Data Protection Quarterly Updates (October – December 2022)

The Personal Data Protection Commission (**PDPC**) published a total of six decisions between October and December 2022 after concluding the following investigations:

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

(b) One investigation relating to the Transfer Limitation Obligation under the PDPA.

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

Name of decision	Obligation(s) breached	Directions imposed
Case No. DP-2106-B8484 *Cognita Asia Holdings Pte Ltd*	Protection Obligation	Financial penalty - $26,000
Case No. DP-2108-B8816 *QCP Capital Pte Ltd*	Protection Obligation	No breach of the PDPA
Case No. DP-2007-B6646 *Farrer Park Hospital Pte Ltd*	Protection Obligation	Financial penalty - $58,000
Case No. DP-2103-B8147, DP-2206-B9935 *Supernova Pte. Ltd.* and *Shopify Commerce Singapore Pte. Ltd.*	Transfer Limitation Obligation	Supernova Pte. Ltd. – Breach of Transfer Limitation Obligation Shopify Commerce Singapore Pte. Ltd. – Breach of Transfer Limitation Obligation
Case No. DP-2010-B7266 *RedMart Limited*	Protection Obligation	Financial penalty - $72,000
Case No. DP-2010-B7246 *Thomson Medical Pte. Ltd*	Protection Obligation	Directions in lieu of financial penalty

We outline below some decisions of interest relating to the enforcement of the Protection Obligation and Transfer Limitation Obligation.

***Farrer Park Hospital Pte Ltd* [2022] SGPDPC 6**

Comments

This case serves as a timely reminder to organisations dealing with sensitive personal data (such as medical information) to put in place stronger security arrangements and/or controls to protect such data.

In addition, the case illustrates the perils of allowing employees to automatically forward emails to external domains, particularly where the organisation uses web-based email services. In light of the PDPC's remarks, it would be prudent for organisations to carefully consider their information technology (**IT**) policy on allowing the automatic forwarding of emails, so as to comply with the Protection Obligation under the PDPA.

Facts

In July 2020, the PDPC received a data breach notification from Farrer Park Hospital Pte Ltd (**Hospital**).

Between March 2018 and October 2019, two employees (**Employees**) configured their Microsoft Office 365 work email accounts (**Email Accounts**) to automatically forward all incoming emails to the email address of a third party.

The Employees were part of the Hospital's marketing department, which processed email requests for the Hospital's medical services. These emails contained personal data relevant to medical treatment requested by individuals. Some emails also contained information relating to medical conditions, history, results and reports (**Medical Information**).

Decision

Protection Obligation

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 stated that, in determining what constitutes reasonable security arrangements, the organisation should take into consideration the nature of the personal data in question, as well as the impact that disclosure of that personal data might have on the affected person.

In this case, the Employees' department routinely received and processed sensitive personal data (including Medical Information), and the Email Accounts were accessible from a web-based system which was more vulnerable to unauthorised access. As such, the PDPC found that the Hospital ought to have implemented stronger security arrangements, policies and/or controls to manage the Email Accounts.

Such arrangements could have included implementing enhanced access controls for access to the Email Accounts (such as multi-factor authentication), implementing processes for collection of Medical Information *via* a more secure platform, regularly purging and moving Medical Information to a more secure system (such as a non-Internet facing system), and password protecting email attachments.

Email Auto-Forwarding

The PDPC underlined the security risks posed by automatic forwarding of emails to external domains, citing a warning from the United States of America's Federal Bureau of Investigations that cyber-criminals have been exploiting auto-forwarding rules on web-based email clients to perpetrate email compromise scams.

The PDPC clarified that the Protection Obligation requires organisations, as part of their periodic security review, to weigh and counter the attendant risks, including the risks of adopting the default settings of "out-of-the-box" software solutions.

In this case, the Hospital represented that it had not previously specifically examined the risks arising from email auto-forwarding, as there were no prevailing standards or guidelines on email auto-forwarding before the incident. The PDPC gave the Hospital the benefit of the doubt that this may have affected its risk assessment, and hence did not factor in this omission in determining the enforcement action to be taken.

However, the PDPC cautioned that, in future cases, failure by an organisation to make a reasonable assessment of the risks from email auto-forwarding would constitute a breach of the Protection Obligation, and would be met with appropriate enforcement action.

Financial Penalty

The Hospital represented that it should receive a reduction in the financial penalty awarded as, among other reasons, no individuals had been harmed or had suffered loss as a result of the incident.

The PDPC held that the lack of evidence of further exploitation, use or disclosure is not, of itself, a factor meriting the reduction of the financial penalty, as the lack of an aggravating factor (i.e., subsequent exploitation, use or disclosure of personal data) is not in itself a mitigating factor.

