation.

The Purpose Limitation Obligation under Section 18 of the PDPA

13 Under Section 18 of the PDPA, 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, and where that individual has been informed of the said purposes under Section 20 of the PDPA (the "**Purpose Limitation Obligation**"). As set out in the Commission's Advisory Guidelines on Key Concepts in the PDPA:[4]

> "The main objective of the Purpose Limitation Obligation is to ensure that organisations collect, use and disclose personal data that are relevant for the purposes, and only for purposes that are reasonable.
>
> For the purposes of section 18 (and as stated in that section), whether a purpose is reasonable depends on whether a reasonable person would consider it appropriate in the circumstances. Hence the particular circumstances involved need to be taken into account in determining whether the purpose of such collection, use or disclosure is reasonable. For example, a purpose that is in violation of a law or which would be harmful to the

[4] Advisory Guidelines on Key Concepts in the PDPA (Rev 16 May 2022) at [13.3] – [13.4]

individual concerned is unlikely to be considered appropriate by a reasonable person."

[emphasis added]

14 The Purpose Limitation Obligation limits the use of personal data to the purposes for which the data subject had been notified and consented to, unless an exception to the consent requirement is applicable. The purpose for processing is subject to a backstop, in that it must be reasonable in the circumstances.[5] In considering whether the Purpose Limitation Obligation was breached, it is obvious that the data subject did not give his consent for his or her personal data to be used for registering SIM cards that were to be sold to other purchasers. The purpose that the data subjects had consented to were for registration of SIM cards that they were purchasing.

15 In the present case, KWM admitted that his purpose for using his customers' personal data was to register illicit SIM cards in order to sell them to third parties and thereby make a profit. KWM also admitted that he knew this was wrong and illegal. Such use of personal data is clearly not a reasonable purpose under any circumstances, as KWM's customers could not have reasonably intended for their personal data to be used to register illicit SIM cards for KWM's financial gain.

[5] See *Re AIA Singapore Pte Ltd* [2016] SGPDPC 10 at [18] and *Re Neo Yong Xiang (trading as Yoshi Mobile)* [2021] SGPDPC 12 at [15]

16 In the premises, KWM has breached the Purpose Limitation Obligation.

The Commissioner's Preliminary Decision

17 In determining whether to impose a financial penalty on KWM pursuant to section 48J(1) of the PDPA, and the amount of any such financial penalty, the matters set out at section 48J(1) and the factors listed at section 48J(6) of the PDPA were taken into account, including the following aggravating and mitigating factors:

Aggravating Factors

(a) KWM's breaches of the PDPA were difficult to detect as they did not come to light until the customers' numbers and personal data had been misused to send marketing messages. The Commission notes that prepaid SIM cards are frequently used to further criminal activities; accordingly, a supplier of prepaid SIM cards who breaches the PDPA must be dealt with severely for deterrence purposes;

(b) KWM's actions were intentional and took place over a long period of 4 years;

(c) KWM's breaches of the PDPA caused inconvenience to innocent parties, as the illicit SIM cards sold by him were used to send unsolicited messages to phone numbers that were registered with the DNC Register;

(d) Through the sale of the illicit SIM cards for approximately 4 years, KWM financially gained approximately $35,000 through the misuse of his customers' personal data; and

Mitigating Factors

(e) KWM admitted to liability early in the investigation process, thus reducing the time and resources expended on investigations.

18 KWM was notified of the preliminary decision by way of the Commission's letter dated 16 May 2023 and was invited to make representations on the same.

Representations Made by KWM

19 On 17 May 2023, KWM made the following representations to the Commission seeking that a financial penalty not be imposed:

(a) He is the sole breadwinner of his family. However, he is likely to have a period without any income as he had been charged with committing an offence under Section 5(1) (read with Section 11A) of the Computer Misuse Act (Cap. 50A, Rev. Ed. 2007) for unauthorised use of computer material, and was likely to be sentenced to an imprisonment term. The Commission notes that on 14 September 2023, he was sentenced to 16 months' imprisonment for the said offence; and

(b) He was seeking treatment at the Institute of Mental Health ("**IMH**") for mental health issues.

20 KWM's representations are not accepted for the following reasons:

(a) Despite the Commission's repeated requests for him to adequately substantiate his assertions of personal and financial hardship, he did not do so.

(b) The fact that he was charged and sentenced for a criminal offence, arising from the same set of actions as those which caused the breaches of the PDPA, is not in and of itself relevant to any enforcement action taken by the Commission.

(c) The fact that he was seeking treatment at the IMH is not, in and of itself, a mitigating factor – especially when he was unable to provide further information about (i) the condition(s) for which he was seeking treatment and (ii) how such condition(s) were related to his breaches of the PDPA.

21 Having considered all the relevant circumstances of this case, the Commissioner hereby requires KWM to pay a financial penalty of $48,000 within 30 days from the date of the relevant notice accompanying this decision, 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.

22 No further directions are required given that the Organisation has ceased the unauthorised sale of preregistered SIM cards.

WONG HUIWEN DENISE
DEPUTY COMMISSIONER
FOR COMMISSIONER FOR PERSONAL DATA PROTECTION