PERSONAL DATA PROTECTION COMMISSION

[2023] SGPDPC 14

Case No. DP-2211-C0404

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

And

Lee Chee Meng

… *Organisation*

DECISION

Data Protection *– Consent obligation – Collection and use of personal data without consent – Failure to perform due diligence prior to collection of personal data from third party*

Data Protection *– Notification obligation – Failure to notify individual of purposes for collection, use and disclosure of personal data – Failure to perform due diligence prior to collection of personal data from third party*

Lee Chee Meng

Wong Huiwen Denise, Deputy Commissioner — Case No. DP-2211-C0404

29 December 2023

Introduction

1 On 8 November 2022, the Personal Data Protection Commission (the "**Commission**") received a complaint regarding the possible unauthorised collection and use of personal data by Mr Lee Chee Meng (the "**Respondent**") for telemarketing purposes. The Commission subsequently commenced investigations to determine whether the circumstances disclosed any breaches by the Respondent of the Personal Data Protection Act 2012 ("**PDPA**").

2 Based on the Commission's investigations, the facts disclose a straightforward breach of the PDPA. In particular, the Respondent admits to committing the infringing acts. The Commission has accordingly found the Respondent in breach of sections 13 and 20 of the PDPA.

Facts of the Case

3 The Respondent is a registered salesperson under the Estate Agents Act 2010. He is appointed by ERA Realty Network Pte Ltd ("**ERA**") to engage in estate agency work and to otherwise promote the business of servicing the public in real estate transactions.

4 At all material times, the Respondent is and was an independent agent of ERA who receives commissions in respect of real estate services or transactions entered into between customers and ERA.

5 The Respondent was upfront in admitting that he has been purchasing personal data from unknown third parties for telemarketing purposes for approximately 10 years from 2013.

6 In the course of 2021, the Respondent purchased 5 sets of personal data amounting to about 420,000 records (the "**Purchased Data**") from an individual with a foreign phone number known to the Respondent only as "Ali" (the "**Seller**"). The Respondent came to know of the Seller through social media and would communicate with the Seller over Whatsapp, following which the Seller would e-mail the Purchased Data to the Respondent in the form of Microsoft Excel spreadsheets. The Respondent paid the Seller a total of about S$1,200 for the Purchased Data.

7 The Purchased Data comprised the following:

Number of affected individuals	~420,000
Types of personal data	• Name • E-mail address • Contact number • Address (either residential or office, but not both) • Partial credit card number, i.e., the last 4 digits (for some entries)

8 After receiving each set of Purchased Data, the Respondent would sort through it for names, e-mail addresses, contact numbers, and residential addresses, and use this personal data to send targeted marketing e-mails and SMSes to the individuals concerned. For example, if the Respondent saw that an individual was living in a certain area of Singapore, he would send an e-mail or SMS to that individual informing him or her of the property transaction prices in that area. The Respondent did not send marketing communications to all the affected individuals as he estimated that about 75% of the Purchased Data contained business-related information and not residential information.

9 The Respondent stated that he did not use the Purchased Data for any other purpose, and that he included an unsubscribe function in his marketing emails. The latter enabled him to delete the personal data of any individuals who used this unsubscribe function. He also stated that he would first check the contact numbers against the Do Not Call ("**DNC**") Registry and would not send marketing SMSes to any DNC-registered contact numbers.

10 The Commission found no evidence to contradict these statements. In particular, the Commission has not received any DNC-related complaints involving the Respondent. There was also no evidence that the Respondent ever re-sold the Purchased Data, or that he was involved in the Seller's business in any capacity other than as a buyer (e.g., as an accomplice).

Findings and Basis for Determination

Preliminary Issues

11 At the outset, the Respondent was bound by the data protection obligations in Parts 3 to 6A of the PDPA as he had operated as an "organisation" in respect of his collection and use of the Purchased Data[1]:

(a) The definition of "organisation" in section 2(1) of the PDPA includes individuals.

