Data Protection Quarterly Updates (October – December 2021)

The Personal Data Protection Commission ("**PDPC**") published a total of seven decisions between October and December 2021 relating to the Protection Obligation (as defined below), the Transfer Limitation Obligation (as defined below), the Accountability Obligation[1] as well as the Retention Limitation Obligation[2] under the Personal Data Protection Act ("**PDPA**"), as summarised in the table below:

Name of decision	Obligation(s) breached	Directions imposed
Belden Singapore Private Limited & Anor [2021] SGPDPC 13	Transfer Limitation Obligations	Warning
Giordano Originals (s) Pte Ltd	Protection Obligation	*Did not breach PDPA*
Commeasure Pte Ltd. [2021] SGPDPC 11	Protection Obligation	Financial penalty - $74,000
ChampionTutor Inc. (Private Limited)	Protection Obligation	Financial penalty - $10,000
The National Kidney Foundation [2021] SGPDPC 10	Protection Obligation	Warning
J & R Bossini Fashion Pte Ltd [2021] SGPDPC 9	Protection and Transfer Limitation Obligations	Directions to put in place intra-group agreements, contracts, or binding corporate rules
Stylez Pte. Ltd. [2021] SGPDPC 8	Accountability, Protection and Retention Limitation Obligations	Financial penalty - $37,500 Directions to develop and implement internal data protection policies and practices

[1] The Accountability Obligation under the PDPA requires organisations to undertake measures in order to ensure that they meet their obligations under the PDPA and demonstrate that they can do so when required. Some of these measures are specifically required under the PDPA. For example, designating one or more individuals to be responsible for ensuring the organisation's compliance with the PDPA, developing and implementing policies and practices that are necessary for the organisation to meet its obligations under the PDPA ("**data protection policies and practices**"), and making information about their data protection policies and practices available.

[2] The Retention Limitation Obligation under the PDPA requires organisations to cease to retain documents containing personal data, or remove the means by which the personal data can be associated with particular customers, as soon as it is reasonable to assume that (i) the purposes for which the personal data was collected is no longer being served by retention of the personal data; and (ii) retention is no longer necessary for legal or business purposes.

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

Commeasure Pte Ltd. [2021] SGPDPC 11

Comments

Under section 24 of the PDPA, an organisation is required to protect personal data in its possession or under its control by implementing reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks, and the loss of any storage medium or device on which personal data is stored ("**Protection Obligation**").

As highlighted in this decision, even where an organisation elects to host and/or store personal data on a third-party's servers located overseas, the organisation is required to comply with the Protection Obligation so long as the personal data remains under its control (i.e., the organisation is able to access, use and remove the personal data), and its responsibility to protect personal data in its possession and control is not diminished by any human resource crunch faced by the organisation and is independent of any staff movement or appointment.

This decision emphasises the importance of conducting regular security reviews to detect and address vulnerabilities in an organisation's systems. The scope of such security reviews should also be sufficiently rigorous to minimise or eliminate the possibility of negligence and/or omissions that may result in a data breach.

Facts

Commeasure Pte Ltd ("**Commeasure**") operates a hotel booking platform and hosted its database of customer records in an Amazon RDS cloud database, which could be accessed *via* an Amazon Web Services ("**AWS**") access key. When Commeasure was still a start-up, its developers had embedded the AWS access key within an Android application package ("**Affected APK**") and erroneously marked the AWS access key as a "test" key. Even though Commeasure regarded the Affected APK as "defunct", it remained available for download by the public from the Google Play Store.

On 25 September 2020, the PDPC received a notification from Commeasure that unknown threat actor(s) had accessed and exfiltrated its database containing 5,892,843 customer records, which included, amongst other information, names, contact numbers, email addresses, dates of birth, and booking information. Significantly, this was the largest data breach since the PDPA came into effect.

Investigations revealed that the threat actor(s) had likely gained access using the AWS access key that was embedded in the Affected APK.

Decision

The Deputy Commissioner for the PDPC ("**Commissioner**") clarified that, even though AWS was responsible for the security of the cloud infrastructure that it provided to Commeasure, Commeasure remained ultimately responsible for complying with the Protection Obligation and ensuring there were reasonable security arrangements to protect all the customers' personal data under its control even if the personal data was hosted by a third-party cloud service provider on servers physically located overseas.

