Navigating data breach notification requirements in Asia-Pacific

DLA PIPER

Select a region to view current data breach notification requirements

For more information, view our

- Data Protection Laws of the World handbook
- GDPR Fines and Data Breach Survey report
- #PracticalGlobalPrivacy: Navigating data complexities webinar series

Australia

General data breach notification requirements

Mandatory data breach notification requirements were introduced into the *Privacy Act 1988* (Cth) (**Privacy Act**) in February 2018. "Eligible data breaches" must be notified to the affected individuals and the Office of the Australian Information Commissioner (**OAIC**).

For an eligible data breach to exist, three criteria must be satisfied:

1. Unauthorised access to or unauthorised disclosure of personal information occurs (or a loss of personal information which is likely to lead to unauthorised access or disclosure);

2. The breach is likely to result in serious harm to one or more individuals; and

3. Prevention of the risk of serious harm through remedial action has not been successful.

No specific time periods are prescribed for notification, however suspected breaches should be investigated within 30 days where possible.

Sector specific requirements

Under Prudential Standard CPS 234 (Information Security), providers of banking, insurance and superannuation services must notify the Australian Prudential Regulatory Authority (**APRA**) of information security incidents which:

1. Materially affect the notifying entity or the interests of its depositors, policyholders, beneficiaries or other customers, or

2. Have been notified to other regulators, either in Australia or overseas.

Notifications must be made to APRA within 72 hours.

Additionally, critical cyber security incidents affecting critical infrastructure assets within 11 key sectors (including banking, data storage and education) must be notified to the Australian Cyber Security Centre within 12 hours under the *Security of Critical Infrastructure Act 2018* (Cth).

Upcoming or recent changes

The maximum civil penalties payable under the Privacy Act (including for failure to comply with the notifiable data breach regime) increased in December 2022 from AUD 2.22 million to the greater of:

- AUD 50 million;

- three times the value of the benefit resulting from the breach; or

- 30% of the adjusted turnover of the entity in the 12 months prior to the breach.

This change was driven, at least in part, by the response to a number of large-scale data breaches occurring in 2022, including those suffered by the telecommunications provider Optus and private health insurer Medibank.

Insights

Since the scheme was introduced, the health sector has consistently been the highest reporting sector (for example, in the period January – June 2022 the health sector accounted for around 20% of all reported breaches), followed by the finance sector.

Increasingly, a material proportion of breaches (41% of all notifications in the period January – June 2022) are attributable to cyber security incidents, with phishing, ransomware and comprised credentials being the most commonly reported types of incidents.

Key contacts

Tim Lyons
Partner
tim.lyons@dlapiper.com

Nicholas Boyle
Partner
nicholas.boyle@dlapiper.com

Sarah Birkett
Senior Associate
sarah.birkett@dlapiper.com

China

General data breach notification requirements

Under the Cybersecurity Law, which governs both personal and non-personal data, "network security incidents" must be reported to the Cyberspace Administration of China (**CAC**) and, if the incident may result in harm to the rights and interests of the affected individuals, to those individuals as well.

Network security incidents are incidents that fall within one of the following seven categories:

1. Incidents associated with hazardous programs and where security defects or vulnerabilities are found in network products or services, such as Trojan horse or computer virus incidents.

2. Cyber-attacks such as network attacks, vulnerability attacks, phishing incidents etc.

3. Incidents relating to information destruction such as information leakage, theft, loss etc. This is also confirmed by the Data Security Law.

4. Content incidents such as the spread of banned information that affects social stability.

5. Infrastructure failures such as software or hardware breakdown.

6. Cyber security incidents resulting from natural disasters and other emergencies.

7. Any other incidents not included in the above categories, which the regulatory authority considers notifiable.

Further guidance has been developed setting out when an actual or suspected network security incident may be potentially reportable. The China National Internet Emergency Center may also be contacted to provide guidance.

