Data Protection Quarterly Updates (January – March 2024)

The Personal Data Protection Commission (**PDPC**) published five decisions between January and March 2024 after concluding the following investigations:

(a) One investigation relating to the Consent and Purpose Limitation Obligations under the Personal Data Protection Act 2012 (**PDPA**);

(b) Two investigations relating to the Protection Obligation under the PDPA;

(c) One investigation relating to the Consent and Notification Obligations under the PDPA; and

(d) One investigation relating to a breach of the Do-Not-Call (**DNC**) provisions under the PDPA.

The following table summarises the directions imposed in each of the decisions:

Name of decision	Relevant Obligation(s)	Decision and directions imposed
Lee Chee Meng [2023] SGPDPC 14	Consent Obligation and Notification Obligation	Financial penalty of S$16,800 imposed. Directions issued: (a) Cease use of all purchased data immediately; and (b) Cease retention of all puchased data within seven days.
Carousell Pte Ltd [2023] SGPDPC 13	Protection Obligation	Financial penalty of S$58,000 imposed. Directions issued: (a) Review procedures on software testing; (b) Review processes and procedures for documenting of functional and technical specifications of software; and (c) Rectify any gaps identified and furnish the PDPC with a report.
Koh Wei Ming @ Muhammad Amin Koh (trading as Mobile Chat) [2023] SGPDPC 11	Consent Obligation and Purpose Limitation Obligation	Financial penalty of S$48,000 imposed.
Whiz Communications [2023] SGPDPCS 7	Protection Obligation	Financial penalty of S$9,000 imposed.

Lin DaoWen Kenny [2023] SGPDPC 6	DNC provisions	Warning administered to a financial advisor for: (a) Using dictionary attack methods to generate telephone numbers; (b) Failing to obtain clear and umambiguous consent; and (c) Failing to check the DNC Register, before making marketing calls to DNC-registered individuals.

We outline below some decisions of interest relating to the enforcement of the Consent, Notification and Purpose Limitation Obligations, as well as the DNC provisions, under the PDPA.

***Koh Wei Ming @ Muhammad Amin Koh (trading as Mobile Chat)* [2023] SGPDPC 11**

Comments

This decision is salient for being the second case to be investigated by the PDPC involving the egregious misuse of personal data to undertake illicit activities. Notwithstanding the representations made by the perpetrator, including, among others, that he was the sole breadwinner of his family, the PDPC imposed a financial penalty of S$48,000 on him. This decision emphasises the PDPC's zero tolerance for such flagrant misuse of personal data and the deterrent penalties that may be imposed.

Facts

Koh Wei Ming @ Muhammad Amin Koh (**KWM**) was the sole proprietor of Mobile Chat (**Organisation**), a retailer of prepaid SIM cards and mobile phones, among others. As part of the SIM card registration process, KWM would scan a customer's identity document (e.g., identity card, passport, work pass etc.) using an M1 Terminal Device issued by the telecommunications company to verify whether the customer had a maximum of three prepaid SIM cards.

Between February 2020 to September 2021, the PDPC received 1,391 complaints from members of the public who, despite having their numbers registered with the DNC Register, received marketing messages. The messages were traced to 95 prepaid SIM cards purchased from KWM.

Upon investigation, the PDPC discovered that KWM had exploited the registration process by scanning the customer's identity document a second time to create a second SIM card. Occasionally, KWM would also keep SIM cards from registrations which should have been cancelled or reversed, e.g., where customers did not want to continue with their purchases after learning that the credit value of the SIM card would have to be separately loaded. These actions were done without the customer's knowledge and consent. KWM then sold the preregistered SIM cards to anonymous and unauthorised purchasers, netting a profit of around S$35,000 over four years.

While 73 customers' personal data (name, addresses and NRIC/FIN/passport numbers) had been used to register 95 SIM cards, the PDPC estimated that it was likely that the personal data of more than approximately 1,000 individuals had been similarly affected based on KWM's admission that he had sold an average of 250 prepaid SIM cards annually over four years.

