Data Protection Quarterly Updates (April – June 2022)

The Personal Data Protection Commission ("**PDPC**") published a total of thirteen decisions between April and June 2022 after concluding the following investigations:

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

(b) One investigation relating to the Accountability Obligation under the PDPA;

(c) One investigation relating to the Consent Obligation under the PDPA;

(d) One investigation relating to the Protection and Accountability Obligations under the PDPA;

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

(f) One investigation relating to the Protection and Transfer Limitation Obligations under the PDPA.

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

Name of decision	Obligation(s) breached	Directions imposed
Case No. DP-2007-B6585, DP-2007-B6591, DP-2007-B6594, DP-2007-B6598 *SLP Scotia Pte. Ltd.* and *SLP International Property Consultants Pte. Ltd.*	Consent Obligation	SLP Scotia – No breach of PDPA SLP International – No breach of PDPA
Case No. DP-2012-B7506 *Aman Group S.a.r.l* and/or *Amanresort International Pte Ltd*	Protection Obligation	No breach of PDPA
Case No. DP-2109-B8857 *(1) Ngian Wen Hao Dennis* *(2) Chan Puay Hwa Melissa*	Consent and Notification Obligations	(1) Dennis - Warning (2) Melissa – Warning (3) Winarto – Warning

(3) Winarto *(4) Aviva Financial Advisers Pte Ltd*		(4) Aviva – No breach of PDPA
Case No. DP-2013-B8138 *Vhive Pte Ltd*	Protection Obligation	Financial penalty - $22,000
Case No. DP-1804-B1931 Royal Caribbean Cruises (Asia) Pte. Ltd.	Protection Obligation	No breach of PDPA
Case No. DP-2008-B6707 *(1) Toll Logistics (Asia) Limited* *(2) Toll Global Forwarding (Singapore) Pte. Limited* *(3) Toll Offshore Petroleum Services Pte. Ltd.* *(4) Toll (TZ) Pte. Ltd* *(collectively, "**Organisations**")*	Protection and Transfer Limitation Obligations	Transfer Limitation Obligation - Warning Protection Obligation – No breach of PDPA
Case No. DP-2102-B7854 *Southaven Boutique Pte Ltd*	Protection Obligation	Financial penalty - $2,000 (reduced from $5,000 after reconsideration)
Case No. DP-2002-B5827 *PINC Interactive Pte Ltd* [2022] SGPDPC 1	Accountability and Protection Obligations	Financial penalty - $12,500
Case No. DP-1912-B5484 *Lovebonito Singapore Pte Ltd* [2022] SGPDPC 3	Protection Obligation	Financial Penalty - $24,000
Case No. DP-2009-B7057 *Trinity Christian Centre Limited*	Protection Obligation	Financial Penalty – $20,000

Case No. DP-2101-B7725 *GeniusU Pte Ltd*	Protection Obligation	Financial Penalty – $35,000
Case No. DP-2102-B7878 *Singapore Telecommunication Limited*	Protection Obligation	No breach of PDPA
Case No. DP-2107-B8598 *ACL Construction (S) Pte Ltd*	Accountability Obligation	Directions given to develop and implement practices and policies for compliance with PDPA, and to conduct compulsory training programme for employees

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

In the matter of an investigation under section 50(1) of the Personal Data Protection Act 2012 And ACL Construction (S) Pte Ltd

Comments

This case demonstrates the importance for organisations to be aware of their obligations under, and to comply with, the PDPA, even though the organisation may be primarily dealing with business contact information.

Facts

ACL Construction (S) Pte Ltd ("**ACL Construction**") is a general contractor and construction management company that provides pre-fabricated structures, structural steel products, and construction services. The PDPC was notified that data from ACL Construction was being offered for sale on the dark web. The data included the names of ACL Construction's customers and relevant liaison persons, as well as their business contact numbers and business emails.

In the course of the PDPC's investigation, the PDPC found that ACL Construction had failed to appoint a Data Protection Officer ("**DPO**") as required under section 11(3) of the PDPA.

Decision

Accountability Obligation

As the names, business contact numbers and business emails were not provided by those customers and liaison persons for a personal purpose, the PDPC held that they would ordinarily constitute "business contact information" as defined under the PDPA and therefore fall outside the scope of the PDPA. Therefore, while ACL Construction may have suffered a data breach, no personal data was in fact affected.

However, as ACL Construction had failed to appoint a DPO and develop data protection policies, the PDPC found ACL Construction in breach of the PDPA by failing to comply with its Accountability Obligation under the PDPA.

The PDPC ordered ACL Construction to develop and implement policies and practices to comply with the PDPA, and to put in place a programme of compulsory training for employees of ACL when handling personal data.

A copy of this decision may be accessed here.

