Data Protection Quarterly Updates (July – September 2022)

The Personal Data Protection Commission (**PDPC**) published six decisions between July and September 2022 after concluding six investigations relating to the obligation of organisations to protect personal data in their possession or under their 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**) under section 24 of the Personal Data Protection Act 2012 (**PDPA**).

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

Name of decision	Obligation(s) breached	Directions imposed
Quoine Pte Ltd [2022] SGPDPC 2	Protection Obligation	Financial penalty of $67,000
Case No DP-2007-B6670 *Terra Systems Pte. Ltd.* (Reconsideration Decision)	Protection Obligation	Financial penalty of $12,000
Case No. DP-2106-B8421 *Audio House Marketing Pte Ltd*	Protection Obligation	Financial penalty of $10,000
Case No. DP-2106-B8446 *Crawfort Pte. Ltd.*	Protection Obligation	Directions issued to, among others: (a) Engage a qualified security service provider to conduct a security audit; (b) Provide the full security audit report to the PDPC; and (c) Rectify any gaps in the security audit report.
Case No. DP-2108-B8798 *Budgetcars Pte. Ltd.* [2022] SGPDPCS 13	Protection Obligation	Directions issued to, among others: (a) Put in place appropriate contractual provisions to set out obligations and responsibilities of data controller and data intermediary;

		(b) Engage a qualified security service provider to conduct a security audit; (c) Provide the full security audit report to the PDPC; and (d) Rectify any gaps in the security audit report.
MyRepublic Limited [2022] SGPDPC 5	Protection Obligation	Financial penalty of $60,000

The Singapore Court of Appeal (**Court of Appeal**) also handed down its decision in *Reed, Michael v Bellingham, Alex (Attorney-General, intervener)* [2022] SGCA 60, holding, among other things, that emotional distress may constitute "loss or damage" in a private action.

We outline below some decisions of interest relating to the enforcement of the Protection Obligation, as well as the Court of Appeal's decision in *Reed, Michael*.

Budgetcars Pte. Ltd. [2022] SGPDPCS 13

Comments

This decision demonstrates that actions taken by an organisation that sufficiently remedy the incident may be viewed favourably by the PDPC. This case also serves as a reminder to organisations that implementing proper design of web application security is important.

Facts

Budgetcars Pte Ltd (**Budgetcars**) was a logistics company delivering parcels to customers on behalf of retailers.

The PDPC received a complaint that personal data of other individuals could be accessed by changing a few digits of a tracking delivery function (**Tracking Function Page**) on Budgetcars' website. This posed a risk of unauthorised access to the personal data of 44,357 people.

Budgetcars requested that the matter be handled under the PDPC's expedited breach decision procedure, meaning it voluntarily provided and admitted to the facts and their breach of the Protection Obligation. Budgetcars further admitted that it failed to conduct a reasonable risk assessment before carrying out the data migration exercise.

Decision

The PDPC found Budgetcars to be in breach of the Protection Obligation.

It observed that the incident was relatively less serious in nature compared to earlier cases – in this case, both the number of affected individuals and the scale of the operation were smaller.

In delivering its directions to Budgetcars, the PDPC considered factors such as the nature of the incident, Budgetcars' upfront voluntary admission of liability, and its prompt remedial actions, which included removing all personal data from the Tracking Function Page, engaging an information technology solutions provider to re-examine the management of the Tracking Function Page, and implementing post-delivery expiry of tracking identification codes after 14 days. As such, the PDPC held that it would be appropriate not to require the payment of a financial penalty, but to direct Budgetcars to, among other things, engage a qualified security service provider to conduct a thorough security audit.

A copy of this decision may be accessed here.

MyRepublic Limited [2022] SGPDPC 5

Comments

This decision highlights that organisations bear ultimate responsibility under the Protection Obligation for making reasonable security arrangements to protect personal data, despite having a vendor responsible for the security of its cloud infrastructure.

Facts

MyRepublic Limited (**MyRepublic**) is a telecommunications operator that holds a Facilities-Based Operations licence (**FBO Licence**). Under the FBO Licence, the operator is required to maintain a register containing certain records, including personal data from their customers.

MyRepublic accepts orders through a mobile order portal (**Portal**) through which customers who have applied submit their customer identity verification and number portability documents. These documents were stored on Amazon Web Services (**AWS**), which could be accessed only by an access key in the Amazon Identity and Access Management feature.

A threat actor used the access key stored in the source code of the Portal to access and exfiltrate the personal data of 79,388 customers. MyRepublic received a ransom email threatening to publish the customer data unless the ransom was paid.

Decision

The PDPC found that the organisation failed to put in place sufficiently strong security arrangements in light of the high volume and sensitivity of customer data (which included information contained in the customers' national registration identity cards, photographs, and thumbprints) in its control. In particular, MyRepublic was found to have failed to:

(a) implement sufficiently robust processes to manage the access key; and

(b) implement reasonable security controls for its AWS environment.

The PDPC held that the organisation contravened the Protection Obligation, notwithstanding that the data was hosted on AWS' cloud service, as MyRepublic still retained control over the data.

Despite mitigation factors such as prompt and effective remedial actions, cooperation during investigations, and voluntary acceptance of liability, the PDPC imposed a financial penalty of S$60,000.

A copy of this decision may be accessed here.