Decision

Whether KWM was an "organisation" under the PDPA

Prior to determining whether there was a breach of the PDPA obligations, the PDPC considered the threshold question of whether KWM, as an individual, fell within the ambit of the PDPA, in particular, section 2(1) of the PPDA. Under section 2(1) of the PDPA, an "organisation" includes "any individual, company, association or body of persons, corporate or unincorporated". Given that the Organisation was a sole proprietorship without separate legal personality from KWM, and KWM was acting in a business capacity in selling the illicit SIM cards for a profit, the PDPC found that KWM was an organisation for the purposes of the PDPA.

Consent Obligation

Pursuant to section 13 of the PDPA (i.e., Consent Obligation), 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 PDPC held that KWM had breached the Consent Obligation as KWM's customers had not provided consent for KWM to use their personal data for purposes other than registering the number of SIM card(s) they had requested. Further, where customers had withdrawn their consent to use their personal data (i.e., when they discovered that the credit value of the SIM card would have to be separately loaded), KWM should have cancelled the SIM card registrations instead of retaining the registered SIM cards and activating them for purposes that the customers had not consented to.

Purpose Limitation Obligation

Pursuant to section 18 of the PDPA (i.e., Purpose Limitation Obligation), an organisation may collect, use or disclose an individual's personal data only for purposes that a reasonable person would consider appropriate in the circumstances, and where that individual has been informed of those purposes under section 20 of the PDPA.

In light of KWM's admission that the purpose of using his customers' personal data was to register illicit SIM cards for sale to third parties for a profit, the PDPC found that such use of personal data was not for a reasonable purpose. This was because 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. As such, the PDPC held that KWM had breached the Purpose Limitation Obligation.

Aggravating and mitigating factors

In determining whether to impose a financial penalty on KWM and the quantum of such financial penalty, the PDPC took into account various aggravating factors, including the fact that KWM's breaches of the PDPA:

(a) 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;

(b) Were intentional and had taken place over a long period of four years;

(c) Had caused inconvenience to innocent parties as the illicit SIM cards sold were used to send unsolicited messages to phone numbers registered with the DNC Register; and

(d) Enabled KWM to gain financially approximately S$35,000.

The sole mitigating factor was KWM's early admission of liability which had reduced the time and resources expended on investigations.

The PDPC also considered but ultimately rejected certain representations made by KWM including, among others, that he was the sole breadwinner and was seeking treatment for mental health issues. This was because KWM had failed to substantiate his representations of personal and

financial hardship, the conditions he was seeking mental health treatment for and how such conditions related to his breaches of the PDPA.

Taking into consideration all the foregoing circumstances, the PDPC imposed a financial penalty of S$48,000 on KWM.

A copy of this decision may be accessed here.

***Carousell Pte Ltd* [2023] SGPDPC 13**

Comments

This decision is significant due to the large number (more than 2.6 million) of individuals impacted by two data breach incidents affecting the same organisation. This decision demonstrates the importance of comprehensive pre-launch testing with a properly scoped code review to detect bugs and gaps in an application prior to it going "live". In addition, this decision serves as a timely reminder to organisations to maintain reliable documentation on functional and technical specifications to keep track of issues and provide context to historical changes on applications as this would be crucial when new personnel are employed to work on such applications.

Facts

Carousell Pte. Ltd. (**Carousell**) runs an online marketplace website and mobile application. In 2022, Carousell notified the PDPC of two separate data breach incidents (**Incidents**).

The first incident (**1st Incident**) involved the unauthorised disclosure of the personal data of 44,777 Carousell users in Singapore, Malaysia, Indonesia, Taiwan, and the Philippines. On 13 July 2022, Carousell made changes to the chat function intended for guest users and registered users in the Philippines to respond to property listings. Where users had provided prior consent, their first names (applicable to guest users), e-mail addresses and telephone numbers would be automatically appended to the message sent to the owner of the property listing. However, the chat function unintentionally disclosed the e-mail addresses and names of guest users to listing owners in *all* categories in *all* markets (**July 2022 Bug**). The telephone numbers of guest users in the Philippines were also appended to the messages. Having not identified the July 2022 Bug, Carousell attempted to fix an unrelated issue with the pre-fill functionality of the chat function on 18 August 2022 (**August 2022 Bug**). However, these changes resulted in the chat function automatically appending the e-mail addresses and names of registered users to messages to listing owners in *all* categories in *all* markets, consequently expanding the effect of the July 2022 Bug. The telephone numbers of registered and guest users in the Philippines were also appended. Carousell eventually resolved both the July and August 2022 Bugs after it was made aware of the August 2022 Bug *via* a user report.