Lovebonito Singapore Pte. Ltd. [2022] SGPDPC 3

Comments

This decision highlights what the PDPC would consider the baseline standard of protection for accounts with administrative privileges i.e., the use of two-factor authentication ("**2FA**") and multi-factor authentication ("**MFA**"). This decision also sets out a tiered approach to how the PDPC would view an organisation's implementation of (or failure to implement) 2FA and MFA as part of its data protection policies.

It would be prudent for organisations to carefully consider how 2FA and MFA are to be incorporated into their information technology ("**IT**") systems for compliance with the Protection Obligation under the PDPA.

Facts

Lovebonito Singapore Pte. Ltd. ("**Lovebonito**") is a Singapore-based fashion brand and retailer that operates an e-commerce platform ("**Website**"). Lovebonito engaged Magento Cloud, a cloud-based service which includes the Magento Content Management System ("**Magento CMS**"), to host and run the Website. Lovebonito also used a payment platform offered by Adyen N.V. ("**Adyen**") to facilitate credit card payments on the Website. This platform would load directly from Adyen's servers as a frame within the "checkout" page ("**Checkout Page**") of the Website when a customer indicated his or her intention to pay for purchases with a credit card.

Adyen would directly collect details such as the full credit card number, the expiry date of the credit card, the card verification value [CVV] number of the credit card, and the customer's billing address (collectively, "**Credit Card Data**"). After processing the credit card payment, Adyen would send some (but not all) of the

Credit Card Data to Lovebonito, namely the last four digits of the credit card number, the expiry date of the credit card, Adyen's payment reference, and billing address (collectively, "**Partial Credit Card Data**"). Lovebonito would then store the Partial Credit Card Data with other details that Lovebonito collects for processing the order e.g., first name, last name, shipping address, email address, phone number, order details, payment type (collectively, "**Order Data**").

After investigation, it was found that one of Lovebonito's Magento CMS accounts with administrator privileges was likely to have been compromised. This compromised account was likely used to modify the Checkout Page to load and execute an unauthorised code each time the Checkout Page was loaded, which caused the Credit Card Data intended to be sent to Adyen to be intercepted and exfiltrated to the malicious actor. The compromised account was also used to access and exfiltrate Order Data from the Website. In total, the personal data of 5,561 customers was accessed and exfiltrated.

Decision

Protection Obligation

The PDPC held that the Credit Card Data constituted personal data, as the Credit Card Data, when put together with the Order Data, could identify individuals together with other data that Lovebonito had access to. Further, Lovebonito was held to have control over the Credit Card Data as it deployed Adyen's code within a frame on its Checkout Page, and could control how the Credit Card Data was collected and processed before it was transmitted to Adyen, even if Lovebonito did not have actual possession. As the Order Data and Credit Card Data included personal data of a financial nature, in assessing the reasonableness of Lovebonito's security arrangements, the PDPC reiterated that such sensitive personal data would require stronger security measures before an organisation would be considered to have discharged its Protection Obligation. Thus, the PDPC held that Lovebonito had failed to put in place such reasonable security arrangements to protect the Order Data and Credit Card Data.

The PDPC also found that the password policy of the Magento CMS was lacking, and contributed to the failure of Lovebonito to meet the standard of a reasonable security arrangement under the Protection Obligation. The PDPC listed the following shortcomings:

- Periodic changes of passwords were not mandated as part of the default settings; and
- Lovebonito's employees were not required to refrain from using easily-guessable passwords.

Representations by Lovebonito

One of the representations made by Lovebonito was that the risk of compromise to the more sensitive Credit Card Data *via* Magento CMS was relatively low. The PDPC disagreed with this, as access and changes to the Website were managed and carried out by Lovebonito. In other words, Lovebonito's Protection Obligation extended over the entire Website, including the Checkout Page (with Adyen's code being deployed therein). It was therefore for Lovebonito to secure the Website having regard to the sensitivity and volume of the personal data in its possession and/or control.

PDPC commentary on 2FA and MFA

The PDPC considered that, as 2FA and MFA tools become more broadly available, the adoption of these tools should become the norm, at least for accounts with administrative privileges. The PDPC emphasised the practices recommended in its handbook on common causes of data breaches (*How to Guard Against Common Types of Data Breaches*), such as using 2FA / MFA for all administrator access to systems holding large volumes / sensitive personal data and using a one-time password or 2FA / MFA as part of the authentication and authorisation process in an organisation's information and communications technology [ICT] systems.

The PDPC held that the requirement of 2FA / MFA for accounts with similar levels of administrative privileges would form the baseline standard that the PDPC would apply in future cases, and set out the following tiered approach:

(a) First, 2FA / MFA should be implemented as a baseline requirement for administrative accounts to systems that hold personal data of a confidential or sensitive nature, or large volumes of personal data. Failure to do so can amount to a breach, unless the organisation can show that the omission to implement 2FA / MFA is reasonable or implementation would be disproportionate.