A copy of this decision may be accessed here.

Supernova Pte Ltd and Shopify Commerce Singapore Pte Ltd **[2022] SGPDPC 7**

Comments

Organisations must impose legally binding obligations on data intermediaries to ensure that data intermediaries provide a standard of protection to transferred personal data that is comparable to the standard of protection under the PDPA. Such obligations must be established from the beginning of the commercial arrangement. Conducting a due diligence assessment on the data intermediary's data protection approach will not suffice.

Further, it is possible to satisfy the Transfer Limitation Obligation by incorporating the Model Contractual Clauses endorsed by the Association of Southeast Asian Nations (**ASEAN**) into parties' agreements. This may be a helpful avenue for small and medium enterprises to comply with the Transfer Limitation Obligation.

Facts

Shopify Inc (**Shopify**) is a Canada-based e-commerce platform for online retailers to conduct sales. Supernova Pte Ltd (**SNPL**) is an online retailer. In December 2018, Shopify and SNPL entered into an agreement for SNPL's use of Shopify's platform to sell products to customers. Pursuant to the agreement, Shopify Commerce Singapore Pte Ltd (**Shopify SG**) was to act as the Asia-Pacific data sub-processor of Shopify. Shopify SG's role was confined to collecting customer personal data *via* the platform and transferring the data out of Singapore to Shopify for both: (a) purchase processing on behalf of merchants (such as SNPL); and (b) platform processing for Shopify's own purposes.

The agreement between Shopify and SNPL was later assigned to Shopify SG. After the assignment, the flow of customer personal data remained the same – Shopify SG continued to transfer personal data to Shopify to carry out the data processing. However, Shopify SG's role in the data flow changed – Shopify SG became the data intermediary of SNPL in relation to purchase processing, and also became the data controller of customer personal data in relation to platform processing.

Between June and September 2020, customer personal data stored in Shopify's systems, including personal data of SNPL's customers, was illegally accessed and exfiltrated.

Decision

Transfer Limitation Obligation – SNPL

The PDPC held that neither SNPL nor Shopify SG was responsible for the security of Shopify's systems in Canada, which held the personal data affected in the incident.

However, it found that SNPL had breached its Transfer Limitation Obligation under section 26 of the PDPA. SNPL was required to ensure that Shopify provided a standard of protection to transferred personal data that was comparable to the protection under the PDPA. This obligation continued even after the agreement was assigned to Shopify SG, as the flow of SNPL's customer personal data remained unchanged. Therefore, from the start of their commercial relationship with Shopify, the onus was on SNPL to put in place relevant contractual clauses to ensure the protection of its personal data to a standard comparable to the PDPA.

However, SNPL failed to put in place such binding contractual clauses. The fact that SNPL carried out a due diligence assessment of Shopify's approach to data protection before entering into an agreement with Shopify was inadequate to fulfil its Transfer Limitation Obligation.

Transfer Limitation Obligation – Shopify SG

The PDPC also held that Shopify SG had breached its Transfer Limitation Obligation under section 26 of the PDPA. In relation to purchase processing, Shopify SG acted as SNPL's data intermediary and was therefore not bound by the Transfer Limitation Obligation. However, as regards platform processing, Shopify SG had processed customer personal data for its own purposes. Shopify SG was therefore the data controller in relation to such personal data, and bound by the Transfer Limitation Obligation.

Shopify SG breached the Transfer Limitation Obligation by failing to put in place legally binding obligations requiring Shopify to provide the requisite standard of protection to personal data transferred from Shopify SG to Shopify for processing. The fact that Shopify was in the process of updating its corporate rules to comply with the PDPA at the time of the decision did not retrospectively ensure compliance with the Transfer Limitation Obligation at the material time.

ASEAN Model Contractual Clauses

The PDPC observed that the ASEAN had adopted and endorsed the Model Contractual Clauses meant to facilitate cross-border transfers of personal data. It also highlighted that the PDPC recognises that the Model Contractual Clauses meet the requirements of the Transfer Limitation Obligation under the PDPA, and can therefore be used by enterprises of any scale as a standard for business-to-business transfers. Organisations can also adapt the Model Contractual Clauses to suit their commercial arrangements. The Model Contractual Clauses may be especially useful in helping small and medium enterprises fulfil the Transfer Limitation Obligation.

A copy of this decision may be accessed here.

***RedMart Limited* [2022] SGPDPC 8**

Comments

This decision illustrates how having a complex IT architecture may still be inadequate in enabling an organisation to meet the Protection Obligation if vulnerabilities at every level are not addressed. This decision also highlights best practices and possible solutions to help organisations fulfil the Protection Obligation.