Reed, Michael v Bellingham, Alex (Attorney-General, intervener) [2022] SGCA 60

Comments

In a significant judgment affirming the importance of the protection of personal data in Singapore, the Court of Appeal has clarified the ambit of the right of private action in section 32(1) of the PDPA. The Court of Appeal held that emotional distress is sufficient to constitute the "loss or damage" required to found a private action. In contrast, the loss of control of personal data does not, without more, constitute such "loss or damage".

This decision also affirms that section 4(1)(b) of the PDPA provides a defence for employees to avoid liability for breaches of the PDPA, if they had engaged in such breaches in the course of their employment.

Facts

IP Investment Management Pte Ltd and IP Real Estate Investments Pte Ltd (**Employers**) commenced civil proceedings under section 32 of the PDPA against Alex Bellingham (**Respondent**). The Respondent was employed by the Employers as a marketing consultant in 2010 and left their employ in 2017. In 2018, the Respondent contacted some investors of an investment fund headed by the Employers, including Michael Reed (**Appellant**).

At first instance, the District Judge (**DJ**) granted the Appellant an injunction restraining the Respondent's use, disclosure or communication of the Appellant's personal data, and an order that the Respondent destroy all of the Appellant's personal data.

The Respondent filed an appeal to the High Court, contending that the Appellant's loss – the "loss of control of his personal data" and "emotional distress" – did not come within the meaning of suffering "loss or damage" in section 32(1) of the PDPA. On appeal, the High Court set aside the DJ's orders.

The Appellant applied to the Court of Appeal seeking a reversal of the above ruling.

In its judgment, the Court of Appeal discussed the following issues:

(a) whether section 4(1)(b) of the PDPA exempted the Respondent from liability for breaching sections 13 and 18 of the PDPA;

(b) whether "loss or damage" in section 32(1) includes emotional distress or loss of control of personal data; and

(c) whether the Appellant suffered emotional distress or loss of control of personal data.

Decision

The Court of Appeal found in favour of the Appellant. It accepted that the Respondent had contravened sections 13 and 18 of the PDPA and restored the orders made by the DJ on the ground that the Appellant's emotional distress was a form of "loss or damage" within the meaning of section 32, whereas the "loss of control over personal data" was not.

The Court of Appeal also set out a multi-factorial approach for determining whether an individual has suffered emotional distress.

Whether section 4(1)(b) exempted the Respondent from liability for breaching sections 13 and 18

Section 4(1) provides that Parts III to VI of the PDPA (**Data Protection Provisions**) do not impose any obligation on any employee acting in the course of his or her employment with an organisation.

The Court of Appeal regarded section 4(1) as a valid defence that may be invoked to avoid liability for a breach of the Data Protection Provisions. It further rejected the proposition that common law principles on vicarious liability could be imported into section 4(1), with the result that employers bear the full liability of their employees' actions leading to data incidents.

The Court of Appeal found that there was insufficient evidence to prove that the breach occurred in the course of employment and for the purposes of the Appellant's employment. As such, the Respondent could not invoke the defence.

Whether "loss or damage" in section 32(1) includes emotional distress and/or loss of control of personal data

(a) **Emotional Distress**: The Court of Appeal held that emotional distress can be considered "loss and damage".

It agreed with the High Court that this was a statutory tort, but disagreed that "loss or damage" would be interpreted according to the actionable heads of loss or damage applicable to torts under common law (e.g., pecuniary loss, damage to property, personal injury including psychiatric illness). The Court of Appeal adopted a three-step approach for statutory interpretation, comparing the possible interpretations of the provision against the statute's legislative purpose.

The Court of Appeal highlighted that a purposive interpretation of section 32(1) should be adopted. On this interpretation, it found that Parliament intended to provide robust protection for personal data belonging to individuals and did not intend to exclude emotional distress. In addition, there was nothing in the plain language of the PDPA which expressly excluded emotional distress as a type of damage covered by "loss or damage".

(b) **Loss of Control**: The Court of Appeal held that loss of control does not constitute "loss or damage" under section 32(1) of the PDPA as every breach of Parts IV to VI of the PDPA would inevitably give rise to some form of loss of control of personal data.

Whether the Appellant suffered emotional distress

The Court of Appeal observed that a multi-factorial approach was necessary and listed a few non-exhaustive considerations to guide courts in their inquiry:

(a) the nature of the personal data involved in the breach (e.g., financial data is likely to be sensitive);

(b) the nature of the breach (e.g., whether the breach of the PDPA was one-off, repeated, and/or continuing);

(c) the nature of the defendant's conduct (e.g., proof of fraudulent or malicious intent may support an inference that the plaintiff was more severely affected);

(d) risk of future breaches of the PDPA causing emotional distress; and

(e) the actual impact of the breach on the claimant.

The Court of Appeal found that the Appellant suffered emotional distress as a direct result of the Respondent's breaches of the PDPA. In particular, the evidence showed that the Appellant was anxious about the potential misuse of his personal data (which included sensitive information relating to his investment activities). Further, the Respondent's refusal to undertake not to misuse the personal data did not provide reassurance that the personal data would not be spread to third parties. It did not help that the Respondent was also evasive and dismissive of the Appellant's concerns over the safety of his personal data.

The Court of Appeal therefore held that the Appellant suffered "loss or damage" for the purposes of section 32(1) of the PDPA and upheld the DJ's grant of an injunction and undertaking order. Monetary damages were also awarded.

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