This decision is subject to final editorial corrections approved by the tribunal and/or redaction pursuant to the publisher's duty in compliance with the law, for publication in LawNet.

Sharon Assya Qadriyah Tang

[2018] SGPDPC 1

Tan Kiat How, Commissioner — Case No DP-1701-B0485

Data Protection – Consent obligation – Individual engaged in unauthorised selling of personal data

Data Protection – Notification obligation – Individual engaged in unauthorised selling of personal data

Data Protection – Personal or domestic capacity

Data Protection – Continued disclosure of personal data collected before appointed day

11 January 2018

Background

1 This is the first reported case of an individual (the "**Respondent**") who was involved in the unauthorised selling of personal data. The facts disclose a straightforward breach of the Personal Data Protection Act 2012 ("**PDPA**"), and the Respondent does not deny committing the infringing acts. The Commissioner has accordingly found the Respondent in breach of sections 13 and 20 of the PDPA.

2 The Commissioner's findings and grounds of decision are set out below.

Material Facts

3 The Respondent was employed as a telemarketer from 2004 to 2014. Sometime in 2012, the Respondent started purchasing 'leads' to expand the reach of her marketing in order to hit her sales targets. These 'leads' typically comprised an individual's name, NRIC number, mobile number and annual income range. A lead would typically cost between $0.20 and $0.30.

4 The Respondent bought the leads from unknown online sellers and did not retain the details of these transactions. Also, the Respondent did not check or verify with the sellers that the leads she purchased were obtained legitimately with the individuals' consent.

5 On average, the Respondent would buy approximately 10,000 leads per year. According to the Respondent, her first purchase of leads was sometime in late 2012 and her last purchase was sometime in either May or June 2014. At the material time, the Respondent had in her possession approximately 30,990 leads. The leads were stored in Microsoft Excel spreadsheets.

6 From late 2012 up until 23 February 2017, the Respondent estimated that she had re-sold the leads she had bought about 9 to 10 times, typically charging customers between $0.05 to $0.20 per lead, depending on the number they purchased. The Respondent would advertise the sale of the leads on various websites, and customers who wished to buy the leads would make payment to the Respondent via a bank transfer. While conducting these transactions, the Respondent concealed her true identity by using an alias (with a corresponding email address), her husband's bank account number, and a mobile phone number registered under her friend's name. The Respondent estimated she had made a profit of $5,000 from selling these leads. The Respondent explained that she had decided to re-sell the leads as a side-line to supplement her income.

During this period of time, the Respondent was concurrently holding a job as a telemarketer and engaging in an apparel business.

Findings and Basis for Determination

7 The following two main issues were canvassed from the facts for the Commissioner's determination:

(a) whether the Respondent was an "organisation" subject to the Data Protection Provisions of the PDPA; and

(b) whether the Respondent's sale and purchase of leads complied with the Consent and Notification Obligations under the PDPA.

8 As a preliminary point, it was not disputed that the 30,990 leads in the Respondent's possession, each of which comprised an individual's name, NRIC number, mobile number and annual income range, fell within the definition of "personal data" under section 2(1) of the PDPA as it was clearly possible to identify an individual from that data.

(a) Whether the Respondent was an "organisation" subject to the Data Protection Provisions of the PDPA

9 The Commissioner first determined whether the Respondent was acting as an "organisation" for the purposes of the PDPA. This is a pertinent issue in this case, because the Respondent is an individual, and the Data Protection Provisions[1] are only applicable to an "organisation" under the PDPA. Although

[1] As borne out by Parts III to VI of the PDPA.

(*cont'd on next page*)

the PDPA defines "organisation" broadly to include individuals,[2] an individual is expressly excluded from the Data Protection Provisions in the PDPA if the individual was acting in a personal or domestic capacity.[3] 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.

11 In earlier cases, the Commissioner had also found individuals, namely, a registered salesperson[4] and a financial consultant[5], to come within the definition of an "organisation" under the PDPA. In those cases, the individuals had been carrying out data processing activities for work or business purposes, and were thus not acting in a personal or domestic capacity.

---

2 Section 2(1) of the PDPA.

3 Under section 4(1)(a) of the PDPA.

4 *Re Chua Yong Boon Justin* [2016] SGPDPC 13.

5 *Re Ang Rui Song* [2017] SGPDPC 13.

12 Given the above, the Respondent is as an "organisation" for the purposes of the PDPA, and subject to the Data Protection Provisions.

