Data Protection Quarterly Updates (April – June 2023)

The Personal Data Protection Commission (**PDPC**) published six decisions between April and June 2023 after concluding the following investigations:

(a) Five investigations relating to the Protection Obligation (described on page 2) under the Personal Data Protection Act 2012 (**PDPA**); and

(b) One investigation relating to section 48B of the PDPA (prohibition on use of dictionary attacks).

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

Name of decision	Obligation(s) breached	Directions imposed
Fullerton Healthcare and Agape CP Holdings [2023] SGPDPC 5	Protection Obligation	Fullerton Healthcare – Financial penalty of $58,000 Agape CP Holdings – Financial penalty of $10,000
Kingsforce Management Services [2023] SGPDPCS1	Protection Obligation	Directions to implement a plan to ensure regular software upgrading and patching
Fortytwo Pte. Ltd. [2023] SGPDPCS 3	Protection Obligation	Financial penalty of $8,000
OrangeTee & Tie Pte Ltd [2023] SGPDPC 3	Protection Obligation	Financial penalty of $37,000
The Law Society of Singapore [2023] SGDPC 4	Protection Obligation	Directions to conduct a security audit
Tai Shin Fatt [2023] SGDPC 2	Section 48B of the PDPA	Warning issued

Fullerton Healthcare and Agape CP Holdings [2023] SGPDPC 5

Comments

This case serves as a reminder that even when an organisation engages a data intermediary to process its data, the company remains responsible for fulfilling its obligations under the PDPA. Though the data intermediary plays a direct role in protecting the personal data in its possession, the organisation is still required to exercise reasonable oversight of the data intermediary's data processing activities.

As such, in addition to requiring the data intermediary to handle personal data responsibly through appropriate contractual provisions, the organisation is expected to regularly monitor and check what security arrangements the data intermediary has implemented.

Facts

Fullerton Healthcare Group Pte. Limited (**Fullerton**) is an enterprise healthcare service provider which provides healthcare services to individuals and employees of its corporate clients. In 2018, Fullerton engaged Agape CP Holdings Pte. Ltd. (**Agape**) to provide call centre and appointment booking services.

In October 2021, the PDPC was notified that the personal data of some 156,900 of Fullerton's customers had been accessed, exfiltrated and offered for sale on the dark web.

Investigations revealed that Agape downloaded Fullerton's customer data and uploaded it onto an internet facing file server (**Online Drive**). This was contrary to the understanding between Fullerton and Agape that Agape was only to access Fullerton's customer data *via* Fullerton's Microsoft SharePoint from one single Agape computer, save in emergency or exceptional situations where Agape was unable to connect to Fullerton's SharePoint.

After discovering the data leak, Fullerton promptly implemented several remedial measures, including informing affected clients of the breach, and advising them to guard against potential risks. Agape also ceased the use of the Online Drive.

Both Fullerton and Agape requested, and the PDPC agreed, for the matter to proceed under the PDPC's Expedited Breach Decision Procedure. To this end, the two organisations voluntarily and unequivocally admitted to the facts in the PDPC's decision and their breaches of the Protection Obligation.

Decision

Breach of Protection Obligation by Agape

Under the Protection Obligation, an organisation is required to protect personal data in its possession or under its control by making reasonable security arrangements.

The PDPC found that while Agape had carried out the requisite periodic security reviews, these reviews were improperly scoped and failed to cover the Online Drive. Agape admitted that this omission was due to the Online Drive having been a legacy feature unique to their engagement by Fullerton and that, owing to such omission, Agape failed to review and assess the Online Drive's security implications and risks.

In addition, Agape was found to have inadequate password policies. While the Online Drive was protected by a password when it was initially installed, at the time of the incident, the password had inadvertently been disabled. As such, the Online Drive had become an open directory listing on the internet without any password protection, causing it to be highly vulnerable to unauthorised access, modification and other

similar risks. Even before the password had been disabled, Agape's agents had been using a common password to access the Online Drive, with no expiry date set for the password.
The PDPC held that, if Agape had properly scoped its periodic reviews to cover the Online Drive, the lapse would have been detected and rectified. In light of the above, Agape had breached the Protection Obligation.

Breach of Protection Obligation by Fullerton

With regard to Fullerton, the PDPC noted that a company that engages a data intermediary to process personal data on its behalf bears the same obligations under the PDPA as if it processed the personal data itself. In particular, in the context of an organisation's relationship with its data intermediary, the organisation has a supervisory or general role for data protection, while the data intermediary has a more direct and specific role in data protection.

