Data Protection Quarterly Updates (July – September 2021)

The Personal Data Protection Commission ("**PDPC**") published seven decisions between July and September 2021 after concluding the following investigations:

(a) Six investigations relating to the Protection Obligation (as defined below) under the Personal Data Protection Act ("**PDPA**"); and

(b) One investigation relating to the Transfer Limitation Obligation (as defined below) under the PDPA.

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

Name of decision	Obligation(s) breached	Directions imposed
SAP Asia Pte Ltd [2021] SGPDPC 6	Protection Obligation	Financial Penalty - $13,500
Seriously Keto Pte Ltd	Protection Obligation	Financial penalty - $8,000
Sendtech Pte Ltd	Protection Obligation	Financial penalty - $9,000 (reduced from $10,000 following the representations made by the company)
Specialised Asia Pacific Pte Ltd	Protection Obligation	Warning
NUInternational Singapore Pte Ltd and Newcastle Research and Innovation Institute Pte Ltd [2021] SGPDPC 5	Transfer Limitation Obligation	Directions to implement intra-group agreements or binding corporate rules in relation to transfers of personal data outside Singapore and review consent and notification processes
Carousell Pte Ltd	Protection Obligation	Did not breach PDPA
Singapore Telecommunications Limited [2021] SGPDPC 7	Protection Obligation	Did not breach PDPA

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

NUInternational Singapore Pte Ltd & Others [2021] SGPDPC 5

Comments

Section 26(1) of the PDPA requires overseas transfers of personal data to be made in accordance with the 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 emphasises the importance of complying with such requirements *before* the transfer is made, even if the receiving organisation may already be subject to data protection laws that may be comparable to the PDPA. Organisations that do not comply with the procedural safeguards of the PDPA in respect of overseas transfers would be in breach of the Transfer Limitation Obligation.

As a practical matter, where personal data is transferred overseas within a corporate group, it is usually more straightforward to establish written intra-group agreements and/or binding corporate rules for compliance with the Transfer Limitation Obligation before such transfers are made.

Facts

NUInternational Singapore Pte Ltd and Newcastle Research and Innovation Institute Pte Ltd ("**SG Entities**") were subsidiaries of a United Kingdom company ("**UK Entity**"), which also controlled a related company in Malaysia ("**Malaysia Entity**"). The SG Entities had previously transferred records containing personal data of Singapore-based individuals from the SG Entities to the UK Entity and Malaysia Entity. The databases containing those records, as managed by the UK Entity and Malaysia Entity, were subsequently infected by ransomware, resulting in exfiltration of personal data of Singapore-based individuals by the threat actor.

Decision

The Commissioner of the PDPC ("**Commissioner**") found that the SG Entities were in breach of the Transfer Limitation Obligation.

Pursuant to the Personal Data Protection Regulations 2014 ("**PDPR 2014**") (which were in force at the time and identical to the latest regulations in all material aspects relating to the Transfer Limitation Obligation), organisations may comply with the Transfer Limitation Obligation by relying on either of the following grounds:

(a) **Reliance on Legally Enforceable Obligations**: Organisations must ascertain and ensure that the receiving organisation overseas is bound by legally enforceable obligations in accordance with the requirements in Regulation 9(1)(b), which include any (i) law; (ii) contract or any binding corporate rules; or (iii) other legally binding instrument; or

(b) **Reliance on Consent**: Under Regulation 9(3)(a), organisations may rely on the individual's consent to overseas transfers, provided the requirements in Regulation 9(4) are satisfied, which include the requirement to give the individual a reasonable summary in writing of the extent to which the personal data to be transferred to that country or territory will be protected to a standard comparable to the protection under the PDPA.[1]

The Commissioner found that the SG Entities did not comply with either of the grounds outlined above in respect of the overseas transfer of personal data.

The SG Entities did not implement any intra-group agreements, binding corporate rules, nor any other legally binding instrument to ensure a comparable standard of protection to the transferred personal data. While the SG Entities contended that the laws of the United Kingdom applied to the UK Entity and Malaysia Entity, and would therefore provide the transferred personal data a comparable protection to the PDPA, the Commissioner noted that the SG Entities did not conduct such an assessment *before* the transfer and therefore took the view that there was a breach of Regulation 9(1)(b) of the PDPR 2014.