(b) Section 4(1)(a) of the PDPA provides that Parts 3 to 6A of the PDPA do not impose any obligation on any individual acting in a personal or domestic capacity. However, the Respondent was not acting in a personal or domestic capacity in respect of his purchase of the Purchased Data from the Seller and subsequent use for telemarketing purposes. These actions were done for profit, in furtherance of the Respondent's business as a real estate salesperson.

(c) Section 4(1)(b) of the PDPA provides that Parts 3 to 6A of the PDPA do not impose any obligation on any employee acting in the course of his or her employment with an organization. However, as mentioned at [4]

[1] The Commission has in earlier cases also determined that individuals fall within the definition of "organisation" under the PDPA, and that individuals are subject to the obligations in Parts 3 to 6A of the PDPA insofar as they are not acting in a personal or domestic capacity (see for example *Re Sharon Assya Qadriyah Tang* [2018] SGPDPC 1 (at [9] to [12]) and *Re Neo Yong Xiang (trading as Yoshi Mobile)* [2021] SGPDPC 12 (at [8])).

(d) above, the Respondent was not in an employee-employer relationship with ERA. He acted at all material times as an independent agent.

The Consent and Notification Obligations under the PDPA

12 The relevant data protection obligations applicable to the Respondent's collection and use of personal data are:

(a) the obligation, before collecting, using or disclosing the personal data, to inform the individual(s) in question of the purposes for which such personal data is being collected, used or disclosed (the "**Notification Obligation**")[2]; and

(b) the obligation to first obtain the consent of the individual(s) in question to the collection, use or disclosure of the personal data for such purposes[3] (an individual cannot be said to have given consent unless he or she has been provided with the information required under the Notification Obligation, and has provided consent for the stated purposes[4]) (the "**Consent Obligation**").

13 The central issue in this case is whether the Respondent breached the Consent Obligation and/or the Notification Obligation under the PDPA.

[2] Section 20 of the PDPA.
[3] Section 13 of the PDPA.
[4] Section 14 of the PDPA.

Whether the Respondent breached the Consent Obligation

14 On the facts of this case, the Respondent breached the Consent Obligation by failing to ascertain that the consent of the individuals concerned had been obtained before purchasing their personal data from the Seller and subsequently sending unsolicited telemarketing communications to them.

15 The fact that the Respondent purchased the Purchased Data from a third party (i.e. the Seller) does not derogate from the Commission's breach finding. The Commission has in *Re Sharon Assya Qadriyah Tang* [2018] SGPDPC 1 (at [13]) and *Re Amicus Solutions Pte. Ltd. & Anor.* [2019] SGPDPC 33 (at [26] and [47]) observed that purchasing personal data from a third-party seller constitutes the collection of personal data under the PDPA, notwithstanding that such personal data was not collected directly from the individuals concerned themselves.

16 The fact of this "indirect" collection does not exempt data buyers from their data protection obligations in relation to the collection or subsequent use or disclosure of the collected personal data. The required standard was articulated in *Re Amicus Solutions* (at [48] and [49]), quoting in turn the UK Information Commissioner's Office ("**ICO**")'s decision in *The Data Supply Company*:

> "48 … The ICO issued a monetary penalty of £20,000 and gave the following guidance in the Monetary Penalty Notice (at [22] to [25]):
>
> **Data controllers buying marketing lists from third parties must make rigorous checks to satisfy themselves that the third party**

obtained the personal data fairly and lawfully, that the individuals understood their details would be passed on for marketing purposes, and that they have the necessary consent.

Data controllers must take extra care if buying or selling a list that is to be used to send marketing texts, emails or automated calls. The Privacy and Electronic Communications Regulations 2003 specifically require that the recipient of such communications has notified the sender that they consent to receive direct marketing messages from them. Indirect consent (ie consent originally given to another organisation) may be valid if that organisation sending the marketing message was specifically named. But more generic consent (eg marketing 'from selected third parties') will not demonstrate valid consent to marketing calls, texts or emails.

Data controllers buying in lists must check how and when consent was obtained, by whom, and what the customer was told. It is not acceptable to rely on assurances of indirect consent without undertaking proper due diligence. Such due diligence might, for example, include checking the following:

- How and when was consent obtained?
- Who obtained it and in what context?
- What method was used – eg was it opt-in or opt-out?