(b) Whether the Respondent's sale and purchase of leads complied with the Consent and Notification Obligations under the PDPA

(i) The Respondent's buying and selling of leads were activities that fell under the scope of the PDPA

13 The PDPA governs the collection, use and disclosure of personal data by organisations. Given that the leads which the Respondent had purchased or sold comprised of personal data of individuals, these were activities that fell under the scope of the PDPA. In respect of the purchase of leads by the Respondent, in which the Respondent *acquired* personal data from the seller of the transaction, this amounted to a "collection" of personal data under the PDPA by the Respondent. In respect of the sale of leads by the Respondent, in which the Respondent *provided* personal data to the buyer of the transaction, this amounted to a "disclosure" of personal data under the PDPA by the Respondent.

14 The relevant obligations under the PDPA that apply to the facts of this case are the Consent and Notification Obligations. The Notification Obligation requires an organisation to inform individuals of the purposes for the collection, use and disclosure of personal data, while the Consent Obligation requires the organisation to obtain consent from the individual for such purposes of the collection, use and disclosure. The appropriate provisions of the Notification and Consent Obligations are found in the Data Protection Provisions of the PDPA at sections 13 to 15 and 20 respectively.

(ii) The Respondent was not subject to the Data Protection Provisions in respect of the purchase and sale of personal data before the Appointed Day

15 According to the Respondent, she was first involved in the buying and selling of leads since 2012 to support her work as a telemarketer.

16 However, the Data Protection Provisions of the PDPA only came into effect on 2 July 2014 (the "**Appointed Day**"). This means that during the period before the Appointed Day, the Respondent was not subject to or required to comply with the Data Protection Provisions of the PDPA in respect of the collection, use and disclosure of the personal data found in the database of leads.

17 Notwithstanding, after the Appointed Day when the Data Protection Provisions came into force, the Respondent was subject to the obligations under the Data Protection Provisions in respect of both the *existing* personal data held in the Respondent's possession or control, and any *new* personal data that the Respondent may come into possession or control with. The Respondent was therefore obliged to take steps to comply with the Data Protection Provisions in respect of both these sets of data. This includes obtaining consent from the individuals for the use of the personal data for a new purpose, which the individuals had previously not consented to, as it falls outside the purposes for which the personal data was originally collected under section 19 of the PDPA (as will be elaborated on below).

18 This was a position that was taken in *Re Social Metric Pte Ltd* [2017] SGPDPC 17. In that case, Social Metric had processed personal data for its clients' social marketing campaigns all the way back before the Appointed Day. The Commissioner took the position that before the Appointed Day, Social Metric was not required to put in place reasonable security arrangements under section 24 of the PDPA to protect the personal data in its possession or under

its control. However, when the Data Protection Provisions came into force after the Appointed Day, Social Metric needed to put in place such security arrangements to protect both the existing and new personal data.

(iii) Grandfathering provision may apply to the continued use but not sale of personal data

19 As the Respondent had been purchasing and selling personal data since 2012, and before the Appointed Day, the question is whether the Respondent can rely on the "grandfathering" provision under section 19 of the PDPA to continue to *use* or *sell* (ie disclose) such personal data to third parties after the Appointed Day. It should be noted that Respondent cannot continue to *purchase* or collect personal data after the Appointed Day, as the Data Protection Provisions would have kicked in on the Appointed Day, and would require the Respondent to provide notification to, and obtain consent from, the individuals pursuant to the Consent and Notification Obligations (unless an exception applies).

20 The grandfathering provision provides that organisations may continue to *use* personal data that they have collected before the Appointed Day, for the purposes for which the personal data was collected, unless consent is withdrawn or the individual gives an indication that there is no such consent.

21 In respect of the personal data that was purchased or obtained before the Appointed Day, it may be possible for an organisation to continue using the personal data if such use falls within the purposes of collection, such as for its own reasonable use (ie telemarketing purposes), provided that there was no indication that the individual did not consent to the continued use. This is a position that the PDPC articulated in its Advisory Guidelines on Key Concepts

in the PDPA ("**Advisory Guidelines**"), of which an extract of the relevant parts is set out below:[6]

> The effect of section 19 is that organisations can continue to use personal data collected before the appointed day for the same purposes for which the personal data was collected without obtaining fresh consent, unless the individual has withdrawn consent (whether before on, or after the appointed day). Organisations should note that section 19 only applies to 'reasonable existing uses' of personal data collected before the appointed day.
>
> For the avoidance of doubt, the purpose of telemarketing (i.e. sending a specified message to a Singapore telephone number) could be a reasonable existing use.