Specifically for personal data, the Personal Information Protection Law (**PIPL**) reiterates that, where there is an actual or potential personal data breach (as defined), the data controller must notify the CAC and other applicable industry regulators and the affected individuals.

Sector specific requirements

- **General personal financial information:** any leakage, damage, loss or unauthorised alteration of personal financial information must be reported to the People's Bank of China and affected individuals if it may endanger the physical or property safety of financial consumers; or otherwise adversely impact the financial consumers. The deadlines for notification range from immediate to within 72 hours, depending upon the severity of the incident for affected individuals.

- **Securities industry:** a malfunction of network systems must be reported to the China Securities Regulatory Commission. The level of reporting varies based on the severity of the incident, ranging from updates every 30 minutes until the system resumes operation to a "summary report after the incident is resolved", etc.

- **Children's personal information:** any actual or suspected breach, damage or loss of children's personal information which may cause serious consequence must be immediately reported to the CAC and the affected minors/their parents or guardians.

Upcoming or recent changes

The Draft Network Data Security Management Regulation (which, if implemented, will supplement the PIPL) clarifies that incidents involving any of the following must be notified to the CAC and other relevant regulators within eight hours:

- personal data of more than 100,000 individuals; or
- any important data.

A second report to the CAC would then be required within five working days of the incident being resolved.

Additionally, we understand that regulators are looking to develop further guidelines regarding the management of network security incidents, modelled on ISO/IEC 27035-1/2:2016.

Insights

Failure to report could result in warnings and orders of rectification being issued by the CAC. In addition, administrative fines of up to 5% of the previous year's annual revenue or RMB 50,000,000 for the organisation and RMB 100,000 for the responsible person could apply if the offence is severe (e.g. hazardous to cyber security).

Key contacts

Carolyn Bigg
Partner
carolyn.bigg@dlapiper.com

Venus Cheung
Registered Foreign Lawyer
venus.cheung@dlapiper.com

Amanda Ge
Of Counsel
amanda.ge@dlapiper.com

Hong Kong

General data breach notification requirements

There are currently no mandatory reporting requirements for data breaches in Hong Kong.

However, the voluntary reporting of incidents is encouraged by the Office of the Privacy Commissioner for Personal Data (**PCPD**) via an online notification form.

The PCPD has also issued a Guidance on Data Breach Handling and the Giving of Breach Notifications (revised 2019) to assist data users in handling data breaches.

Sector specific requirements

Again, there are no mandatory reporting requirements. However the reporting of "serious" incidents to the Hong Kong Monetary Authority is expected as soon as practicable after becoming aware of the incident.

Serious incidents include those that are likely to have a significant impact on the entity's reputation, affect a large number of customers or involve sensitive customer data.

Upcoming or recent changes

Compared to the rapid and extensive changes to data protection laws in neighbouring jurisdictions, developments in Hong Kong have been slow.

However, potentially as a response to several, high-profile data breaches in Hong Kong in recent years, and in order to stay aligned with international standards (such as the GDPR), proposed amendments to the Personal Data (Privacy) Ordinance were put before the Legislative Council in January 2020.

The amendments include the introduction of a mandatory data breach notification, however there is no clear timeline on when this change will be implemented.

Insights

Several high-profile data incidents in recent years, including a data leak incident in 2022 reported by a hotel chain which affected approximately 1.2 million customers, have prompted the PCPD to take a more active approach in following up with data users and conducting investigations to protect public interest.

Data breaches and data security are increasingly areas of enforcement focus. Priority areas of the PCPD's enforcement also include direct marketing contraventions and cases which concern doxxing.

Hong Kong introduced anti-doxxing legislation in September 2021. The law empowers the PCPD to investigate and prosecute individuals who disclose the names and other details of private individuals and their families online without consent, with an intent to cause harm or being reckless about the harm caused.

