Data Protection Quarterly Updates (July – September 2023)

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

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

(b) One investigation relating to Parts 9 and 9A of the PDPA (**DNC Provisions**).

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

Name of decision	Relevant Obligation(s)	Decision and directions imposed
E-Commerce Enablers Pte. Ltd. [2023] SGPDPCS 6	Protection Obligation	Financial penalty of $74,400
Wee Jing Kai Leon [2023] SGPDPC 8	DNC Provisions	Warning administered
Autobahn Rent A Car Pte. Ltd. [2023] SGPDPCS 4	Protection Obligation	Financial penalty of $3,000 and directions to strengthen access control measures to administrator accounts and conduct reasonable security review of technical and administrative arrangements for the protection of personal data
Century Evergreen Private Limited [2023] SGPDPC 5	Protection Obligation	Financial penalty of $9,000

We outline below some decisions of interest relating to the Protection Obligation and DNC Provisions under the PDPA.

E-Commerce Enablers Pte. Ltd. [2023] SGPDPCS 6

Comments

In this decision, the PDPC emphasised that organisations cannot rely solely on their employees' proper performance of duties as a security arrangement to protect personal data.

This decision illustrates the importance of incorporating independent verifications or checks into processes involving personal data and/or tasks that may be regarded as critical or high risk, to ensure that employees carry out steps required to be taken.

Facts

E-Commerce Enablers Pte. Ltd. (**EE**) runs an online platform offering cashback for purchases made through affiliated merchant programmes.

On 25 September 2020, EE notified the PDPC and its customers of an incident involving unauthorised access to its customer data servers (**Incident**).

At the time of the Incident, EE hosted its customer database on virtual servers (**Customer Storage Servers**) in an Amazon Web Services (**AWS**) cloud environment. EE's Site Reliability Engineering (**SRE**) team used an AWS access key with full administrative privileges (**AWS Key**) to, among other things, manage EE's cloud environment on AWS. Only SRE team members had access, and were authorised, to use the AWS Key.

Prior to the Incident, the AWS Key was inadvertently committed to software code in a private repository in GitHub (a code hosting platform for version control and collaboration) by a senior SRE team member. The AWS Key was removed from GitHub two days later, but remained viewable in GitHub's "commit history".

Thereafter, the AWS Key was to be deleted and replaced by a new key as part of an out-of-cycle key rotation. However, after creating the replacement key, the SRE team member in charge of the key rotation did not fully disable and remove the AWS Key, which continued to be usable for access to EE's AWS environment until shortly after the Incident.

On 9 September 2020, a malicious threat actor gained access to EE's AWS environment using the AWS Key. The threat actor, among other things, exfiltrated data from EE's Customer Storage Servers, including email addresses, names, mobile numbers, NRIC numbers, bank account numbers, and partial credit card information.

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 found that EE had breached the Protection Obligation as it: (a) did not ensure that its processes for managing the AWS keys were sufficiently robust; and (b) did not conduct regular security reviews on whether the AWS keys had been properly rotated or deleted.

EE submitted that the Incident was a one-off case of human error, and not due to any systemic issue with its security practices. However, the PDPC rejected this argument, highlighting that organisations cannot rely solely on their employees to perform their duties properly as a security arrangement to protect personal data. Where a high-risk task is involved, the PDPC emphasised that it would be important to have additional verifications and checks.

The PDPC imposed a financial penalty of $74,400 on EE. In coming to its decision, the PDPC considered it an aggravating factor that EE responded to the exposure of the AWS Key only after 15 days, and that the AWS Key was exposed for 15 months.

However, the PDPC also noted that, among other things, EE took prompt remedial actions, including notifying affected individuals, and was cooperative during investigations.

A copy of this decision may be accessed here.

Wee Jing Kai Leon [2023] SGPDPC 8

Comments

This decision sounds a note of caution that certain obligations under the DNC Provisions may still apply in respect of Singapore telephone numbers obtained prior to 2 January 2014, i.e., before the DNC Provisions came into effect.

In particular, before sending out marketing messages to such telephone numbers, organisations should either verify that their subscribers or users are not on the Do-Not-Call (**DNC**) Registry or ensure that they have obtained valid consent to send such messages in written or other forms.

Facts

Between November 2022 and March 2023, the PDPC received complaints that one Wee Jing Kai Leon (**Mr Wee**) had sent unsolicited telemarketing messages to telephone numbers registered on the No Text Message Register of the DNC Registry.

Mr Wee is a real estate salesperson who maintained a marketing list of 2,918 Singapore telephone numbers, of which 1,224 were registered with the No Text Message Register of the DNC Registry on or around 31 March 2023.

Mr Wee admitted to sending short message service (**SMS**) messages each month from November 2022 to March 2023 to the telephone numbers on his marketing list to offer, advertise and/or promote his services as a real estate salesperson. The PDPC found that he had sent approximately 6,210 such SMS messages to telephone numbers registered on the DNC Registry.

Decision

DNC Provisions

The DNC Registry is a national database kept and maintained by the PDPC. People may register their Singapore telephone numbers with the DNC Registry in order to not receive unsolicited telemarketing calls and messages.

It is a breach of the DNC Provisions to send "specified messages" to Singapore telephone numbers without having valid confirmation that such telephone numbers are not listed in the DNC Registry unless:

(a) The subscriber or user of the Singapore telephone number has given clear and unambiguous consent to the sending of the specified message; and

(b) The consent is evidenced in writing or other form so as to be accessible for subsequent reference. This means that the consent must be captured in a manner or form which can be retrieved and reproduced at a later time in order to confirm that such consent was obtained. Possible forms include an audio or video recording of the consent given.

"Specified messages" include, among other things, messages for the purpose of advertising, promoting, or offering to provide goods or services.