22 However, in this case, the Respondent went beyond using the personal data for her own telemarketing purposes, and proceeded to sell personal data to third parties. The "grandfathering" provision only permits the continued "use" of personal data for the purposes for which the personal data was collected. Such "use" does not extend to "disclosure" of personal data unless, as set out at paragraph 23.1 of the Advisory Guidelines, the disclosure "is necessarily part of the organisation's use of such personal data". In the case of the sale of personal data, the disclosure of personal data is the main activity being carried out, and is not incidental to any of the organisation's own uses of the personal data. Thus, it is not a disclosure "that is necessarily part of the organisation's use of such personal data". The PDPC has stated this position in its Advisory Guidelines as an example:[7]

> Organisation XYZ has been selling databases containing personal data. <u>This would be considered a disclosure of personal data and not a reasonable existing use under section</u>

---

6 PDPC, Advisory Guidelines on Key Concepts in the PDPA (revised 27 July 2017) at [23.3]-[23.4].

7 PDPC, Advisory Guidelines on Key Concepts in the PDPA (revised 27 July 2017) at [23.6].

> 19. After the appointed day, XYZ needs to ensure that consent has been obtained before selling these databases again.
>
> [Emphasis added.]

23 Consequently, the grandfathering provision would not apply to the instances where the Respondent had been selling personal data before the Appointed Day, and continued to sell personal data after the Appointed Day. In respect of personal data that was not sold before the Appointed Day, it is all the more so that the Respondent cannot rely on the grandfathering provision, because there was never an existing practice of selling the personal data in the first place, and hence there is no "use" to be carried on in respect of the personal data.

(iv) The Respondent's sale of leads comprising of personal data after Appointed Day was a serious contravention of the PDPA

24 During the investigations, the Commissioner found no evidence that the Respondent had continued to purchase leads from the online sources after the Appointed Day. However, there was clear evidence that the Respondent was still selling leads after the Appointed Day. In respect of the Respondent's sale of such leads, the Commissioner finds that there was a clear breach of the Consent and Notification Obligations under the PDPA.

25 When questioned about the sale of personal data, the Respondent admitted that she did not obtain consent from the individuals for the sale of their personal data to third parties. The Respondent also admitted that she did not check or verify with the online sellers if they had obtained consent from the individuals to the selling of their personal data. Similarly, the Respondent had also admitted that she did not provide any notification to the individuals of the sale of their personal data. The Commissioner also carried out further investigations and separately contacted several individuals whose personal data

were found in the database of leads, and all of them confirmed that they had not consented to their personal data to be disclosed or sold.

26 Accordingly, on the evidence that the individuals had not been informed of the sale of their personal data nor did they provide consent to the sale of their personal data, the Respondent is in breach of both the Consent and Notification Obligations under the PDPA.

27 The sale of personal data in contravention of the PDPA is a serious breach of the PDPA. In the UK, data selling is expressly prohibited by legislation. Section 55 of the Data Protection Act 1998 ("**DPA**") provides that it is an offence for any person who (a) knowingly or recklessly, without the consent of the data controller, obtains or discloses personal data or procures such disclosure, or (b) sells or offers to sell the personal data so obtained. Specifically, section 55(6) of the DPA clarifies that "*an advertisement indicating that personal data are or may be for sale is an offer to sell the personal data*".[8] In this regard, both the advertisement of the sale of personal data, and the actual sale of personal data carried out, would constitute an offence under the DPA.

28 The UK's Information Commissioner's Office ("**ICO**") has recently found a data broker to be in breached of the DPA for obtaining customer data from various sources and selling the data to third party organisations for the purposes of direct marketing. The individuals whose data was traded by the data broker were not informed that their personal data would be disclosed to the data

---

[8] UK, Data Protection Act 1998 <https://www.legislation.gov.uk/ukpga/1998/29/section/55>.

(*cont'd on next page*)

broker, or the organisations to which the data broker sold the data on to, for the purpose of sending direct marketing text messages. In total, the ICO found that there were 580,302 records containing personal data that were disclosed without the data subjects' knowledge or consent.[9] In terms of the harm, the ICO stated that "*the unlawful trade in personal data [led] directly to the wholescale sending of unsolicited direct marketing texts and the making of nuisance calls*", and was satisfied that the "*cumulative amount of distress suffered by the large numbers of individuals affected, coupled with the distress suffered by some individuals, means that overall the level was substantial*".[10] As such, the data broker was found to be in breach of the DPA and was issued a monetary penalty of £20,000.

