

PERSONAL DATA PROTECTION COMMISSION

[2021] SGPDPC 12

Case No. DP-2013-B8088

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

And

Neo Yong Xiang (trading as Yoshi Mobile)

... Organisation

DECISION

Data Protection – Consent obligation – Use of personal data without consent

Data Protection – Purpose limitation obligation – Use of personal data for purposes that a reasonable person would consider appropriate in the circumstances

Neo Yong Xiang (trading as Yoshi Mobile)

[2021] SGPDPC 12

Lew Chuen Hong, Commissioner – Case No. DP-2013-B8088

29 October 2021

Introduction

1. When customers purchased pre-paid SIM cards from a mobile phone shop at Geylang Road, they would not have anticipated that their personal data would be misused to register additional SIM cards for illegal sale. Unfortunately, this was exactly what happened to at least 78 individuals who purchased pre-paid M1 SIM cards from one Mr Neo Yong Xiang (“**NYX**”) the sole proprietor of Yoshi Mobile (“**YM**”).

2. The Commission observed that between January 2020 and November 2020, there were 3,636 Do Not Call (“**DNC**”) complaints from persons who received specified messages even though their telephone numbers are registered with the DNC register¹. Further analysis revealed that 1,379 of the messages were sent from 98 SIM cards registered at YM. The Commission initiated investigations against NYX (trading as YM) for suspected breaches of the Personal Data Protection Act 2012 (“**PDPA**”).

Facts of the Case

3. NYX has operated YM since 2013. As an exclusive retailer of M1 SIM cards, NYX was provided a terminal device installed at YM’s premises for the purposes of SIM card

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.

registration (the “**M1 Terminal Device**”). 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). The typical SIM card registration process in YM 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. 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. 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 NYX exploited the above registration process in order to use his customers’ personal data without consent to register for additional prepaid M1 SIM cards that his customers did not intend to purchase. NYX would do so by one of two methods:

- (a) **Method 1** – After scanning a customer’s identity documents via the M1 Terminal Device, NYX would check whether the customer was still entitled to purchase more SIM cards (in addition to the SIM card(s) that were intended to be purchased). If so, NYX would proceed to register additional SIM card(s) to the same customer without their knowledge (the “**illicit SIM card(s)**”).

(b) **Method 2** – 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, NYX would keep the SIM card(s) and activate them without the customer’s knowledge.

5. During investigations, NYX admitted that his purpose for registering the illicit SIM cards was to sell them to earn extra money. In his three years of selling such illicit SIM cards to anonymous walk-in customers, NYX estimated that he earned approximately \$15,000 (i.e. around 100 illicit SIM cards per year at a price of \$50 per card).

6. The affected personal data collected and used by NYX to register the illicit SIM cards include, at a minimum, the following personal data of 78 individuals (used to register 94 SIM cards):

- (a) the customers’ names;
- (b) the customers’ addresses; and
- (c) the customers’ NRIC numbers and/or work permit numbers.

7. After registering the illicit SIM cards, NYX would sell them to anonymous buyers who occasionally patronised YM from 2018 to 2020. Investigations revealed that illicit SIM cards registered at YM were exploited by unknown perpetrators to send unsolicited spam and/or scam messages, often also in contravention of the DNC provisions of the PDPA.

Findings and Basis for Determination

8. Section 2(1) of the PDPA defines an “*organisation*” broadly to include “*any individual, company, association or body of persons, corporate or unincorporated*”. YM is a sole

proprietorship and has no separate legal personality from NYX. Accordingly, NYX constitutes an organisation under the PDPA. Further, NYX is bound by the provisions of the PDPA (including Part IV) as he was acting in a business capacity in selling the SIM cards to make a profit, and not a domestic capacity. As stated in *Re Sharon Assya Qadriyah Tang* [2018] SGPDP 1:

“9 ...Although the PDPA defines “organisation” broadly to include individuals, an individual is expressly excluded from the Data Protection Provisions in the PDPA if the individual was acting in a personal or domestic capacity. *Therefore, when it comes to the application of the PDPA to individuals, it is usually germane to the issue to determine whether the individual was acting in a personal or domestic capacity. If the individual was not acting in a personal or domestic capacity, then she will be treated as an “organisation” for the purposes of the PDPA, and obliged to comply with the Data Protection Provisions.*

10 *On the facts, the Respondent was clearly not acting in a personal or domestic capacity in respect of the buying and selling of leads. The purchase and sales of the leads were not for her own personal use or purposes, but in order to make a profit.* Under the PDPA, “business” includes an activity of any organisation, whether or not carried on for purposes of gain, or conducted on a regular, repetitive or continuous basis, but does not include an individual acting in his personal or domestic capacity. In this regard, the converse of a person acting in a personal or domestic capacity is one that acts in a business capacity. This was the case for the Respondent in respect of the purchase and sale of leads.”

[emphasis added]

9. Based on the circumstances set out above, the issues to be determined in this case are:

- (a) Whether NYX breached the Consent Obligation under section 13 of the PDPA; and
- (b) Whether NYX breached 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, an exception to the requirement for consent applies, or if otherwise authorised under the PDPA or any other written law (the “**Consent Obligation**”). In this connection, Section 14(1) of the PDPA further provides that an individual has not given consent unless he has been notified of the purposes for which his personal data was being collected, used or disclosed. If an organisation fails to do so, any consent obtained from an individual is invalid.

11. On the facts of this case, NYX breached the Consent Obligation by using his customers’ personal data to register the illicit SIM cards for sale to anonymous buyers. When NYX used Method 1, NYX’s customer(s) only consented to the collection and use of their personal data for the purpose of registering the number of SIM cards which they had requested. They did not provide consent to NYX to use their personal data for any other purpose, including the registration of additional SIM cards.

12. In the case of Method 2, the customers withdrew their consent to the collection and use of their personal data to purchase M1 SIM cards, and NYX should have cancelled the SIM card registrations. Instead, he went behind his customers’ backs and used their personal data without consent to register illicit SIM cards.

13. In the premises, NYX is determined to have breached the Consent Obligation by using his customers' personal data without their consent.

The Purpose Limitation Obligation under Section 18 of the PDPA

14. 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 PDPA²:

“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. Consistent with the Notification Obligation, the Purpose Limitation Obligation also limits the purposes for which personal data may be collected, used or disclosed to those which have been informed to the individuals concerned pursuant to the Notification Obligation (where applicable).

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

[emphasis added]

² [Advisory Guidelines on Key Concepts in the PDPA](#) (Rev 1 February 2021)

15. The Purpose Limitation Obligation operates independently from the Consent Obligation. Even if the data subject gave his consent for his personal data to be used for a particular purpose, it does not follow that the said purpose is reasonable in the circumstances.

As stated in *Re AIA Singapore Pte Ltd* [2016] SGPDPC 10 at [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.”

[emphasis added]

16. In this case, NYX has admitted that he had fraudulently used his customers’ personal data for the purpose of registering illicit SIM cards in order to sell them to anonymous buyers. This is plainly not a reasonable purpose under any circumstances, as individuals could not have reasonably intended for their personal data to be used to register illicit SIM cards purely for NYX’s financial gain.

