Data Protection Quarterly Updates (January – March 2023)

The Personal Data Protection Commission (**PDPC**) published four decisions between January and March 2023 after concluding the following investigations:

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

(b) One investigation relating to the Protection Obligation and Retention Limitation Obligation under the PDPA; and

(c) One investigation relating to the Consent, Notification and Purpose Limitation Obligations 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
Sembcorp Marine Ltd [2023] SGPDPCS 2	Protection Obligation	No breach of Protection Obligation
Eatigo International Pte. Ltd. [2022] SGPDPC 9	Protection Obligation	Breach of Protection Obligation Financial penalty of $62,400
CPR Vision Management Pte Ltd *L'Oréal Singapore Pte Ltd* *L'Occitane Singapore* [2022] SGPDPCS 17	Protection Obligation and Retention Limitation Obligation	Breach of Protection Obligation and Retention Limitation Obligation by CPR Vision Management Pte Ltd Directions issued to, among others: (a) Conduct a security audit; (b) Rectify any security gaps identified; (c) Conduct a review of its databases containing personal data; and (d) Review and update its personal data policies No breaches by L'Oréal Singapore Pte Ltd and L'Occitane Singapore
RedMart Limited [2023] SGPDPC 1	Consent, Notification and Purpose Limitation Obligations	Breach of Consent, Notification and Purpose Limitation Obligations. No further directions issued as earlier directions had already been complied with

We outline below some decisions of interest relating to the enforcement of the Protection Obligation, Retention Limitation Obligation and Consent, Notification and Purpose Limitation Obligations under the PDPA.

***Sembcorp Marine Ltd* [2022] SGPDPCS 2**

Comments

Even if an organisation may have several vulnerabilities in its systems or applications, the PDPC will assess holistically whether the organisation has: (a) implemented reasonable security arrangements, including the time taken by the organisation to react to a new vulnerability; and (b) taken expeditious steps to patch the vulnerability after being made aware of it.

Facts

In July 2022, the PDPC received a data breach notification from Sembcorp Marine Ltd (**Sembcorp**).

Investigations by Sembcorp revealed that a threat actor had exploited three Log4J vulnerabilities in an application to gain unauthorised access to a server in January 2022. As a result, the threat actor exfiltrated the personal data of more than 25,000 individuals.

After discovering the Log4J vulnerability, Sembcorp took prompt action to identify the vulnerability across all its software applications and apply security patches. Workarounds were implemented for systems for which patches were not available or had not been released. Incoming and outgoing Log4J traffic was also blocked.

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 recognised that Sembcorp had little reaction time to detect and prevent the threat actor from infiltrating its server in January 2022, as the Log4J vulnerability was first reported in December 2021, and the threat actor had infiltrated Sembcorp's servers as early as January 2022. The PDPC also acknowledged the swiftness with which Sembcorp took steps to address the vulnerability after its discovery (as described above).

The PDPC noted that Sembcorp had adopted good practices in relation to its information and communications technology systems by implementing a cybersecurity testing programme, regular vulnerability assessment and penetration testing, and cyber security monitoring.

As such, the PDPC was satisfied that Sembcorp had met its Protection Obligation under the PDPA and no enforcement action was taken in relation to the data breach.

A copy of this decision may be accessed here.

***Eatigo International Pte. Ltd.* [2022] SGPDPC 9**

Comments

This decision illustrates the importance of maintaining up-to-date personal data asset inventories which catalogue all the personal data assets in an organisation's possession or control. This is to ensure that all such personal data is protected by the organisation's security measures.

In addition, this case demonstrates how an organisation's cooperation (or lack thereof) with the PDPC during investigations may impact the PDPC's decision. An organisation's lack of cooperation may unnecessarily prolong investigations, and may also be considered an aggravating factor when imposing directions.

Facts

Eatigo International Pte. Ltd. (**Eatigo**) is an online restaurant reservation platform which offers incentives (e.g., dining discounts) to its users. As part of its daily operations, Eatigo collects and processes the personal data of its users to facilitate restaurant reservations and the provision of incentives.

In October 2020, the PDPC was notified of a possible data leak by Eatigo, as a cache of personal data suspected to have originated from Eatigo's database was offered for sale on an online forum. Eatigo was separately informed of the data leak by the PDPC and a journalist, and thereafter proceeded to investigate.

Eatigo's investigations revealed that the personal data for sale on the online forum did not match any of its current databases in use at the time of the data leak but matched the structure of a legacy database (**Affected Database**). The Affected Database was in use until 2018, and contained Eatigo's users' personal data as of late 2018. Thereafter, Eatigo migrated to its current online platform. Although Eatigo had no intention of continuing to use the personal data in the Affected Database, it had retained such data to facilitate the migration onto its new platform. However, following the migration, the Affected Database was not included in Eatigo's Virtual Private Network (VPN) infrastructure. Further, Eatigo's new engineering team had no knowledge of, and did not have credentials to access, the Affected Database.