In the alternative, the SG Entities argued that the overseas transfer of personal data relating to certain individuals complied with Regulation 9(3)(a) of the PDPR 2014, as consent was obtained prior to such overseas transfer. However, the Commissioner took the view that the SG Entities did not comply with Regulation 9(4) of the PDPR 2014 as they did not provide such individuals a summary in writing of the extent to which their personal data would be protected to a standard comparable under the PDPA.

Consequently, the SG Entities were directed by the Commissioner to implement intra-group agreements or binding corporate rules and make the necessary changes to its consent and notification processes in order to comply with the Transfer Limitation Obligation.

A copy of the decision may be accessed here.

SAP Asia Pte Ltd [2021] SGPDPC 6

Comments

Section 24 of the PDPA requires an organisation to, among other things, protect personal data in its possession or under its control by taking reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks ("**Protection Obligation**"). Although an organisation may engage vendors to process personal data on its behalf, the organisation will still be responsible for compliance with the Protection Obligation.

[1] Further, the transferring organisation must not have required the individual to consent to the transfer as a condition of providing a product or service, unless the transfer is reasonably necessary to provide the product or service to the individual, and the transferring organisation must not have obtained or attempted to obtain the individual's consent for the transfer by providing false or misleading information about the transfer, or by using other deceptive or misleading practices. In addition, individuals may withdraw their consent to any overseas transfer.

In this decision, the PDPC observed that the Protection Obligation requires organisations to clearly and accurately convey their requirements to vendors and that a failure to properly communicate business requirements can result in insecure collection, processing, and disclosure of personal data. Further, the PDPC also highlighted the importance of pre-launch testing in order to identify data protection risks before new features are deployed in a live environment. Such pre-launch testing should be appropriately scoped to simulate real-world use of the new features. Inadequate pre-launch testing can potentially constitute a breach of the Protection Obligation.

Facts

SAP Asia Pte Ltd ("**SAPA"**) had engaged an external vendor ("**Vendor**") to develop a new programme ("**Programme"**) within SAPA's existing human resources system to automate the process of issuing payslips to former employees. SAPA had intended to use the Programme to email multiple payslips to multiple former employees simultaneously in one execution. However, this intention was not properly communicated to the Vendor, and the Vendor had therefore designed the Programme to email a single payslip to a single employee at a time.

Subsequently, when SAPA executed the Programme with the intention to generate and deliver payslips to 43 former employees in one execution, 29 former employees were emailed their own payslips as well as the payslips of other employees. In all, the personal data of 43 former employees was improperly disclosed, including names, NRIC or FIN numbers, employee numbers, bank account numbers, and salary information.

Decision

As the Vendor was not a data intermediary that was processing personal data on behalf of SAPA, the Commissioner found that SAPA was therefore solely responsible for the protection of personal data in compliance with the Protection Obligation.

The Commissioner held that SAPA was in breach of the Protection Obligation as:

(a) SAPA did not ensure that the specifications provided to the Vendor accurately reflected SAPA's intended use of the Programme being developed; and

(b) SAPA did not accurately scope pre-launch testing of the Programme to simulate the full range of intended use of the new feature.

In particular, the Commissioner noted that SAPA's instructions to the Vendor on the Programme were contained in a short service request containing the words "the selected employee" and that this reference to using the feature for a single employee had been repeated by SAPA when later responding to other queries from the Vendor, for example: "This is for employee [sic] who have left the organization". SAPA did not adequately communicate its business requirements to the Vendor, which resulted in the Programme being designed in an insecure way.

In addition, the Commissioner noted that SAPA's breach of the Protection Obligation had been compounded as it did not adequately test the Programme. SAPA's representative conducted only two test scenarios as part of user acceptance testing, and neither scenario involved issuance of multiple payslips.

Accordingly, the Commissioner directed SAPA to pay a financial penalty of $13,500. As remedial actions were already implemented by SAPA, no further directions were issued by the Commissionner.

A copy of the 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

wongpartnership.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
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