17. In the premises, NYX is determined to have breached the Purpose Limitation Obligation.

The Commissioner's Decision

18. In determining whether NYX should be required to pay a financial penalty under section 48J of the PDPA, the factors listed at section 48J(6) of the PDPA were considered, with particular emphasis on the following aggravating and mitigating factors:

Aggravating Factors

- (a) NYX's breaches of the PDPA were difficult to detect as it included a high degree of planning and pre-meditation by him to evade detection by authorities;
- (b) NYX was entrusted by his customers with their personal data for the purpose of registering prepaid SIM cards, and he abused their trust by misusing their personal data;
- (c) NYX'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 3 years, NYX financially gained at least \$15,000 for his misuse of his customers' personal data; and

Mitigating Factor

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

NYX's representations

19. On 7 September 2021, NYX was notified of the Commissioner's Preliminary Decision (as set out above) and intention to impose a financial penalty of \$35,000. On 20 September 2021, NYX submitted written representations on the amount of financial penalty that was to be

imposed. NYX raised the following factors to argue for either a waiver of the imposition of a financial penalty, or (in the alternative) for a lower financial penalty:

- (a) NYX was facing a difficult financial situation, as he had low savings / monthly income, and was responsible for servicing several outstanding liabilities (such as a vehicle loan, housing loan and renovation loan). Additionally, he was also responsible for paying the medical bills of his parent. NYX claimed that it would cause him undue hardship if a high financial penalty was imposed.
- (b) NYX had breached the PDPA for financial gain due to extenuating circumstances, as his business was adversely affected by COVID-19 and the landlord of Yoshi Mobile had refused to pass on the relevant COVID-19 rental relief provided by the Government.
- (c) NYX's breaches of the PDPA can be distinguished from the breaches committed by other organisations on the basis that he did not leak or sell the personal data for financial gain. Instead, he had merely used his customers' personal data to register for SIM cards and was not the person who used the illicit SIM cards to send unsolicited text messages to telephone numbers on the DNC register. In this connection, NYX pointed to other decisions where the Commission had imposed a lower financial penalty or a warning on other organisations that had breached the PDPA.

20. After careful consideration, we have accepted and taken into account NYX's representation at [19(a)] above, but are unable to do the same with respect to the representations set out in [19(b)] and [19(c)] above.

21. When imposing financial penalties, the Commission may consider the personal and financial circumstances of the organisation / individual, bearing in mind that financial penalties imposed should avoid imposing a crushing burden or cause undue hardship on organisations: see *Re Jigyasa* [2021] SGPDP 1. In considering NYX's representations at [19(a)], the Commission gave due consideration to the existing financial commitments on NYX and accepted that the imposition of a heavy financial penalty would cause substantial hardship to NYX.

22. We are unable to accept NYX's representation at [19(b)] that he had breached the PDPA due to extenuating financial difficulties that arose due to the COVID-19 pandemic. Based on the Commission's investigations, NYX has been using his customers' personal data to register illicit SIM cards for the purpose of selling them to third parties since 2018. NYX's *modus operandi* (as described in [4]) predated the onset of COVID-19, and it is disingenuous for NYX to attribute his actions to the financial difficulties that followed the COVID-19 pandemic.

23. We are also unable to accept NYX's representation at [19(c)] that his breach of the PDPA was less serious than the breaches committed by various other organisations. Compared with the decisions that NYX mentioned, NYX's culpability is more egregious as his breach involved the intentional misuse of personal data from a position of trust, over a protracted period of time, for personal financial gain. While NYX did not send any unsolicited text messages or make any unsolicited calls directly to telephone numbers on the DNC register, his sale of the unsolicited SIM cards to anonymous buyers (that NYX did not verify or identify) facilitated the commission of those offences and the harm caused as a consequence. The anonymous sale of illicit SIM cards may also be the catalyst or precursor for other illicit activities.

24. Having carefully considered the all the relevant factors of this case including the representations made by NYX, the Commissioner has decided to reduce the financial penalty to \$21,000. This decision is made on an exceptional basis, and should not be taken as setting any precedent for future cases. The Commissioner hereby requires NYX to pay a financial penalty of \$21,000 in 18 monthly instalments by the due dates as set out in the 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.

25. The Commission will not be issuing any further directions given that M1 has barred NYX from offering the sale of its prepaid SIM cards.

**YEONG ZEE KIN
DEPUTY COMMISSIONER
FOR COMMISSIONER FOR PERSONAL DATA PROTECTION**