The Affected Database lacked several security measures, including, among others, password rotation rules, a security review on the protection provided to the personal data in the Affected Database, and a system to monitor the exfiltration of large volumes of data.

After discovering the data leak, Eatigo swiftly implemented several remedial actions including, among others, ensuring that the Affected Database was securely backed-up and then deleted, notifying affected individuals, and conducting penetration testing.

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. In determining what constitutes a "reasonable" security arrangement, organisations should take into account the nature of the personal data in its possession and control and the impact that the disclosure of the data might have on affected persons. Given that the Affected Database contained personal data of approximately 2.76 million individuals, the PDPC was of the view that Eatigo should have implemented policies and practices to meet the security needs to fulfil the Protection Obligation.

Further, the PDPC cautioned that organisations with substantial personal data assets should maintain an accurate and up-to-date personal data asset inventory as part of the Protection Obligation. Such an inventory should catalogue all personal data assets in the organisation's possession or control to ensure that the personal data is secured by the organisation's security measures, and that the organisation retains the necessary institutional memory of all its personal data assets regardless of staff turnover.

The PDPC found that Eatigo was uncooperative during investigations and that its negligence in failing to maintain the Affected Database in its personal data asset inventory had resulted in the omission to extend its existing security arrangements to the Affected Database. The PDPC also found that Eatigo did not implement robust security monitoring for the exfiltration of large volumes of data and periodic security audits, including a reasonable vulnerability assessment of its information technology infrastructure.

While Eatigo had implemented swift remedial measures to address the data leak, the PDPC found Eatigo grossly negligent in its handling of the Affected Database. Eatigo's uncooperative responses to the PDPC were also an aggravating factor. As such, the PDPC imposed a financial penalty of $62,400 on Eatigo. No further directions were issued to Eatigo in view of its remedial actions.

A copy of this decision may be accessed here.

CPR Vision Management Pte Ltd, L'Oréal Singapore Pte Ltd and L'Occitane Singapore [2022] SGPDPCS 17

Comments

This decision is a timely reminder of the importance of ensuring that contractual arrangements with vendors and other data intermediaries include appropriate data protection terms for compliance with the PDPA.

In addition, this case illustrates the importance of regularly reviewing data protection policies and practices and ensuring that such policies and practices are implemented in day-to-day operations. Doing so mitigates the risk that certain servers, databases, or storage devices are inadvertently overlooked, especially following a data migration or technology refresh.

Facts

CPR Vision Management Pte Ltd (**CPR**) was a customer relationship management (**CRM**) system vendor that helped to process personal data collected by L'Oréal Singapore Pte Ltd (**L'Oréal**) and L'Occitane Singapore Pte Ltd (**L'Occitane**).

The PDPC received data breach notification reports from L'Oréal and L'Occitane, on 29 October 2021 and 1 November respectively, of a ransomware attack on CPR. The data breach affected a server and three network attached storage devices in CPR's office and involved the encryption of personal data belonging to 83,640 of L'Occitane's customers and 35,079 of L'Oréal's customers. The types of personal data affected included customers' names, addresses, email addresses, mobile numbers, NRIC numbers, dates of birth, ages, gender, race, nationality, loyalty points, and amount spent.

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

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.

Although CPR had implemented an endpoint security solution which would have been able to detect and block unauthorised entry attempts to its office network, CPR had omitted to extend the deployment of this solution to the affected office network. While the nation-wide COVID-19 circuit breaker in Singapore in April 2020 could have partly excused CPR's omission to include the affected office network in its data inventory, the PDPC observed that the omission to extend the deployment of the solution had persisted for more than one and a half years, until October 2021.

Furthermore, as a CRM system vendor, CPR processed a high volume of web traffic containing personal data on behalf of many e-commerce retailers, including L'Oréal and L'Occitane, and would ordinarily be held to a higher standard. As such, the omission to deploy its endpoint security solution suggested that CPR had failed to maintain an inventory of its data assets.

In light of the above, the PDPC found that CPR was in breach of the Protection Obligation.

Retention Limitation Obligation

CPR admitted that it was in breach of the Retention Limitation Obligation.

CPR admitted that the affected personal data had been legacy content, which should have been deleted and for which no business or legal purpose justified retention. In fact, L'Oréal had specifically instructed CPR to delete the affected personal data, and CPR had furnished a purported Certificate of Destruction stating that the personal data had been deleted in 2021.

The PDPC found that L'Oréal and L'Occitane were not in breach of their Retention Limitation Obligation because they had adequately provided in their contracts with CPR that CPR was to ensure compliance

with the Protection and Retention Limitation Obligations under the PDPA. It also observed that they had no knowledge of the retention and storage of the legacy personal data by CPR and had no control over the device used by CPR to store the personal data affected by the ransomware attack.