Investigations revealed that Mr Wee did not obtain valid confirmation that the telephone numbers on his marketing list were not listed in the DNC Registry.

Further, Mr Wee represented to the PDPC that he was under the impression that he could use those telephone numbers for marketing purposes as he had obtained them before the PDPA was enacted.

In this regard, the PDPC recognised that a subscriber of a Singapore telephone number is deemed to have given his consent to a person to send a "specified message" to that telephone number if the subscriber consented to the sending of the "specified message" before 2 January 2014 (i.e., before the DNC Provisions came into effect), and that consent has not been withdrawn. Even if the subscriber subsequently adds his telephone number to the DNC Registry, this would not amount to withdrawal of consent.

However, the PDPC held that this would not relieve Mr Wee of his obligation to obtain clear and unambiguous consent from the subscribers or users of the Singapore telephone numbers to which the "specified messages" were sent. As there was no evidence that he had obtained such consent before or after 2 January 2014, the PDPC found that Mr Wee had breached the DNC Provisions, specifically section 43(1) of the PDPA.

The PDPC only issued Mr Wee a warning, taking into account the fact that he:

(a) Cooperated with PDPC's investigations;

(b) Had made efforts to ensure his compliance with other DNC Provisions; and

(c) Made efforts to register a sender ID under the SMS Sender ID Regime, thus showing a willingness to comply with regulatory regimes.

No other directions were found to be necessary in view of Mr Wee's voluntary cessation of sending "specified messages" to numbers on his marketing list.

A copy of this decision may be accessed here.

Autobahn Rent A Car Pte. Ltd. [2023] SGPDPCS 4

Comments

This decision illustrates the importance of putting in place and maintaining robust access controls for accounts and systems with access to personal data. As part of their access control measures, organisations should also ensure that processes are put in place to revoke access to such accounts and systems during the employee offboarding process to reduce the risk of dormant accounts being compromised.

Facts

Autobahn Rent A Car Pte. Ltd. (**Autobahn**) operates a car-sharing service, Shariot, in Singapore.

On 24 September 2022, Autobahn discovered that a photograph on its mobile application had been replaced with a pornographic photograph through an unrevoked administrator account belonging to an ex-employee.

Autobahn subsequently discovered that the ex-employee had received an email from an unknown sender on 10 September 2022 stating that his personal laptop had been hacked.

The threat actor was able to log into the Shariot mobile application administrator portal through the ex-employee's administrator account, and had downloaded a copy of personal data belonging to Shariot's users. This led to the exfiltration of 53,000 personal data sets of Shariot users, which included names, email addresses, mobile phone numbers, NRIC numbers, and general location data.

Decision

Protection Obligation

This matter proceeded under the expedited breach decision procedure. To this end, Autobahn voluntarily admitted to a breach of the Protection Obligation.

In particular, Autobahn admitted that it did not implement and ensure reasonable access control to its back-end administrator web portal by, for instance, revoking the log-in credentials of the administrator account belonging to the ex-employee once the employment relationship came to an end. It also

admitted that the incident would not have happened if it had implemented multi-factor authentication as an additional access control.

The PDPC decided that it would be appropriate to impose a financial penalty of $3,000 as the personal data breach was not insignificant. It also considered Autobahn's turnover, as well as mitigating factors such as the fact that Autobahn was cooperative during the course of investigations, voluntarily admitted to the breach of the Protection Obligation under the expedited breach decision procedure, and took prompt remedial actions.

The PDPC also directed Autobahn to:

(a) Implement processes for revoking access to systems and applications within a reasonable period of time once such access by an employee is no longer necessary;

(b) Strengthen access control measures to administrator accounts with access to databases holding personal data;

(c) Conduct reasonable security reviews of technical and administrative arrangements for the protection of personal data in Autobhan's possession or under its control within 60 days of the date of the PDPC's direction;

(d) Rectify any security gaps identified in the security review directed above; and

(e) Inform the PDPC within one week of the completion of the steps directed above.

A copy of this decision may be accessed here.

Century Evergreen Private Limited [2023] SGPDPC 5

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 decision illustrates the importance of conducting regular security tests on all information technology (**IT**) systems to ensure that any vulnerabilities are identified and remedied in a timely manner.

Facts

Century Evergreen Private Limited (**CE**) is a manpower contracting services company which requires jobseekers to submit their identification documents for verification purposes.

On 11 December 2022, the PDPC received a complaint against CE that images of identification documents (including NRICs) submitted by jobseekers were publicly accessible on CE's website.

CE admitted that an Insecure Direct Object References (**IDOR**) vulnerability on its website allowed the Uniform Resource Locator to be manipulated from the time the website was launched on 9 November 2015. As a result, 96,889 images of identification documents belonging to 23,940 individuals were downloaded from the CE's website.

Decision

This matter proceeded under the PDPC's expedited breach decision procedure. To this end, CE admitted that it had contravened the Protection Obligation under the PDPA.

In particular, CE admitted that it did not include any security requirements to protect personal data in its contract with the vendor who developed and maintained the website. It also admitted that, apart from conducting functionality testing when the website was first launched, CE had no arrangements with its IT vendor to conduct any security tests prior to the launch of the website or thereafter.

The PDPC held that, even though CE had engaged an IT vendor for the development and launch of its website, CE remained solely responsible for protecting the personal data in its possession and control at all material times.

The PDPC imposed a financial penalty of $9,000, considering that, among other things, the breach was not insignificant and there was a long period of non-compliance. The PDPC also took into account CE's turnover and profitability, its cooperation throughout the investigation, its voluntary admission of breach at an early stage under the expedited breach decision procedure, and the prompt remedial actions it took after becoming aware of the IDOR vulnerability.

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

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

wongpartnership.com