The PDPC found that, while Fullerton had conducted a due diligence review of Agape and required Agape to undertake in writing certain PDPA obligations before engaging Agape, Fullerton failed to exercise reasonable oversight over Agape as it did not regularly monitor and inquire about Agape's data management procedures throughout the engagement.

The PDPC also found that Fullerton had unnecessarily disclosed more personal data to Agape than was needed for Agape's purpose, causing unnecessary data security risks. Therefore, the PDPC found that Fullerton had breached its Protection Obligation.

In determining whether any directions or financial penalties should be imposed on Fullerton and Agape, the PDPC took into account both organisations' voluntary admissions of their breach, timely remediation efforts and willingness to cooperate during investigations.

Ultimately, the PDPC imposed a financial penalty of $10,000 on Agape and a financial penalty of $58,000 on Fullerton. The PDPC rationalised the higher financial penalty imposed on Fullerton on the ground that Fullerton's annual turnover was almost 50 times higher than that of Agape's.

In addition to the financial penalties imposed, the PDPC directed Agape to:

(a) Ensure that the scope of its periodic security review included the protection of personal data handled by all of Agape's systems; and

(b) Record in writing with Fullerton the data protection requirements for the processing of personal data on behalf of Fullerton, including arrangements for the exercise of regular oversight by Fullerton.

The PDPC also directed Fullerton to:

(a) Review processes and contractual obligations with Agape and other existing vendors processing data for Fullerton to ensure that such vendors have sufficiently robust data-handling processes; and

(b) Review existing internal processes to ensure that only personal data necessary for fulfilling contractual obligations are disclosed to vendors *via* secure channels.

A copy of this decision may be accessed here.

Kingsforce Management Services [2023] SGPDPCS1

Comments

This decision illustrates how timeous remediation efforts and admission of liability may serve as key mitigating factors in the PDPC's determination whether to impose financial penalties.

In this case, the PDPC's decision to not impose financial penalties on Kingsforce is aligned with PDPC's Active Enforcement Framework, which aims to promote accountability by organisations when handling personal data. This affords organisations an opportunity to conduct themselves in a dignified manner when breaches are found.

Facts

Kingsforce Management Services Pte Ltd (**Kingsforce**) is a specialist recruitment firm. On or about 27 December 2021, Kingsforce discovered that some 54,900 jobseeker datasets had been put up for sale on a hacking forum. Investigations revealed that the breach was a result of Kingsforce's outdated website coding technology.

Upon discovery of the data breach, Kingsforce promptly implemented several remedial actions including suspending its original website and engaging a new developer to create a new website.

Subsequently, Kingsforce requested, and the PDPC agreed, for the matter to proceed under the PDPC's Expedited Breach Decision Procedure. To this end, Kingsforce voluntarily and unequivocally admitted the facts in the PDPC's decision and admitted to breaches of the Protection Obligation.

Decision

Protection Obligation

Although Kingsforce engaged information technology (**IT**) maintenance vendors to ensure the security of its website, the scope of the maintenance was limited to troubleshooting functionality issues and excluded database protection. Kingsforce also failed to conduct reasonable periodic security reviews of its website.

In light of the above, the PDPC was satisfied that Kingsforce was in breach of the Protection Obligation.

Despite this, the PDPC did not impose a financial penalty on Kingsforce, explaining that timely remediation efforts and voluntary admissions of an organisation's role in a breach are strong mitigating factors in determining whether to impose financial penalties.

As Kingsforce had admitted liability upfront and the affected personal data was no longer accessible, the PDPC decided it would be most appropriate to issue Kingsforce directions to:

(a) Submit a plan to ensure regular patching, updates and upgrades for all software and firmware through which personal data may be accessed;

(b) State whether it intends to implement the plan through external vendors or its own resources, and if external vendors are to be engaged, to provide the job specifications to be communicated to the vendors; and

(c) Outline each implementation step with deadlines such that the entire plan is completed within 60 days from the date the Direction is issued.

A copy of this decision may be accessed here.

Fortytwo Pte. Ltd. [2023] SGPDPCS 3

Comments

This decision serves as an important reminder for organisations to ensure that software which they employ is kept up to date, including by applying security patches and updates. This is crucial as such patches and updates often contain the latest cybersecurity measures to fend off cyber-attacks, and consequently ensures that any personal data in the organisations' possession and control is adequately protected.

Furthermore, organisations should be aware that their obligations under the PDPA apply to all datasets in their possession and control, even if any personal data contained in such datasets is false or inaccurate.

Facts

Fortytwo Pte. Ltd. (**Fortytwo**) operates an online furniture store. In December 2021, Fortytwo notified the PDPC of a data leak through the injection of malicious codes. Personal data, such as billing addresses and credit card information, of more than 6,000 individuals was captured.