In September 2022, Carousell implemented several remedial actions to mitigate the effects of the 1st Incident and prevent its recurrence. These remedial actions included, among others, deleting all affected personal data disclosed, notifying users who had written to Carousell about the 1st Incident, and implementing an automated unit test which automatically runs on every build of the platform to ensure that the platform did not erroneously append any personal data in chat messages.

In the second incident (**2nd Incident**), Carousell launched a public-facing Application Programming Interface (**API**) during a system migration process but inadvertently omitted to apply a filter to the API. This resulted in a vulnerability which was exploited by a threat actor who scraped the accounts of users to access and sell the personal data (user names, names and profile images) of at least 2.6 million Carousell users. The API was originally intended to retrieve the personal data of users (**Following/Follower Users**) followed by or following a particular Carousell user (**Subject User**). However, Carousell inadvertently omitted a filter which would have ensured that only publicly available personal data of the Following/Follower Users (e.g., user names, names and profile images) would be

called up. As such, the API was able to call up non-public personal data of Following/Follower Users (e.g., e-mail addresses, telephone numbers and dates of birth).

Following the 2nd Incident, Carousell implemented several remedial actions to mitigate the effects of the 2nd Incident and prevent its recurrence. These remedial actions included notifying all affected users by e-mail, deploying a fix to resolve the issue with the API and conducting a security audit for all existing APIs and implementing a systemic regular audit.

Decision

Protection Obligation

Pursuant to section 24 of the PDPA (i.e., Protection Obligation), an organisation is required to protect personal data in its possession or under its control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks.

The PDPC found that Carousell had negligently breached the Protection Obligation in both incidents by failing to conduct adequately scoped pre-launch testing and failing to adequately document functional and technical specifications of its software.

Regarding the 1st Incident, Carousell's pre-launch testing was limited to registered users in a specific category of listings (i.e., property listings in the Philippines market). The PDPC held that Carousell should have expanded testing to assess how changes to the chat function would affect categories *other than property listings* in the Philippines market. Reasonable code reviews and testing would have detected the July 2022 and August 2022 Bugs before the changes went "live". Regarding the 2nd Incident, Carousell had selectively performed code reviews and tests only for certain purposes and on certain APIs. As the function of the API in the 2nd Incident was to retrieve personal data, the PDPC held that Carousell should have identified this specific API and tested the same for data security risks.

In light of the Incidents, the PDPC stressed the importance of pre-launch testing with a properly scoped code review. Notably, PDPC's Handbook on How to Guard Against Common Types of Data Breaches (**PDPC Handbook**) provides that "organisations should ensure that applications are subjected to comprehensive testing, such as unit testing, regression testing, security tests, and User Acceptance Testing before deployment". Further, the PDPC Checklist to Guard Against Common Data Breaches (**PDPC Checklist**) recommends carrying out a test suite encompassing functional and non-functional requirements and security testing.

The PDPC also stressed the importance of "maintaining reliable documentation on functional and technical specifications" as this helps an organisation to keep track of issues over time and provide context to historical changes which would be important when new personnel are employed to take over work on an application. In relation to the 1st Incident, the PDPC found that poor employee handover processes and a lack of proper documentation had contributed to the error which resulted in the data breaches. The engineer who had implemented the changes to the chat function was not the original author of the function and did not have the context necessary to know that such changes would affect messages regarding other users and listing categories. As for the 2nd Incident, the APIs involved in the system migration were built in 2016 and did not have proper documentation to inform personnel of the need to apply a filter to the relevant API post-migration.

In determining whether to impose a financial penalty on Carousell and the quantum of such financial penalty, the PDPC took into account the following mitigating factors, with the first being the most significant:

(a) Carousell had voluntarily admitted liability early;

(b) Carousell was cooperative with the PDPC;

(c) Carousell had taken prompt and effective remediation actions upon discovery of the July 2022 and August 2022 Bugs;

(d) Carousell has not previously contravened the PDPA;

(e) Prior to the 2nd Incident, Carousell had put in place API processes and security measures (e.g., rate-limiting and traffic monitoring against API vulnerabilities); and

(f) The threat actor in the 2nd Incident was particularly sophisticated in avoiding security measures implemented by Carousell which were found to be adequate.