(b) Second, remote access by privileged accounts to information systems that host confidential or sensitive personal data, or large volumes of personal data, should be secured by 2FA / MFA, as the risks concerning remote access are higher.

(c) Third, organisations using IT systems to host confidential or sensitive personal data, or large volumes of personal data, are expected to enable and configure 2FA / MFA if it is a feature that is available out-of-the-box. Omission to do so may be considered an aggravating factor.

A copy of this decision may be accessed here.

***Toll Logistics (Asia) Ltd & Ors* [2022] SGPDPC 4**

Comments

When it comes to ensuring compliance with the PDPA at a group level, organisations should ensure that all entities in the group are suitably covered under the relevant agreements, and consistently review the relevant agreements to keep them up to date.

In this case, although the parent organisation was careful to implement the necessary data protection provisions in the agreement between itself and its third-party Human Resources ("**HR**") provider, as the other entities in the group were not included in the agreement and there was otherwise no contractual obligation on the parent organisation to protect the personal data of its subsidiary organisations, the PDPC found the subsidiary organisations to be in breach of the PDPA.

Facts

Toll Holdings Limited ("**Toll Holdings**") is an integrated logistics services provider headquartered in Australia. Toll Logistics (Asia) Limited ("**Toll Logistics**"), Toll Global Forwarding Singapore Pte. Ltd. ("**Toll Forwarding**"), Toll Offshore Petroleum Services Pte. Ltd. ("**Toll Offshore**"), and Toll (TZ) Pte. Ltd. ("**Toll TZ**") are Singapore-registered entities (collectively, "**Organisations**") that form part of a group of companies headed by Toll Holdings ("**Group**").

Toll Holdings executed a series of Corporate Services Agreements ("**CSAs**") whereby Toll Holdings would provide finance, HR and IT services to all the Organisations. Under the terms of the CSAs, Toll Holdings was permitted to appoint subcontractors to perform part or all of the services subject to the CSAs, but was responsible to the same extent as if it had performed the services itself.

Toll Holdings also contracted with a third-party HR vendor ("**HR Vendor**") to provide a global HR Platform for the Group's use ("**HR Platform**"). The Group entities would upload the personal data of employees to the HR Platform, and such data was hosted by the HR Vendor in data centres in the European Economic Area.

A data breach occurred when a malicious actor gained access to Toll Holdings' IT environment in Australia using credentials stolen from a third-party vendor, and executed a ransomware attack, encrypting files on a number of the Group's servers. The exfiltrated files were uploaded by the malicious actor onto the dark web. However, there was no evidence of data exfiltration from the Group's Singapore servers or any other servers in the Group's IT environment, other than the Australia server; nor was there any evidence of exfiltration of personal data of the Organisations' current or former employees.

Decision

Protection Obligation

Members of a corporate group may satisfy the Protection Obligation by relying on binding group-level written policies or intra-group contracts which specify the respective data protection obligations of the members of the group. In the present case, while the Organisations had entered into the CSAs, the CSAs did not deal with data protection obligations. As such, the Protection Obligation remained with the Organisations. The CSAs were found to be insufficient to show that the data protection operations had been centralised with Toll Holdings at the Group-level.

The PDPC held that, notwithstanding the above, Toll Holdings was responsible for IT support services including Group-level IT security standards, which the Organisations would then develop and implement. In accordance with these standards, a number of industry-standard technical solutions and tools were implemented to protect the personal data in the Singapore servers. As such, the PDPC held that the Organisations had not breached their Protection Obligation as the security arrangements in place prior to the data breach were reasonable and consistent with existing industry standards, and the security lapse had resulted from the theft of credentials from the third-party vendor which was beyond the control of the Organisations.

Transfer Limitation Obligation

The Organisations had been transferring the personal data of their employees from Singapore to the European Economic Area for storage as part of the HR Platform since around July 2013. The Organisations were required to take appropriate steps to ensure that the personal data would be protected to a standard comparable to that under the PDPA before any such transfers were made. However, there was no evidence of any such steps taken by the Organisations.

Although the contract between Toll Holdings and the HR Vendor included data protection obligations imposed on the HR Vendor, the Organisations were not party to the contract. The CSAs also did not contain any provisions imposing obligations on Toll Holdings to protect the personal data of the Organisations for the purposes of the centralised corporate functions to be undertaken pursuant to the CSAs. The PDPC thus held that the Organisations had breached the Transfer Limitation Obligation in relation to the personal data uploaded onto the HR Platform. The PDPC issued a warning to the Organisations in light of the mitigating factors and remedial actions already taken by the Organisations.

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