Fortytwo requested, and the PDPC agreed, for the matter to proceed under the PDPC's Expedited Breach Decision Procedure. To this end, Fortytwo voluntarily and unequivocally admitted the facts in the PDPC's decision and admitted to breaches of the Protection Obligation.

Decision

Whether fictitious names or pseudonymous personal particulars constitute "personal data"

In this case, an issue arose as to whether fictitious names or pseudonymous personal particulars formed part of the personal data in Fortytwo's possession and control. Fortytwo stated that as it did not

verify the details provided by its users, the impact of the data incident may have been more limited as it included names which were incomplete, fictitious or pseudonymous.

The PDPC reiterated that "personal data", as defined under the PDPA, includes data "*whether true or not* …", emphasising that the obligations under the PDPA apply even where not every record of personal data in the possession or control of an organisation is verified. On the other hand, where an organisation has applied pseudonymisation or anonymisation techniques to personal data, such that the risk of re-identification is adequately addressed and managed, the resulting dataset may be treated as anonymised. Such data would therefore no longer constitute "personal data".

Even though some of Fortytwo's customers might have provided inaccurate information, the fact remained that Fortytwo had collected personal data. Fortytwo's obligations under the PDPA therefore applied to its entire customer database.

Protection Obligation

Fortytwo admitted that it had, between November 2017 and April 2020, failed to apply four security patches for the software used (**Magento**) for its online store, resulting in vulnerabilities which the threat actor had successfully exploited in capturing personal data.

In addition, Adobe announced in November 2015 that it was ending support for Magento in June 2020. Although Fortytwo had planned to upgrade to a newer version of Magento (**Magento Version 2**) in response to the announcement, it failed to do so, claiming that the COVID-19 pandemic disrupted its upgrading plans. The PDPC did not accept Fortytwo's explanation, given the ample notice from Adobe of the need to upgrade to Magento Version 2 in order for Fortytwo to continue receiving support and security patches from Adobe.

The PDPC imposed a financial penalty of $8,000, accounting for mitigating factors such as Fortytwo's cooperation during investigations, prompt remedial action, including the notification of affected individuals, and implementation of technical measures to improve security.

A copy of this decision may be accessed here.

The Law Society of Singapore **[2023] SGPDPC 4**

Comments

This decision is a timely reminder that an organisation should ensure that security arrangement reviews are conducted on a regular basis, despite having contractual arrangements with an external vendor for IT security maintenance.

In addition, passwords used for administrative accounts should be sufficiently complex and utilise multi-factor authentication (**MFA**) when sensitive or large volumes of data are involved.

Facts

The Law Society of Singapore (**LSS**) represents members of the legal profession in Singapore. For the purpose of carrying out its statutory functions, the LSS stores the personal data of all current and former members in one of its servers.

In February 2021, the PDPC received a notification from the LSS that a ransomware attack had occurred on its servers. A threat actor had gained access to the IT administrator's account and encrypted the personal data of the LSS' current and former members. Over 16,000 members' personal data was affected, including each member's full name, residential address, date of birth, and NRIC number.

The attack was detected by malware detection software deployed by the LSS, which took immediate steps to remove the new administrator account created by the threat actor and restore the servers to their original state from secured back-ups.

Investigations by PDPC centred on whether the LSS had breached its obligation under section 24 of the PDPA to protect personal data in its possession or under its control by making reasonable security arrangements to prevent unauthorised access.

The investigations revealed that there could have been multiple threat actors or the same group of threat actors targeting the LSS through multiple channels, such as brute force attacks, phishing emails, and exploiting the unpatched virtual private network (**VPN**) vulnerability of the VPN system. Of the three possible attack vectors, the vulnerability in the LSS' VPN system was likely to have allowed the threat actor entry, as MFA was not implemented for administrative access to the LSS' servers.

Decision

No Breach of the Protection Obligation for Omission to Patch the Vulnerability

Under the PDPA, organisations may rely on vendors engaged to provide IT security maintenance to obtain and apply needed software upgrades and patches. The PDPC noted that, given the technical nature of information on software patching and upgrading, this would limit the degree of oversight that many organisations can exercise over vendor performance.

In this case, the LSS had instituted a process to ensure that there were maintenance logs to monitor its vendor's activities. In technical areas where the LSS depended on its vendor's technical expertise, the LSS' oversight was found to be reasonably adequate.

In the circumstances, the PDPC held that the LSS had not breached the protection obligation as: (a) it was reasonable for LSS to rely on its vendor to perform software security patching; and (b) LSS had discharged its duty of oversight over the vendor's patching function.