Taking into consideration these mitigating factors, the PDPC imposed a financial penalty of S$58,000 on Carousell. The PDPC also directed Carousell to review its internal procedures on software testing and processes for documenting functional and technical specifications, rectify any gaps identified from these reviews, and furnish the PDPC with a report within 90 days.

A copy of this decision may be accessed here.

***Lee Chee Meng* [2023] SGPDPC 14**

Comments

This decision serves as a timely reminder that any indirect collection of personal data by data buyers does not exempt them from their data protection obligations in relation to the collection or subsequent use or disclosure of the collected personal data. This decision also reiterates the standard required of data controllers who buy marketing lists from third parties, in particular, that such data controllers must perform rigorous checks to satisfy themselves that the third parties obtained the personal data fairly and lawfully.

Facts

Lee Chee Meng (**Respondent**) was a registered salesperson under the Estate Agents Act 2010 and appointed by ERA Realty Network Pte Ltd (**ERA**) as an independent agent who received commissions for real estate services or transactions between customers and ERA.

In 2021, the Respondent purchased for S$1,200 from an unknown seller (**Seller**) five sets of personal data comprising about 420,000 records (**Purchased Data**) which included names, e-mail addresses, contact numbers, addresses (either residential or office) and, in some cases, the last four digits of credit card numbers. After receiving the Purchased Data (in the form of Microsoft Excel spreadsheets), the Respondent first checked the contact numbers against the DNC Register and subsequently used the personal data to send targeted marketing e-mails and SMSes to individuals whose contact numbers were not registered with the DNC Register. 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 property transaction prices in that area if the individual's contact number was not registered with the DNC Register. The Respondent did not send marketing communications to all affected individuals as only about 75% of the Purchased Data contained business-related information and not residential information.

The Respondent claimed that he did not use the Purchased Data for any other purpose, and that he had included an unsubscribe function in his marketing e-mails so that he could delete the personal data of any individual who unsubscribed.

On 8 November 2022, the PDPC received a complaint regarding the possible unauthorised collection and use of personal data by the Respondent for telemarketing purposes.

Decision

Whether the Respondent was an "organisation" under the PDPA

Prior to determining whether there was a breach of the PDPA obligations, the PDPC considered the threshold question of whether the Respondent (as an individual) had operated as an "organisation" in respect of his collection and use of the Purchased Data. Given that the Respondent: (a) had acted in the furtherance of his business as a real estate salesperson and not in a personal or domestic capacity; and (b) was not in an employee-employer relationship with ERA but was an independent agent, the PDPC found that the Respondent had operated as an "organisation" under the PDPA.

Consent Obligation

Pursuant to section 13 of the PDPA (i.e., Consent Obligation), 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. Under the Consent Obligation, 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.

The PDPC held that the Respondent had 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. The Respondent had also admitted that he did not know whether the Seller had obtained the individuals' consent 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. Further, the Respondent was not aware of whether the Purchased Data had originated from any data breaches.

The fact that the Respondent had purchased the Purchased Data from a third party (i.e., the Seller) did not derogate from the PDPC's breach finding. The PDPC cited past decisions which held that the purchase of personal data from third party sellers would constitute the collection of personal data under the PDPA, despite the fact that such personal data had not been collected directly from the individuals concerned. Such "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 standard required of data controllers buying marketing lists from third parties is that they "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 buying in lists "must check how and when consent was obtained, by whom and what the customer was told" as it is "not acceptable to rely on assurances of indirect consent without undertaking proper due diligence". Such due diligences checks could include, among others, checking how and when consent had been obtained, who had obtained such consent and the context in which consent had been obtained.

The PDPC had accepted that the Respondent had provided an opt-out option in his telemarketing e-mails, taken pains to ensure compliance with the DNC provisions under the PDPC and had breached the PDPA out of ignorance of his data protection obligations. Nonetheless, the PDPC held that ignorance was not a legitimate excuse for breaching the Consent Obligation.

