Data Protection Quarterly Updates (January – March 2022)

The Personal Data Protection Commission ("**PDPC**") published a total of four decisions between January to March 2022 relating to the Protection Obligation, the Accountability Obligation, the Consent Obligation, as well as the Purpose Limitation Obligation (each term as defined below) under the Personal Data Protection Act ("**PDPA**"), as summarised in the table below:

Name of decision	Obligation(s) breached	Directions imposed
Nature Society (Singapore)	Protection and Accountability Obligations	Financial penalty - $14,000
North London Collegiate School (Singapore) Pte. Ltd.	Protection Obligation	Financial penalty - $10,000
Tanah Merah Country Club	Protection Obligation	Financial penalty - $4,000
Neo Yong Xiang (trading as Yoshi Mobile) [2021] SGPDPC 12	Consent and Purpose Limitation Obligations	Financial penalty - $21,000

We outline below some decisions of interest relating to the enforcement of the Protection Obligation, Accountability Obligation, Consent Obligation and Purpose Limitation Obligation.

Nature Society (Singapore)

Comments

Under Section 24 of the PDPA, organisations are required to protect personal data in their possession or under their control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification or disposal, or similar risks, and the loss of any storage medium or device on which personal data is stored ("**Protection Obligation**").

As highlighted in this decision, in developing and establishing a website which may collect, use, disclose and/or store the personal data of its users, an organisation must ensure that reasonable security arrangements are in place to protect such personal data, such as conducting necessary security updates, patches and penetration tests on a regular basis. Where the organisation chooses to engage an external vendor or service provider to establish and maintain the security of its website, it

should ensure that the vendor or service provider is capable of providing the requisite standard of website and information technology security to satisfy the Protection Obligation.

Facts

On 6 November 2020, the PDPC received information on hacked databases being made available for download on various hacking forums and Telegram channels. Nature Society (Singapore) ("**NSS**") was one of the organisations affected by this hacking incident.

The personal data of 5,131 members and non-members who had created membership and user accounts on NSS' website which was accessed and extracted by unauthorised parties included, among other information, their names, usernames, email addresses, telephone numbers, gender, mailing addresses, dates of birth, occupations, companies and nationalities ("**Affected Data**").

NSS' internal investigations revealed vulnerabilities in its website and suspicious Structured Query Language ("**SQL**") injections prior to the hacking incident. It was believed that the unknown parties had accessed and exfiltrated the Affected Data *via* an SQL injection attack.

Decision

NSS admitted its breach of the Accountability Obligation and Protection Obligation under the PDPA and requested that the matter be dealt with under the PDPC's Expedited Decision Procedure.[1]

Breach of Accountability Obligation

The PDPA requires an organisation to undertake measures to ensure that it meets its obligations under the PDPA and demonstrate that it can do so when required ("**Accountability Obligation**").

For instance, an organisation is required to designate one or more individuals to be responsible for ensuring its compliance with the PDPA (i.e., the Data Protection Officer(s) ("**DPO**")). The DPO is generally tasked with:

(a) fostering a data protection culture within the organisation;

(b) handling queries and complaints relating to personal data that are received by the organisation;

(c) alerting the organisation's management to any personal data risks; and

(d) liaising with the PDPC where necessary.

Further, an organisation is also required to develop and implement personal data protection policies to ensure a consistent minimum data protection standard across its practices, procedures and activities.

[1] According to the Guide on Active Enforcement published by the PDPC, the Expedited Decision Procedure generally entails (a) an upfront voluntary admission of liability by the organisation for the breach of the relevant obligations under the PDPA and of its role in the breach; (b) provision of the relevant facts of the incident by the organisation to the PDPC; and (c) the organisation's compliance with relevant direction(s) issued by the PDPC.

In the present case, NSS admitted that it had breached the Accountability Obligation as it did not appoint a DPO or implement any personal data protection policy prior to the hacking incident.

Breach of Protection Obligation

NSS admitted that it had breached the Protection Obligation as it did not establish reasonable security arrangements to protect the personal data stored on its website database, which left the website susceptible to attacks.

In particular, after the development of its website by an external vendor in 2011, NSS did not engage any vendor to maintain the website's security. Nor did NSS itself implement any such security measures (e.g., performing necessary security updates, patches and penetration tests).

Financial penalty

In finding that NSS had breached the Accountability Obligation and Protection Obligation, the PDPC directed NSS to pay a financial penalty of $14,000.

A copy of this decision may be accessed here.

Neo Yong Xiang (trading as Yoshi Mobile) [2021] SGPDPC 12

Comments

This decision affirms the principle that the Purpose Limitation Obligation operates independently of the Consent Obligation. Accordingly, organisations must ensure that the purpose(s) for any collection, use and/or disclosure of personal data are what a reasonable person would consider appropriate in the circumstances.