- Was the information provided clear and intelligible? How was it provided – eg behind a link, in a footnote, in a pop-up box, in a clear statement next to the opt-in box?
- Did it specifically mention texts, emails or automated calls?
- Did it list organisations by name, by description, or was the consent for disclosure to any third party?
- Is the seller a member of a professional body or accredited in some way?

…

[Emphasis added.]

49 While there is no uniform industry standard in relation to how a buyer should verify whether the seller has obtained the consent of the individuals, the positions articulated by the ICO must be right. A reasonable person would likely undertake proper due diligence, such as seeking written confirmation that the personal data sold was actually obtained via legal sources or means, or inquire further as to whether the individuals had provided their consent and were notified of the disclosure, and if so, obtain a sample of such consent and notification."

17 The Respondent has fallen short of the standard set out in *Re Amicus Solutions Pte. Ltd.* by failing to perform the required due diligence to ensure that the individuals' consent had been obtained for the sale of the Purchased Data by the Seller to the

Respondent, or for the Respondent's subsequent use for the purposes of telemarketing. During the Commission's investigations, the Respondent admitted that he did not know whether the Seller had obtained the consent of the individuals in relation to the sale of the Purchased Data, and that he did not perform any additional verification checks or question the Seller as to how he had obtained the Purchased Data. There is no evidence that the Respondent contacted the individuals directly to obtain their consent. The Respondent also stated that he was not aware of whether the Purchased Data originated from any data breaches[5].

18 The Respondent was negligent in purchasing and using the Purchased Data from an unknown online seller without performing any due diligence in relation to the provenance of the Purchased Data or whether the individuals concerned had been notified of or given their consent for its collection and use. He therefore did not take sufficient steps to discharge the requirements under the Consent Obligation. As stated at [9] and [10] above, the Commission accepts that the Respondent had provided an opt-out option in his telemarketing e-mails, took pains to ensure compliance with the DNC provisions under the PDPA, and had breached the PDPA out of ignorance towards his data protection obligations. Nevertheless, ignorance is not a legitimate excuse for breaching the Consent Obligation. Accordingly, the Respondent was found to have negligently breached the Consent Obligation in relation to both his collection and use of the Purchased Data.

Whether the Respondent breached the Notification Obligation

[5] Based on the Commission's investigations, the Purchased Data may have originated from the data breach incident involving RedMart Limited (see *Re RedMart Limited* [2022] SGPDPC 8).

19 The Commission applied the same standards set out at [18] above to its assessment of whether the Respondent breached the Notification Obligation. In this regard, the Respondent also did not perform the required due diligence to ensure that the individuals had been informed of the purposes for which their personal data was subsequently collected, used and/or disclosed by the Respondent and the Seller, and there is likewise no evidence that the Respondent contacted the individuals directly to inform them of this. The Respondent has accordingly also negligently breached the Notification Obligation in relation to both his collection and use of the Purchased Data.

The Deputy Commissioner's Decision

20 In determining whether any directions should be imposed on the Respondent under section 48I of the PDPA, and/or whether the Respondent 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, including the following mitigating factors:

Mitigating Factors

(a) The Respondent was highly cooperative during the Commission's investigations. In particular, the Respondent candidly admitted to the infringing acts at first instance and co-operated fully with the investigation process.

(b) The Respondent is a first-time offender.

21 The Commission considers that there are compelling policy reasons in favour of taking a strong stance against the unauthorised buying of personal data. Some of

these policy reasons have been enumerated in *Re Sharon Assya Qadriyah Tang* (at [30]), in the context of the unauthorised sale of personal data:

> "The Commissioner likewise takes a serious view of such breaches under the PDPA. There are strong policy reasons for taking a hard stance against the unauthorised sale of personal data. Amongst these policy reasons are the need to protect the interests of the individual and safeguard against any harm to the individual, such as identity theft or nuisance calls. Additionally, there is a need to prevent abuse by organisations in profiting from the sale of the individual's personal data at the individual's expense. It is indeed such cases of potential misuse or abuse by organisations of the individual's personal data which the PDPA seeks to safeguard against. In this regard, the Commissioner is prepared to take such stern action against organisations for the unauthorised sale of personal data."