Breach of the Protection Obligation

Nonetheless, the LSS was found to have negligently breached the Protection Obligation by:

(a) Using a password that could be easily guessed for the compromised administrator account. The password used for the compromised account was "Welcome2020lawsoc", which was a weak password and vulnerable to dictionary attacks due to the use of a full word and the LSS' name;

(b) Failing to change the password for the compromised administrator account at reasonable intervals; and

(c) Failing to conduct any periodic security reviews in the three years leading up to the incident.

The PDPC referred to its published Guide to Data Protection Practices for information and communications technology (ICT) systems, which noted that unauthorised access is one of the most common types of data breaches, and can be caused by the use of a weak password that can be easily guessed by hackers. To remediate this, MFA should be adopted for accounts with administrative privileges, and for systems managing sensitive data or large volumes of personal data.

As the LSS had taken prompt remedial action in response to the incident, no financial penalty was imposed by the PDPC. Instead, the PDPC issued various directions to, among other things:

(a) Engage qualified security service providers to conduct a thorough security audit of its technical and administrative arrangements for the security, maintenance, creation and removal of administrative accounts that can access directly and/or create access to personal data in the LSS' possession or control;

(b) Furnish to the PDPC a schedule stating the scope of the security audit, and to provide the full security audit report to the PDPC; and

(c) Rectify any security gaps identified in the security audit report, review and update its personal data protection policies as applicable.

A copy of this decision may be accessed here.

Tai Shin Fatt **[2023] SGPDPC 2**

Comments

This decision highlights that organisations should always verify that automated processes deployed for any business functions adhere strictly to industry guidelines and regulations. This is the first published enforcement decision concerning the prohibition under section 48B of the PDPA on the use of a "dictionary attack". The PDPC defines a "dictionary attack" as a method by which a recipient's telephone number is obtained using automated means that generates possible telephone numbers by combining numbers into numerous permutations.

While the sending of unsolicited commercial messages through legitimate direct marketing practices is not prohibited, organisations should still exercise caution and ensure compliance with the PDPA when engaging in such practices.

Facts

In July 2021, the PDPC received a notification from the Singapore Police Force that the Singapore Civil Defence Force (**SCDF**) had received an influx of marketing calls between 25 and 28 June 2021.

The PDPC's investigations revealed that an individual named Tai Shin Fatt (**Tai**), who was an insurance director at a prominent insurance company, employed LongSheng Consultancy Pte Ltd (**LongSheng**) for marketing services. Through LongSheng, Tai engaged the services of two companies, referred to as the "Call Automation Vendor" and "Checker", with the aim of conducting marketing calls more efficiently. The Call Automation Vendor provided software that facilitated automated calls using customised scripts, while the Checker's service involved providing telephone numbers for making the automated calls, along with software to verify whether the recipients' telephone numbers were registered in the Do Not Call Registry (**DNCR**).

To generate telephone numbers for the marketing calls, Tai's staff used a combination of commonly observed telephone numbers for the first four digits, together with a set of randomly generated numbers for the last four digits. Using this method, a list of 18,809 telephone numbers was generated, including 400 telephone numbers starting with "995". Notably, "995" is the SCDF emergency line.

Between 25 June and 28 June 2021, over 22,000 automated marketing calls were made, of which over 400 were directed to the SCDF emergency line. These calls were not blocked because the SCDF emergency line was not registered in the DNCR.

Subsequently, Tai discovered that calls were made to the SCDF emergency line and directed the Call Automation Vendor to stop making further automated marketing calls and delete the generated phone numbers. The PDPC's investigation focused on whether Tai had violated section 48B of the PDPA.

Decision

Section 48 Prohibition

The prohibition in section 48B targets the indiscriminate manner in which recipient telephone numbers may be generated and targeted, usually by automated means. It does not serve as a blanket prohibition on the sending of unsolicited commercial messages, and leaves room for legitimate direct marketing.

However, the PDPC found that Tai had breached the section 48B prohibition for a combination of reasons, including that:

(a) Tai had specifically authorised and caused the making of such calls;

(b) The calls were made in Singapore, and as such, the calls had a "Singapore link"; and

(c) The method deployed by which strings of numbers were combined and resulted in the creation of over 18,000 permutations using automated means was a "dictionary attack".

The PDPC therefore found that Tai had breached section 48B of the PDPA.

The PDPC also noted that numerous calls had been made to the SCDF's emergency line pursuant to Tai's instructions and took pains to emphasise the importance of keeping the SCDF emergency line open and unobstructed for genuine emergencies.

In view of earlier remedial actions taken by Tai, a warning was issued in respect of his breach and no other directives were found to be necessary.

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