Notification Obligation

Pursuant to section 20 of the PDPA (i.e., Notification Obligation), organisations should, prior to collecting, using or disclosing personal data, inform the individual(s) in question of the purposes for which such personal data is being collected, used or disclosed.

Applying the same standards set out above, the PDPC held that the Respondent had breached the Notification Obligation as he had not performed the required due diligence to ensure that individuals had been informed of the purposes for which their personal data was subsequently collected, used and disclosed by the Respondent and the Seller.

In determining whether any directions should be imposed on the Respondent and whether the Respondent should pay a financial penalty, the PDPC took into account the following mitigating factors:

(a) The Respondent was highly cooperative during the PDPC's investigations and had candidly admitted the infringing acts at first instance;

(b) The Respondent was a first-time offender; and

(c) The Respondent's financial situation was extremely challenging as he was struggling to meet his ongoing expenses, including medical expenses for a family member's treatment.

The PDPC also observed that there are compelling policy reasons in favour of taking a strong stance against the unauthorised buying of personal data, including the need to protect the interests of the individual and safeguard against any harm such as identity theft or nuisance calls, and the need to prevent abuse by organisations in profiting from the sale of the individual's personal data at the individual's expense.

In light of the above, the PDPC imposed a reduced financial penalty of S$16,800 but stressed that the reduced financial penalty was due to the exceptional financial circumstances demonstrated by the Respondent and should not be taken as setting any precedent for future cases.

The PDPC also directed the Respondent to:

(a) Cease his use of all Purchased Data immediately;

(b) Cease the retention of all Purchased Data within seven days from the date of the PDPC's decision; and

(c) Inform the PDPC of the completion of the foregoing steps within seven days from the date of the PDPC's decision.

A copy of this decision may be accessed here.

If you would like information or assistance on the above or any other area of law, you may wish to contact the Partner at WongPartnership whom you normally work with or any of the following Partners:

LAM Chung Nian
Head – Intellectual Property, Technology & Data
d: +65 6416 8271
e: chungnian.lam@wongpartnership.com
Click here to view Chung Nian's CV.

Kylie PEH
Partner – Intellectual Property, Technology & Data
d: +65 6416 8259
e: kylie.peh@wongpartnership.com
Click here to view Kylie's CV.

Connect with WongPartnership.

WPG MEMBERS AND OFFICES

- contactus@wongpartnership.com

SINGAPORE

-
WongPartnership LLP
12 Marina Boulevard Level 28
Marina Bay Financial Centre Tower 3
Singapore 018982
t +65 6416 8000
f +65 6532 5711/5722

CHINA

-
WongPartnership LLP
Shanghai Representative Office
Unit 1015 Link Square 1
222 Hubin Road
Shanghai 200021, PRC
t +86 21 6340 3131
f +86 21 6340 3315

INDONESIA

-
Makes & Partners Law Firm
Menara Batavia, 7th Floor
Jl. KH. Mas Mansyur Kav. 126
Jakarta 10220, Indonesia
t +62 21 574 7181
f +62 21 574 7180
w makeslaw.com

MALAYSIA

-
Foong & Partners
Advocates & Solicitors
13-1, Menara 1MK, Kompleks 1 Mont' Kiara
No 1 Jalan Kiara, Mont' Kiara
50480 Kuala Lumpur, Malaysia
t +60 3 6419 0822
f +60 3 6419 0823
w foongpartners.com

MIDDLE EAST

-
Al Aidarous Advocates and Legal Consultants
Abdullah Al Mulla Building, Mezzanine Suite 02
39 Hameem Street (side street of Al Murroor Street)
Al Nahyan Camp Area
P.O. Box No. 71284
Abu Dhabi, UAE
t +971 2 6439 222
f +971 2 6349 229
w aidarous.com

-
Al Aidarous Advocates and Legal Consultants
Oberoi Centre, 13th Floor, Marasi Drive, Business Bay
P.O. Box No. 33299
Dubai, UAE
t +971 4 2828 000
f +971 4 2828 011

PHILIPPINES

-
Gruba Law
27/F 88 Corporate Center
141 Valero St., Salcedo Village
Makati City 1227, Philippines
t +63 2 889 6060
f +63 2 889 6066
w grubalaw.com

wongpartnership.com