Decision

As CPR had admitted liability upfront and there was no evidence that data exfiltration or modification had occurred, the PDPC decided it would be most appropriate to issue CPR directions rather than impose a financial penalty. Accordingly, the PDPC directed CPR to:

(a) Conduct a thorough security audit of its technical and administrative arrangements for the protection of personal data in its possession and control and conduct;

(b) Rectify any security gaps identified;

(c) Conduct a comprehensive review of its databases containing personal data to ensure full compliance with the Retention Limitation Obligation; and

(d) Review and update its personal data policies, including clarifying the roles of data intermediaries and vendors in complying with the Retention Limitation Obligation.

A copy of this decision may be accessed here.

***RedMart Limited* [2023] SGPDPC 1**

Comments

This decision highlights the importance of ensuring that the collection, use, and disclosure of personal data is conducted only on clearly identified and justifiable grounds. In light of the PDPC's clarification that the National Interest Exception and Investigations Exception have a relatively narrow scope, it would be prudent for organisations relying on these exceptions to ensure they have alternative bases for the collection, use, and disclosure of personal data, such as express consent and the general Legitimate Interests Exception.

Facts

The PDPC received a complaint stating that RedMart Limited (**RedMart**) was collecting images of the physical NRICs and other identification documents of suppliers making deliveries to its warehouses. Security checkpoints at RedMart's warehouses used a RedMart-issued tablet computer to take photographs of these documents (**ID Photographs**).

According to RedMart, the ID Photographs were collected to deter acts that could compromise food safety and also to facilitate the investigation of food safety incidents. However, there were no notices at the warehouses' security checkpoints informing suppliers of the purpose for the collection of the ID Photographs.

Decision

RedMart sought to justify the collection of the ID Photographs on the following two legal bases.

Inferred or Implied Consent

RedMart first sought to rely on inferred or implied consent on the basis that the suppliers had volunteered the documents to be photographed on request. However, the PDPC noted that RedMart had failed to comply with its Notification Obligation because it did not inform the suppliers of the purpose for collecting the ID Photographs. Further, even if the Notification Obligation had been complied with, since the collection of ID Photographs was a condition for entry to the warehouses, and the suppliers made deliveries to the warehouses as part of their employment or business, the PDPC found that any such consent would have been invalid.

The PDPC rejected RedMart's submission that there was deemed consent from the suppliers because the suppliers had no choice in the matter. They could not therefore be said to have voluntarily provided their documents in order for deemed consent to be made out. Further, the PDPC observed that it would not have been obvious to suppliers that photographic images of their documents would be taken and stored.

Legitimate Interests Exception

Alternatively, the PDPC accepted that RedMart could in principle have relied on the general Legitimate Interests Exception to collect the ID Photographs without the suppliers' consent, since the collection was for the purpose of ensuring good public hygiene and safety, which was not only a legitimate interest of RedMart but also benefited all downstream food and beverage businesses, supermarkets, and diners who eventually consumed the food stored in the warehouses.

To rely on the general Legitimate Interests Exception, RedMart would have, prior to collecting the ID Photographs, had to:

(a) Conduct and document an assessment determining whether RedMart's interests in collecting the ID Photographs outweighed the adverse effect on suppliers;

(b) For any adverse effects identified, RedMart would have had to implement reasonable measures to eliminate, mitigate, or reduce the likelihood of occurrence; and

(c) Provide suppliers reasonable access to information about RedMart's collection of the ID Photographs (e.g., by way of disclosure in RedMart's public data protection policy).

National Interest Exception

The PDPC rejected RedMart's submission that it could rely on the National Interest Exception on the basis that it was in the national interest to collect ID Photographs to establish the identities of suppliers to a high level of fidelity and deter potential food security incidents at the warehouses. It held that, while RedMart's food security concerns were valid, they were limited to its own warehouses and did not reach the level of "national defence" or "national security" concerns contemplated by the National Interest Exception.

Investigations Exception

The PDPC also rejected RedMart's reliance on the Investigations Exception in the PDPA, on the basis that the collection of ID Photographs was necessary to facilitate investigations into food security incidents at the warehouses. It held that, in order for RedMart to rely on the Investigations Exception, the collection of personal data must have been for the purpose of an ongoing investigation and could not be for a hypothetical future investigation.

Decision

The PDPC found that RedMart had not complied with the PDPA in respect of the collection and use of ID Photographs from suppliers prior to 8 July 2022.

In view of its findings and the fact that RedMart had taken some steps to address the issues raised, the PDPC's preliminary decision was to give directions to RedMart to evaluate whether the collection of ID Photographs was reasonably necessary for RedMart's interest in deterring and investigating security incidents at the warehouses and, if RedMart intended to rely on the general Legitimate Interests Exception, to take the necessary steps described above.

However, the PDPC observed that RedMart had already taken steps to address the issues raised, including an internal assessment to rely on the Legitimate Interests Exception and action to eliminate and mitigate the adverse effects that might have resulted from its collection and use of the ID Photographs (including the implementation of enhanced access controls to protect the ID Photographs).

Consequently, the PDPC found that the risks of unauthorised access, use, and/or disclosure of the ID Photographs had been significantly lowered and that RedMart had already complied with the directions contemplated in its preliminary decision. The PDPC therefore decided that it was unnecessary to issue any further directions.

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