Key contacts

Carolyn Bigg
Partner
carolyn.bigg@dlapiper.com

Venus Cheung
Registered Foreign Lawyer
venus.cheung@dlapiper.com

Jane B. Li
Associate
jane.li@dlapiper.com

Japan

General data breach notification requirements

Under changes to the Act on the Protection of Personal Information (**APPI**) made in April 2022, personal data breaches must be reported to the Personal Information Protection Commission (**PPC**) if they are likely to:

- involve Sensitive Information;
- harm an individual's property (such as breaches involving credit card numbers or other financial information);
- be caused by a wrongful purpose (such as breaches caused by unauthorised access, ransomware etc); or
- involve over 1,000 data subjects.

Additionally, personal data breaches must be notified to affected individuals immediately.

However, if a factual situation demonstrates that the personal data which has been disclosed was not accessible by a third party (such as where the data is encrypted), a report to the PPC or a notification to data subjects are not mandatory.

In addition, the PPC guidelines suggest that companies make necessary investigations and take any necessary preventive measures.

Sector specific requirements

Specific notification requirements also apply:

- for personal data breaches suffered by businesses in financial sectors, under the Guidelines for Protection of Personal Information in Financial Sectors; and
- for certain serious breaches of MyNumber, the ID number issued to Japanese residents, such as where more than 100 data subjects are affected.

Insights

Failure to report a data breach to the PPC itself does not trigger any penalties. If the PPC finds that a business operator has not filed a mandatory data breach report then the PPC may recommend the business operator rectify such violations of the APPI. If the business operator does not voluntarily comply with such recommendation, the PPC may formally order the business operator to rectify such noncompliance. If the business operator fails to comply with such formal order, the business operator (if it is a legal entity) may be punished by a fine of up to JPY 100 million, and individuals responsible for a breach (such as directors or employees) may also be subject to fines of up to JPY 1 million or imprisonment for not more than 1 year.

Key contact

Tomomi Fujikouge
Of Counsel
tomomi.fujikouge@dlapiper.com

New Zealand

General data breach notification requirements

Mandatory data breach reporting was introduced under the Privacy Act 2020 (**Privacy Act**) in December 2020.

The mandatory data breach reporting regime moves New Zealand closer to international best practice. Similar to the Australian regime, any organisation carrying on business in New Zealand that suffers a privacy breach that it is reasonable to believe has caused or is likely to cause serious harm to affected individuals must notify the Privacy Commissioner and the individuals concerned as soon as practicable after becoming aware of the breach. Although not binding, the Privacy Commissioner's guidance states that notifiable privacy breaches should be notified to the Privacy Commissioner within 72 hours.

A privacy breach is any unauthorised or accidental access to, or disclosure, alteration, loss, or destruction of, personal information, or any action that prevents an organisation accessing personal information it holds (on a temporary or permanent basis). The Privacy Act includes guidelines for assessing the likelihood of serious harm, including:

- any action taken to reduce the risk of harm following the breach;
- whether the personal information is sensitive in nature;
- the nature of the harm that may be caused to affected individuals;
- who obtained (or could obtain) the personal information as a result of the breach (if known); and
- whether the personal information is protected by a security measure.

There are some circumstances where individuals do not have to be notified, or notification can be delayed. An example given is where an organisation's security systems were shown to be vulnerable as a result of a privacy breach – public notification could risk wider exploitation of the vulnerability and should be delayed to prevent the risk of more harm (although the Privacy Commissioner would still need to be notified).

Failure to notify the Privacy Commissioner of a notifiable privacy breach (without reasonable excuse) is an offence punishable by fine of up to NZUSD10,000. Failure to notify an affected individual could be an 'interference with privacy', resulting in a complaint to the Human Rights Review Tribunal and, in serious cases, a damages award.