29 In Hong Kong, the Office of the Privacy Commissioner for Personal Data ("**PCPD**") found that the Octopus group of companies ("**Octopus Group**"), which provides an extensive smartcard payment system for transport and other services, had contravened the requirements of the Personal Data (Privacy) Ordinance (Cap. 486) by entering into contracts with several business partners to sell its members' personal data without their consent.[11] In that case, the Octopus Group had failed to inform individuals registering for its rewards programme that one of the purposes was the sale of their personal data for

---

9 UK, ICO, Monetary Penalty Notice: The Data Supply Company Ltd (27 January 2017) <https://ico.org.uk/action-weve-taken/enforcement/the-data-supply-company-ltd/> at [26], [29].

10 UK, ICO, *Monetary Penalty Notice: The Data Supply Company Ltd* (27 January 2017) <https://ico.org.uk/action-weve-taken/enforcement/the-data-supply-company-ltd/> at [32]-[34].

11 H.K., PCPD, *The Collection and Use of Personal Data of Members under the Octopus Rewards Programme run by Octopus Rewards Limited*, Report Number R10-9866 <https://www.pcpd.org.hk/english/enforcement/commissioners_findings/investigation_reports/files/R10_9866_e.pdf>.

(*cont'd on next page*)

monetary gain. This purpose was neither expressly stated in the terms and conditions on the member's registration form, nor could it be said to be a purpose of use within the reasonable expectation of the individuals.[12] In this regard, despite providing their signature on the registration form, the individuals could not be said to have consented to the data selling. It should be noted that the Hong Kong case had a widespread impact, eventually becoming the catalyst for amendments to the data protection law in Hong Kong.

30 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.[13] In this regard, the Commissioner is prepared to take such stern action against organisations for the unauthorised sale of personal data.

Enforcement Action

31 Given that the Commissioner has found the Respondent to be in breach of sections 13 and 20 of the PDPA, the Commissioner is empowered under section 29 of the PDPA to give the Respondent such directions as it deems fit

---

12 *Ibid*.at [3.36] and [3.40].

13 Sing., *Parliamentary Debates*, vol. 89 (15 October 2012) (Assoc Prof Dr Yaacob Ibrahim) at p. 1: "*The personal data protection law will safeguard individuals' personal data against misuse by regulating the proper management of personal data*".

to ensure the Respondent's compliance with the PDPA. This may include directing the Respondent to pay a financial penalty of such amount not exceeding S$1 million as the Commissioner thinks fit.

32 In assessing the breach and determining the directions to be imposed to the Respondent, the Commissioner took into account the following aggravating factors:

(a) the database of leads included personal data of a sensitive nature, i.e. NRIC numbers and salary ranges of individuals;

(b) the Respondent had used means to obscure her identity when she was selling the leads, which is indicative of a guilty conscience and of a premeditated and deliberate contravention of the PDPA; and

(c) as elaborated above at paragraph 30, the profiteering from the sales of personal data by organisations at the expense of consumer or individuals is the very kind of activity which the PDPA seeks to curb, and hence, must be severely dealt with.

33 In relation to the mitigating factors of this case, the Commissioner took into account the fact that the Respondent had candidly admitted to the wrongdoing at the first instance, and co-operated fully with investigations. Additionally, the Respondent was fully cooperative with the Commissioner's investigations and was helpful in providing evidence of the matter.

34 Crucially, the Commissioner also considered the special financial circumstances of the Respondent in determining a suitable amount of financial penalty to impose on the Respondent. During the course of investigation, the Commissioner learnt that the Respondent and her husband were of limited

financial means and were earning modest salaries, and had a child and family to support. In the Commission's assessment, imposing a high financial penalty on the Respondent would likely place a crushing burden on the Respondent and her family in the circumstances and cause undue hardship.

35 From the evidence, the cumulative amount of payment received by the Respondent from the sale of the leads was unlikely to exceed $5,000, and this was based on a conservative estimate. In addition, the investigation showed that the Respondent was not carrying out the sale and purchase of personal data on a large-scale basis, but was simply conducting these activities opportunistically and on the side to supplement her income.

36 Accordingly, taking into account all relevant factors of this case, and given the special financial circumstances that the Respondent is in, the Commissioner has decided to adjust the amount of financial penalty to an amount which would adequately reflect the seriousness of the breach of the PDPA, but at the same time not impose a crushing burden on the Respondent or her family.

37 Although the Commissioner has imposed a lower financial penalty in this case, this is exceptional and should not be taken as setting any precedent for the extension of the same leniency or indulgences in other cases. The Commissioner wishes to remind organisations of their obligations under the PDPA and that it takes a serious view towards any unauthorised sale of personal data.

38 The Commissioner hereby directs the Respondent to pay a financial penalty of S$6,000 within 30 days from the date of the Commissioner's direction.

YEONG ZEE KIN
DEPUTY COMMISSIONER
FOR COMMISSIONER FOR PERSONAL DATA PROTECTION