Facts

In October 2020, the PDPC was notified that a database containing personal data of customers of RedMart Limited (**RedMart**) was being offered for sale on an online forum.

After RedMart was acquired by Lazada Group (**Lazada**) in 2016, RedMart integrated its platform with Lazada's. To this end, RedMart re-designed and migrated various databases and applications from one cloud environment to another. In the midst of this migration process in September 2020, an unidentified threat actor gained unauthorised access to customer personal data stored in RedMart's Alibaba Cloud Storage.

Decision

Protection Obligation

The PDPC found that the Protection Obligation was breached. It also reiterated that, in determining what constitutes reasonable security steps or arrangements, an organisation must have regard to the nature of the personal data in its possession and control as well as the impact that the disclosure of the data might have on affected persons.

Even though RedMart had adopted a complex IT architecture, there were still vulnerabilities at every level of defence that should have been addressed. In particular:

- RedMart failed to implement reasonable access control on its employers' user GitHub accounts. User accounts, like administration accounts, were allowed access to important files. However, unlike administration accounts, user accounts were protected only by a password instead of two-factor authentication. The PDPC noted that data with higher security implications ought to have been secured to a higher degree than other types of data.

- RedMart did not implement sufficient access controls to protect and limit access to important files which enabled highly privileged access to various environments within its systems. The PDPC observed that the principle of least privilege should have applied (i.e., each employee should have been granted only the minimum level of access rights or privileges necessary for that employee to complete an assigned operation). Moreover, periodic management reviews should have been conducted to ensure that access to such important files was limited to accounts that needed such access, with accounts that no longer needed access having access rights revoked.

- Insufficient security measures were implemented to protect important files. In this case, the application programming interface (API) keys which enabled the threat actor to access and exfiltrate the customer personal data were stored in plain text files and not encrypted or password-protected. The PDPC highlighted that such keys ought to have been stored in a separate location within the cloud storage system.

- RedMart also did not implement separate authentication requirements for the database containing customer personal data. The only protection was the general access requirements for the cloud storage that the database was on. The PDPC took the view that, at the minimum, access controls such as password protection should have been implemented.

Financial Penalty

In determining the quantum of the financial penalty, the PDPC considered RedMart's voluntary notification of the incident, lack of antecedents, and voluntary acceptance of liability after the PDPC's preliminary decision.

The PDPC also clarified that lack of subsequent misuse of the affected personal data and lack of antecedents do not merit a reduction in the financial penalty. These factors simply do not increase the financial penalty to be imposed.

A copy of this decision may be accessed here.

Thomson Medical Pte. Ltd. [2022] SGPDPCS 15

Comments

This decision demonstrates that relying solely on individual employees to perform their tasks diligently is insufficient to comply with the Protection Obligation. Organisations must ensure they have processes in place to ensure that their instructions are complied with.

Further, organisations should consider performing pre-launch security testing on any new websites, applications or features involving personal data to identify weaknesses in their systems that may lead to a potential breach of the Protection Obligation.

Facts

In July 2020, the PDPC was notified that the Health Declaration Portal of Thomson Medical Pte. Ltd. (**Thomson Medical**) was not secure, as a CSV (comma separated values) file containing personal data of visitors (**CSV file**) was publicly accessible. Such personal data included visitors' names, contact numbers, national registration identity card or passport numbers, purposes of visits and answers to a health declaration questionnaire.

Thomson Medical's in-house developer had omitted to remove a software code and change the default web-server configuration, which led to the CSV file being publicly accessible between April and September 2020.

Decision

Thomson Medical accepted that it was in breach of the Protection Obligation to make reasonable security arrangements to protect personal data in its possession or under its control. The PDPC also held that Thomson Medical was in breach of the Protection Obligation.

Although Thomson Medical's existing policies required visitor data to be stored in a secured database, and Thomson Medical had instructed its in-house developer to act in line with those policies, the PDPC found that Thomson Medical had failed to ensure that there were processes in place to ensure that these policies and instructions were complied with. For example, Thomson Medical could have required

its developer to demonstrate to another staff member, and required that staff member to verify, that the instructions were complied with. But it did not. The PDPC cautioned against relying solely on individual employees to perform their tasks diligently with no oversight or supervision.

Further, the PDPC found that Thomson Medical failed to conduct reasonable pre-launch testing before the portal went live, to verify that there were access controls to the visitor data collected.

In light of several mitigating factors (including the limited scope of personal data disclosed, and Thomson Medical's swift rectification efforts), the PDPC imposed directions in lieu of a financial penalty, ordering Thomson Medical to take remedial actions including arrangements for reasonable pre-launch security testing before the launch of any new website, application or feature for the processing of personal data.

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