Data Protection Quarterly Updates (April – June 2021)

The Personal Data Protection Commission ("**PDPC**") published ten decisions between April to June 2021 after concluding the following investigations:

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

(b) one investigation relating to the Consent Obligation under the PDPA;

(c) two investigations relating to the Protection and Accountability Obligations under the PDPA;

(d) one investigation relating to the Protection and Consent Obligations under the PDPA; and

(e) one investigation relating to the Access Obligation under the PDPA.

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

Name of decision	Obligation(s) breached	Directions imposed
Larsen & Toubro Infotech Limited, Singapore Branch	Consent and Protection Obligation	Financial penalty – S$7,000
Webcada Pte Ltd	Accountability and Protection Obligation	Financial penalty – S$25,000
HMI Institute of Health Sciences Pte. Ltd. [2021] SGPDPC 4	Protection Obligation	Financial penalty – S$35,000
ST Logistics Pte Ltd [2020] SGPDPC 19	Protection Obligation	Financial penalty – S$8,000
Progressive Builders Private Limited and *Greatearth Corporation Pte. Ltd.* [2021] SGPDPC 2	Consent Obligation – With respect to Greatearth Corporation (No particular obligation specified with respect to Progressive Builders)	Greatearth Corporation – Warning Progressive Builders – Did not breach PDPA

Name of decision	Obligation(s) breached	Directions imposed
HSBC Bank (Singapore) Limited [2021] SGPDPC 3	Access Obligation (Review Application)	Did not breach PDPA
Flying Cape Pte Ltd and *ACCA Singapore Pte Ltd*	Protection Obligation	Flying Cape – Warning ACCA Singapore – Did not breach PDPA
St. Joseph's Institution International Ltd.	Protection Obligation	Warning
Chapel of Christ the Redeemer	Accountability and Protection Obligation	Directions to develop and implement internal data protection policies and practices to comply with the PDPA within 90 days from the date of the direction, and inform the Commission within 1 week of implementation
Tripartite Alliance Limited	Protection Obligation	Financial penalty – S$29,000

In addition, in the first private action brought under the PDPA in *Bellingham, Alex v. Reed, Michael* [2021] SGHC 125, the Singapore High Court ("**SGHC**") considered the issue of the loss or damage required for a private action to be brought against an organisation for a breach of the PDPA. To this end, the SGHC found that "loss or damage" is limited to the heads of loss or damage under common law, and does not include distress or loss of control over personal data.

We outline some decisions of interest below.

Bellingham, Alex v Reed, Michael [2021] SGHC 125

Comments

This decision concerns the first private action brought under the PDPA and is the first time the Singapore courts have considered the scope of "loss or damage" required for such an action.

The former Section 32 of the PDPA gave individuals a right of private action, and enabled any person who had suffered "loss or damage" as a result of breaches of certain provisions of the PDPA to seek relief through civil proceedings. While Section 32 of the PDPA has been repealed with effect from 1 February 2021, it has been replaced with Section 48O of the PDPA, which substantially reproduces the former Section 32 and retains the prerequisite for "loss or damage".

In this decision, the SGHC clarified that the term "loss or damage" is limited to the heads of loss or damage under common law, and does not include distress or loss of control over personal data. Therefore, if the plaintiff has not suffered any such loss or damage, his/her remedies ought to be sought through the PDPC, which is empowered by the PDPA to, amongst other things, give directions to: (a) stop collecting, using or disclosing personal data in contravention of the PDPA; and/or (b) destroy all personal data collected in contravention of the PDPA.

Facts

Alex Bellingham ("**Bellingham**") was an employee of IP Real Estate Investments Pte Ltd ("**IP Real Estate**"), and was seconded to IP Investment Management (HK) Ltd ("**IPIM HK**"). These companies were both part of the IP Investment Management group ("**IPIM Group**"). Bellingham's role in IPIM HK involved taking charge of and managing an investment fund known as the "Edinburgh Fund". Michael Reed ("**Reed**") was a customer of the Edinburgh Fund.

Bellingham later left his employment with IP Real Estate (and secondment with IPIM HK) and joined a competitor, Q Investment Partners Pte Ltd ("**QIP**"). While at QIP, he contacted Reed using Reed's personal email address (which Bellingham had used Reed's name to obtain), to discuss various investment opportunities with him as the Edinburgh Fund was scheduled to be terminated soon after.

Reed was subsequently joined to a suit against Bellingham (which was initially brought by several companies in the IPIM Group) pursuant to the former Section 32 of the PDPA. At first instance, the District Judge granted Reed's application and made several orders against Bellingham. The present case was an appeal by Bellingham against the aforementioned orders.

Decision

Bellingham's breach of obligations under the PDPA

As a starting point, it was argued that Bellingham had breached his obligations under Sections 13 and 18 of the PDPA. These obligations may be summarised as follows:

(a) Section 13 of the PDPA states that an organisation shall not collect, use or disclose personal data about an individual without his consent, unless certain exceptions apply ("**Consent Obligation**"); and

(b) Section 18 of the PDPA provides that an organisation may collect, use or disclose personal data about an individual only for purposes that a reasonable person would consider appropriate in the circumstances and if applicable, that the individual has been notified of as required under the PDPA ("**Purpose Limitation Obligation**").

Having found that Bellingham was bound by the obligations under the PDPA (as an "organisation" under the PDPA is defined to include individuals), the SGHC held that Bellingham had breached the Consent and Purpose Limitation Obligations as he had obtained and used Reed's name, email address and the fact of Reed's being an investor in the Edinburgh Fund, without Reed's consent, to contact Reed and market QIP's services to him and these purposes exceeded what a reasonable person would have considered appropriate in the circumstances.