22 Although the Commission's investigations did not disclose that the Respondent re-sold the Purchased Data, the demand generated by buyers such as the Respondent incentivises sellers to engage in the unauthorised sale of personal data, contributing to the market for the unauthorised buying and selling of personal data. There are strong policy reasons to deter would-be participants of such a market as its existence significantly increases the risk of potential misuse or abuse of personal data.

The Respondent's Representations

23 On 20 October 2023, the Respondent was notified of the Commission's Preliminary Decision, which sets out:

(a) the Commission's findings on the Respondent's breaches of the Consent Obligation and the Notification Obligation (as set out above);

(b) the Commission's intention to impose a financial penalty of S$28,000; and

(c) the Commission's intention to give certain directions on the Respondent to ensure compliance with the PDPA.

24 On 1 November 2023, the Respondent submitted written representations on the amount of the financial penalty to be imposed. These representations included the following:

(a) The Respondent stated that while he had made sure not to send any marketing SMSes to any DNC-registered contact numbers, he was unaware that using e-mail addresses for telemarketing purposes was also a violation of the PDPA;

(b) The Respondent had no malicious intentions in using the Purchased Data and was only seeking to provide for his family; and

(c) The Respondent's financial situation was extremely challenging. The financial penalty imposed would exacerbate his financial difficulties. In

particular, the Respondent stated that he was already struggling to meet his ongoing expenses, including medical expenses for a family member's treatment.

Decision

25 The Commission is unable to accept the Respondent's representations at [24(a)] and [24(b)] above:

(a) As stated at [18] above, ignorance is not a legitimate excuse for breaching the PDPA. To the Respondent's credit, he has in his representations accepted that ignorance does not excuse his actions, and stated that he had only raised this point to provide context.

(b) Notwithstanding the Respondent's personal motivations in this regard, the Respondent's actions were ultimately still done for profit, in furtherance of his business as a real estate salesperson.

Additionally, the Commission has already taken the Respondent's self-confessed ignorance about his data protection obligations and his personal motivations into account when it determined that the Respondent had negligently breached the Consent and Notification Obligations: see [18-19] above.

26 However, the Commission accepts and takes into account the Respondent's representation at [24(c)] above. When imposing financial penalties, the Commission may take into consideration the personal and financial circumstances of the organisation / individual, bearing in mind that financial penalties should not impose a

crushing burden or cause undue hardship[6]. The Commission has given due consideration to the Respondent's financial situation based on the evidence furnished by the Respondent and accepts that the imposition of a high financial penalty would cause substantial hardship to the Respondent.

27 Having considered all the relevant factors in this case, including the Respondent's representations, the Commission hereby imposes a reduced financial penalty of **S$16,800**. This decision is made on the basis of the exceptional financial circumstances demonstrated by the Respondent, and should not be taken as setting any precedent for future cases. The Commission requires the Respondent to pay the financial penalty of **S$16,800** in accordance with 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.

Directions

28 Having considered all the relevant factors of this case, including the fact that the Purchased Data is still in the Respondent's possession, the Commission also determines that the following directions should be imposed on the Respondent under section 48I of the PDPA, in order to ensure the Respondent's compliance with the Consent Obligation and the Notification Obligation:

[6] See *Re Neo Yong Xiang (trading as Yoshi Mobile)* [2021] SGPDPC 12 (at [21]).

(a) the Respondent is to cease his use of all of the Purchased Data immediately;

(b) the Respondent is to cease the retention of all of the Purchased Data within 7 days from the date of this Decision; and

(c) the Respondent is to inform the Commission within 7 days from the date of this Decision of the completion of the steps directed above.

WONG HUIWEN DENISE
DEPUTY COMMISSIONER
FOR PERSONAL DATA PROTECTION