PERSONAL DATA PROTECTION COMMISSION

[2024] SGPDPCS 1

Case No. DP-2208-C0053

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

And

Tok Leng Leng (trading as Top Mobile Gallery (BR)

DECISION

Data Protection *– Protection obligation – Unauthorised use of and access to personal data – Insufficient administrative security arrangements and lack of access controls*

SUMMARY OF THE DECISION

Introduction

1. Between the period December 2020 to April 2021, the Personal Data Protection Commission ("the **Commission**") received 435 Do Not Call ("**DNC**") complaints relating to property messages, despite their numbers being registered with the DNC Register. The complaints were traced to 44 M1 pre-paid SIM cards sold by Tok Leng Leng (trading as Top Mobile Gallery (BR)) ("**Organisation**"), located in a foreign worker dormitory at 2 Seletar North Link.

2. The Commission commenced investigations into the Organisation for suspected breaches under the Personal Data Protection Act 2012 ("**PDPA**").

Facts of the Case

3. The 44 M1 pre-paid SIM cards were registered under 33 unique individuals who were foreign workers. Investigations confirmed that these foreign workers lived in the dormitory at 2 Seletar North Link, and had purchased pre-paid SIM cards from the Organisation. Additional pre-paid SIM cards were registered under their names even though they had not in fact purchased these SIM cards (the **"illicit SIM cards**").

4. As a retailer of M1 SIM cards, the Organisation used a terminal device issued by M1 for the purposes of SIM card registration. The SIM card registration process with the M1 terminal device was as follows:

a. First, the customer's identity document (e.g. identity card, passport, work pass etc.) would be scanned using the terminal device, which is connected directly to M1's registration system. The system would capture the customer's particulars, and whether the customer had reached the limit of 3 pre-paid 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, the retailer would use a mobile application 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 the money paid by the customer.

5. At a certain point in time, the Organisation started registering M1 pre-paid SIM cards via a M1 mobile application on a mobile phone.

6. As the Organisation registered M1 pre-paid SIM cards by scanning the front and back of the affected individuals' work permits, the following types of personal data was affected:

a. Name;

b. Sex;

c. FIN / work permit number;

d. Date of Birth;

e. Nationality; and

f. Name of employer.

Findings and Basis for Determination

7. 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 Tok Leng Leng ("**TLL**"). Accordingly, TLL (trading as Top Mobile Gallery (BR)) is an organisation for the purposes of the PDPA.

8. Based on the circumstances set out above, the Commission's investigation centered on whether the Organisation had breached the Protection Obligation under section 24 of the PDPA.

The Protection Obligation under section 24 of the PDPA

9. Under section 24(a) of the PDPA, organisations must protect personal data in its possession or under its control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification or disposal, or similar risks (the "**Protection Obligation**").

10. During investigations, the Organisation admitted to a breach of section 24 of the PDPA. TLL, the sole proprietor of Top Mobile Gallery (BR), accepted that she failed to have security arrangements in place to protect against the unauthorised use of and access to customers' personal data for registration of M1 pre-paid SIM cards:

a. First, TLL admitted that she could have but failed to maintain an inventory of M1 pre-paid SIM cards. TLL explained that in contrast to the SIM cards sold by other retailers such as Singtel or Starhub which came with a pre-paid balance, M1 pre-paid SIM cards came with zero initial-balance. This contributed to her omission to maintain an inventory. Furthermore, the M1 salesperson did not have a fixed schedule for delivering the pre-paid SIM cards to the Organisation and would deliver more pre-paid SIM cards to the Organisation sporadically, which her employees would then acknowledge receipt.

b. Second, TLL admitted that she failed to have processes in place that would require the employees to account for each M1 pre-paid SIM card sold and to whom the pre-paid SIM card was registered. TLL admitted that all her employees had equal access to the M1 pre-paid SIM cards. The Deputy Commissioner notes that the Organisation could have maintained a record of the name of the employee who sold each pre-paid SIM card, the date, time and place of registration, and sufficient particulars of the individual to whom the SIM card was sold and registered to.

c. Third, TLL alluded in her statements of how her employees enjoyed the same “access” to register the pre-paid SIM cards. This was corroborated by an employee, who stated that the login credentials to the M1 application used for registration of pre-paid SIM cards was shared amongst the employees, and that the employees would login to the M1 application on their personal mobile devices if the Organisation’s mobile

device was not readily available. In the Deputy Commission's view, the Organisation's failure to implement access control restrictions and to prohibit the sharing, amongst its employees, of the login credentials to the M1 mobile application used to register pre-paid SIM cards made it much easier for the employees to turn rogue, as it became harder to detect the errant employee.

d. TLL also admitted that there was little or no supervision over the Organisation's employees regarding how they used or accessed the customers' personal data. She was often not at the shop and left the shop to be managed by her employees. While there was CCTV footage installed at the Organisation, she did not review the CCTV footage often.

11. For the reasons set out above, the Deputy Commissioner finds the Organisation in breach of the Protection Obligation under section 24 of the PDPA as there has been a complete failure to adopt any security arrangements to protect the customers' personal data from misuse.

The Deputy Commissioner's Preliminary Decision

12. In determining whether to impose a financial penalty on the Organisation 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.

13. In addition, the Deputy Commissioner also considered the following factors which would justify an increase or decrease in the financial penalty:

Factors that justify an increase in the financial penalty

a. The Organisation's breaches of the PDPA had caused inconvenience to other innocent parties. The illicit SIM cards sold by the Organisation were used to send unsolicited messages to phone numbers that were registered with the DNC Register.

b. Even though TLL denied knowledge of any wrongdoing on the part of her employees, TLL has been the registered sole-proprietor of Top Mobile since 2014. She ought to have been aware of the practice of registering illicit SIM cards. The Organisation's lackadaisical attitude towards preventing the potential misuse of individuals' personal data and failure to introduce reasonable safeguards displayed a higher level of culpability.

Factors that justify a decrease in the financial penalty

c. The Organisation admitted to its contravention to the PDPA and co-operated fully with the investigation process.

d. This is the first incident of a personal data breach by the Organisation.

14. Having considered the above factors and circumstances, the Commission preliminarily determined that a financial penalty of $7,000 would be imposed in respect of the Organisation's contravention of the Protection Obligation. On 23 November 2023, the Organisation was notified of the Commission's preliminary decision, including the full findings set out above, and given 14 days to make written representations.

Representations Made by the Organisation

15. While the Organisation did not challenge the findings and bases of the contravention, the Organisation made representations to the Commission seeking that a financial penalty not be imposed, summarised as follows:

a. TLL, as the sole proprietor of Top Mobile Gallery (BR), admitted that as the boss it was her fault in failing to realise that her staff had misappropriated the information provided by the customers in time;

b. The Organisation had been in business since 2014 and had always complied with applicable laws and regulations. Effectively, this is the Organisation's first contravention of the PDPA;

c. The financial penalty of $7,000 is a hefty amount for the Organisation.

16. The Commission considered the representations made carefully but was unable to accept them for the following reasons:

a. The Commission had already taken into account the first two factors raised by the Organisation, in arriving at the preliminary decision;

b. The Organisation had not substantiated to the Commission that it is experiencing financial difficulties and would be unable to continue with its usual business activities following the imposition of the financial penalty.

17. Having considered all the relevant circumstances of this case, the Commission hereby requires the Organisation to pay a financial penalty of $7,000 within 30 days from the date of the relevant notice accompanying this decision.

The following section of the Personal Data Protection Act 2012 had been cited in the above Summary of the Decision:

Protection of personal data

24(a). An organisation must protect personal data in its possession or under its control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification or disposal, or similar risks.