While Bellingham obtained Reed's email address from Reed's public LinkedIn page, the SGHC held that Bellingham could not rely on the "publicly available" exception under Section 17(1) of the PDPA. This is because Bellingham would not have been able to find Reed's email address without the use of Reed's name. In this regard, it was held that, where personal data that is publicly available is obtained only through the unlawful use of other personal data, Section 17(1) of the PDPA cannot apply and the personal data so obtained cannot be collected, used or disclosed without consent.

Discussion on right of private action

(1) Scope of the term "loss or damage"

Having found that Bellingham breached his PDPA obligations, the next issue to consider was whether Reed was entitled to bring a private action under the PDPA – in particular, whether Reed had satisfied the requirement of having suffered "loss or damage".

To this end, the PDPA does not define "loss or damage". Nevertheless, applying a purposive approach, the SGHC held that the term "loss or damage" is limited to the heads of loss or damage under common law (pecuniary loss, damage to property, and personal injury including psychiatric illness), and does not include distress or loss of control over personal data.

While compensation for distress and loss of control over personal data is allowed in other jurisdictions, the positions taken in these jurisdictions are primarily due to the recognition of the right to privacy. As such, these positions were not followed as the introduction of the PDPA was not driven by a recognition of the need to protect an absolute or fundamental right to privacy – rather, it was to enhance Singapore's competitiveness and to strengthen Singapore's position as a trusted business hub and to safeguard individuals' personal data against misuse.

(2) Whether Reed suffered loss or damage due to Bellingham's breaches of the PDPA

In the present case, the SGHC found that Reed had not suffered any financial loss, psychiatric injury or nervous shock. Accordingly, the SGHC allowed Bellingham's appeal and set aside the orders made against Bellingham in the court below.

Reed has since been granted leave to appeal this decision.

A copy of this decision may be accessed here.

HMI Institute of Health Sciences Pte. Ltd. [2021] SGPDPC 4

Comments

Section 24 of the PDPA provides that an organisation shall protect personal data in its possession or under its 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**").

In the context of an organisation-vendor relationship, where the scope of the vendor's engagement does not involve the processing or handling of any personal data on behalf of the organisation, the vendor will not be regarded as a "data intermediary" under the PDPA. As such, the responsibility to protect the personal data concerned would fall squarely on the organisation.

This decision highlights that:

(a) even if a vendor is expected to handle personal data in the course of its work or make decisions which affect the security of personal data, it may *not* be considered a data intermediary under the PDPA if its scope of engagement does not involve the processing or handling of any personal data on behalf of the organisation; and

(b) organisations should take reasonable or sufficient steps to stipulate clear requirements of its vendor to ensure that the vendor understands its role in the protection of personal data on servers.

Facts

HMI Institute of Health Sciences Pte. Ltd. ("**HMI**") is a private provider of healthcare training to individuals in Singapore ("**Participants**"). In the course of its business, HMI collects personal data from its employees and the Participants. This personal data was stored on a file server owned by HMI ("**Server**") and maintained by its appointed information technology solution service provider ("**Vendor**").

The Server was later affected by a ransomware attack, which encrypted and denied access to various files on the Server, including the personal data of HMI's employees and Participants.

Decision

The PDPC found that HMI did not implement reasonable security arrangements to fulfil its Protection Obligation. Accordingly, HMI was directed to pay a financial penalty of S$35,000.

This was because:

(a) First, HMI did not have sufficiently robust processes to ensure safe remote access to the Server. In this case, HMI had, from the time the Server was set up, left open a Remote Desktop Protocol port ("**RDP Port**") to the server through which the attacker had accessed the server and executed ransomware.

While there is no strict requirement for an RDP Port (or other server ports) to always be closed, organisations should regularly review and assess the potential risks of keeping such public facing ports open. Relevant factors would include the type and volume of personal data that is stored on the server. However, in cases where an organisation holds a high volume of personal data (which could be highly sensitive), the PDPC's view is that the default approach should be to close all ports, including RDP Ports.

Further, where it may be impractical to keep the port closed by default (for example, where there would be significant downtime whenever the port would have to be opened or closed), organisations should put in place technical measures to secure port access to the server.

(b) Second, the PDPC found that HMI had not implemented proper password management policies. Although HMI had generally directed its staff to follow the standards in the password policy of one of its affiliates (which were consistent with the PDPC's recommendations), HMI had not taken steps to ensure that the password policy was complied with in practice. As a result, none of the passwords used by HMI met the password policy's recommended complexity rules.

The PDPC also observed that user accounts should generally not be shared between different individuals, especially in the case of administrator accounts. In the present case, the login credentials for the administrator account on the server were shared between one administrator in HMI and at least three other individuals in the Vendor. Although the sharing of account credentials was not a direct contributing factor to the incident, it created an additional risk factor which could have diminished the robustness of other security measures put in place by HMI.

(c) Third, the PDPC found that HMI did not take reasonable steps to ensure that the vendor would protect personal data. Even though the Vendor was not a data intermediary, it was expected to handle personal data in the course of its work or make decisions which affected the security of personal data stored on the server.

In this case, the PDPC found that in order for HMI to have discharged its Protection Obligation by relying on the vendor's technical expertise, HMI could have adopted the following approaches: (a) specified clear business requirements on the protection of data on the server; or (b) approved and adopted recommendations made by the Vendor on the data protection requirements based on its understanding of the engagement.

That said, the PDPC highlighted that the exact requirements for a given case would depend on the services that a vendor is engaged to provide. For example, if a vendor is engaged to put in place protection features for its client's information technology systems, the business requirements should describe the risks that the vendor is to address.

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 Corporate Avenue 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 International Legal Practice
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 International Legal Practice
Zalfa Building, Suite 101 - 102
Sh. Rashid Road
Garhoud
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