This case also sheds some light on how the PDPC takes into account mitigating factors (e.g., financial difficulties faced by the relevant organisation or individual) when deliberating on the appropriate financial penalty to impose. In particular, what constitutes a mitigating factor is highly dependent on the circumstances of the case at hand.

Facts

Neo Yong Xiang ("**NYX**"), trading as Yoshi Mobile ("**YM**"), was an exclusive retailer of M1 subscriber identity module ("**SIM**") cards and was provided a terminal device installed at YM's premises for SIM card registration ("**M1 Terminal Device**"). As part of a typical SIM card registration process at YM, the customer's identity document (e.g., identity card, passport, work pass etc) would be scanned using the M1 Terminal Device. This would capture the customer's personal data and would also reveal if the customer had reached the permitted limit of three prepaid SIM cards.

It was revealed that NYX had exploited this registration process in two ways:

(a) If, upon scanning customers' identity documents, NYX realised that the customers were entitled to purchase more SIM cards in addition to the SIM card(s) they intended to

purchase, NYX would register additional SIM cards in those customers' names without their knowledge ("**Method 1**"); and

(b) If customers decided that they did not want to continue their purchase after the SIM card(s) had been registered but before activation, NYX would, instead of cancelling the registrations, activate the SIM card(s) without the customers' knowledge ("**Method 2**").

These illicit SIM cards were later sold to anonymous walk-in customers. This affected 78 individuals' personal data, including their names, addresses, NRIC numbers and/or work permit numbers. It was also discovered that these illicit SIM cards registered at YM were subsequently exploited by unknown perpetrators to send unsolicited spam and/or scam messages.

Decision

The PDPC found that NYX had breached the Consent Obligation and the Purpose Limitation Obligation under the PDPA.

Breach of Consent Obligation

Under Section 13 of the PDPA, organisations are prohibited from collecting, using or disclosing an individual's personal data unless the individual, among others, consents to the same ("**Consent Obligation**"). In this regard, Section 14(1) of the PDPA further provides that, for the consent given to be valid, the individual must be notified of the purposes for which his or her personal data is being collected, used or disclosed.

On the facts, it was held that NYX had breached the Consent Obligation in the following ways:

(a) In respect of Method 1, the customers had only consented to their personal data being used to register SIM cards that they had intended to purchase, and not for the registration of the illicit SIM cards for sale to anonymous buyers; and

(b) In respect of Method 2, when the customers decided not to continue with the purchase of the SIM cards, they had withdrawn their consent to the collection and use of their personal data for the purposes of purchasing the SIM cards. However, NYX had continued to use their personal data without their consent to activate those SIM cards without the customers' knowledge.

Breach of Purpose Limitation Obligation

Section 18 of the PDPA provides that an organisation may collect, use or disclose an individual's personal data only for purposes that: (a) a reasonable person would consider appropriate in the circumstances; and (b) the individual has been informed of by the organisation, where applicable ("**Purpose Limitation Obligation**").

At the outset, the Purpose Limitation Obligation operates independently of the Consent Obligation. Therefore, even if the data subject gives his consent for his personal data to be used for a particular purpose, it does not follow that the particular purpose is reasonable in all circumstances.

In the present case, given that the customers' personal data was used to register illicit SIM cards which were later sold for NYX's financial gain, the PDPC found that the customers' personal data had not been used for a reasonable purpose.

Financial penalty

NYX raised the following mitigating factors to avoid or mitigate the financial penalty that the PDPC intended to impose on him:

(a) He was in a difficult financial situation;

(b) He had breached the PDPA for financial gain as his business was adversely affected by COVID-19 and the landlord of YM had refused to pass on the relevant COVID-19 rental relief provided by the Government; and

(c) His breaches of the PDPA were less egregious than breaches committed by other organisations as he did not leak or sell personal data for financial gain.

While the PDPC accepted mitigating factor (a), it found mitigating factor (b) to be disingenuous, given that NYX had been misusing his customers' personal data since 2018, before the COVID-19 pandemic. As for mitigating factor (c), the PDPC was of the view that NYX's breaches of the PDPA were in fact more egregious as they involved the intentional misuse of personal data and abuse of trust over a protracted period of time, and had facilitated the commission of breaches of Do-Not-Call provisions.

Taking into account NYX's financial circumstances, the PDPC directed him to pay a reduced financial penalty of $21,000.

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

MYANMAR

-
WongPartnership Myanmar Ltd.
Junction City Tower, #09-03
Bogyoke Aung San Road
Pabedan Township, Yangon
Myanmar
t +95 1 925 3737
f +95 1 925 3742

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

-
ZGLaw
27/F 88 Corporate Center
141 Sedeño Street, Salcedo Village
Makati City 1227, Philippines
t +63 2 889 6060
f +63 2 889 6066
w zglaw.com/~zglaw

wongpartnership.com