In concluding that Commeasure was in breach of the Protection Obligation, the Commissioner noted that:

(a) the root cause of the data breach was the embedded AWS access key in the Affected APK, which clearly fell within the scope of Commeasure's responsibility; and

(b) while Commeasure conducted quarterly security testing and reviews, the vulnerability in the Affected APK was not detected due to its negligence in wrongly labelling the Affected APK as "defunct" and the AWS access key as a "test" key. As a result, the Affected APK was omitted from Commeasure's security reviews.

Consequently, the Commissioner found that the security reviews conducted by Commeasure did not meet the rigour or standard required under section 24 of the PDPA.

Although Commeasure sought to explain that its failure to establish sufficiently robust processes was attributable to its high turnover of employees, the Commissioner found this explanation unacceptable. Commeasure's responsibility to properly and adequately protect the personal data in its possession or control should be independent of staff movement or appointment.

Accordingly, the Commissioner directed Commeasure to pay a financial penalty of $74,000.

A copy of this decision may be accessed here.

Belden Singapore Private Limited & Anor [2021] SGPDPC 13

Comments

Section 26(1) of the PDPA requires overseas transfers of personal data to be made in accordance with requirements prescribed under the PDPA to ensure that the receiving organisation provides a standard of protection to personal data so transferred that is comparable to the protection under the PDPA ("**Transfer Limitation Obligation**").

This decision highlights that, in the context of cross-border transfers of personal data within a corporate group, it is important for group members transferring personal data out of Singapore to ascertain and ensure that the receiving member(s) have established adequate and sufficient policies, practices and measures to ensure that the transferred personal data is afforded the requisite level of protection under the PDPA.

Additionally, as a practical matter, organisations should verify that all technical and legal formalities have been fulfilled in complying with the Transfer Limitation Obligation. For instance, where a corporate group elects to structure its data governance architecture around an intra-group agreement, it should ensure that all group members are parties to the agreement and able to enforce the rights and obligations therein.

Facts

Belden Singapore ("**Belden SG**") is part of the Belden Group. The overall parent entity of Belden Group is Belden Incorporated ("**Belden Inc.**") which is headquartered in the United States. As the human resource functions of Belden SG are conducted by Belden Inc., Belden SG transfers the personal data of its employees to Belden Inc. which are stored on the latter's servers. The terms of personal data transfer and processing between the members of Belden Group are governed by an intra-group Global Data Transfer Agreement ("**GDTA**"). The GDTA requires Belden Inc. to comply with applicable standards under the PDPA when importing or processing personal data from Singapore.

On 19 November 2020, Belden SG notified the PDPC that an unauthorised third party had gained access to Belden Inc.'s servers and exfiltrated information which included the personal data of 164 individuals related to Belden SG, such as current and former employees. The exfiltrated personal data included the individuals' names, addresses, email addresses, telephone numbers, dates of birth, identification numbers, marital status, photographs, salary information and tax information.

It was subsequently discovered that, at the time of the data breach, the GDTA was not in fact legally binding on Belden SG as it had not acceded to the GDTA.

Decision

At the outset, it was clarified that the obligations under the PDPA were not applicable to Belden Inc. as it does not process personal data in Singapore. Hence, the present investigations by the PDPC were focused on whether Belden SG was compliant with the Transfer Limitation Obligation in transferring personal data out of Singapore.

To comply with the Transfer Limitation Obligation, the organisation transferring personal data overseas must undertake appropriate due diligence and obtain assurances that the entity receiving the transferred

personal data is bound by legally enforceable obligations to provide to the transferred personal data a standard of protection that is at least comparable to that under the PDPA.

Based on the Commissioner's findings, even though the Belden Group had put in place a suite of policies and measures concerning the treatment of personal data, it was determined that Belden SG did not comply with the Transfer Limitation Obligation when transferring personal data out of Singapore. Specifically, the fact that Belden SG did not execute a Deed of Accession to the GDTA meant that Belden SG was not a party to the GDTA and had no legal means to ascertain and ensure that personal data it had transferred out of Singapore would be afforded the level of protection required under the PDPA.

In deciding to administer a warning to Belden SG, the Commissioner considered the following factors:

(a) Belden SG did not sign a Deed of Accession to the GDTA due to an oversight and this lapse was subsequently rectified;

(b) the suite of policies, practices and technical measures implemented within the Belden Group were sufficient to ensure that personal data transferred out of Singapore from Belden SG to Belden Inc. was afforded the requisite level of protection under the PDPA; and

(c) Belden SG's breach of the Transfer Limitation Obligation therefore resulted from a lapse in legal formalities that was not substantive in nature.

Given that Belden SG had since acceded to the GDTA, no further directions were deemed necessary by the Commissioner.

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