Sector specific requirements

Additional data breach notification requirements apply for the banking and finance sector. As part of the full Financial Advice Provider Licence Conditions, the Financial Markets Authority (**FMA**) requires all licensees to notify the FMA of any event that materially impacts the information security of critical technology systems within 10 working days of the licensee becoming aware of that event. A material event is one where the confidentiality, integrity or availability of information and/or technology systems have been compromised. For example, notification is not required for minor events such as receiving a phishing email but notification should occur if that phishing campaign results in the compromise of data or sensitive information or financial loss.

Listed companies may also be required to notify stock exchanges on which they are listed (e.g., the NZX) and public sector bodies may be required to notify their responsible Minister.

Insights

New Zealand: Significant changes to NZ's Privacy Act – but where is the bite? – Privacy Matters (dlapiper.com)

Key contact

Nick Valentine
Partner
nick.valentine@dlapiper.com

Singapore

General data breach notification requirements

"Notifiable breaches" must be notified to the Personal Data Protection Commission (**PDPC**) as a soon as practicable and no later than three calendar days after the data breach is assessed to fall within the notification criteria. A notifiable data breach is:

- any data breach that results in, or is likely to result, in "significant harm" to the affected individuals; or
- any data breach that is of a significant scale (i.e. involves personal data of 500 or more individuals).

Breaches must also be notified to affected individuals as soon as practicable, at the same time or after notifying the PDPC if:

- the data breach results in, or is likely to result in, significant harm to the affected individuals; or
- instructed to do so by a prescribed law enforcement agency or directed by PDPC.

Sector specific requirements

REPORTING REQUIREMENTS FOR FINANCIAL INSTITUTIONS

Under various technology risk management notices issued by the Monetary Authority of Singapore (**MAS**), applicable financial institutions must notify MAS of any system malfunction or IT security incident that:

- has a severe and widespread impact on the bank's operations; or
- materially impacts the bank's service to its customers.

Notifications must be made to MAS as soon as possible and not later than one hour following discovery of the relevant incident. A root cause and impact analysis report must be submitted to MAS within 14 days from the discovery of the relevant incident (or such longer periods as the MAS may allow).

REPORTING REQUIREMENTS FOR OWNERS OF CRITICAL INFORMATION INFRASTRUCTURE

Under Singapore's Cybersecurity Act, an owner of a critical information infrastructure must:

a) within two hours after becoming aware of a cybersecurity incident, notify the Commissioner of Cybersecurity of the occurrence of the cybersecurity incident with the following details:

i) the critical information infrastructure affected;

ii) the name and contact number of the owner of the critical information infrastructure;

iii) the nature of the cybersecurity incident;

iv) the resulting effect that has been observed; and

v) the name, designation, organisation and contact number of the individual submitting the notification; and

b) within 14 days after a), provide the following supplementary details to the fullest extent practicable using the form set out at https://www.csa.gov.sg –

i) the cause of the cybersecurity incident;

ii) its impact on the critical information infrastructure, or any interconnected computer or computer system; and

iii) what remedial measures have been taken.

Upcoming or recent changes

The maximum financial penalty for data breaches has been increased to the higher of:

i) up to 10% of an organisation's annual turnover in Singapore (for organisations with annual turnover that exceeds SGD10 million); or

ii) SGD1 million.

In addition, the outsourcing and reporting requirements for technology risk management have been codified into law with amendments to the Banking Act and the passing of the Financial Services and Markets Act 2022 (**FSMA**). Once the FSMA (and the technology risk management sections therein) fully comes into force, among other things, failure by a financial institution to comply with MAS' directions will constitute a breach and fines not exceeding SGD1 million per breach may be issued.

Key contacts

Carolyn Bigg
Partner
carolyn.bigg@dlapiper.com

Yue Lin Lee
Senior Associate
yuelin.lee@dlapiper.com

Thailand

General data breach notification requirements

The Personal Data Protection Act B.E. 2562 (2019) (**PDPA**) came into force on 28 May 2019. However, full implementation did not occur until 1 June 2022.

Under the PDPA, data controllers must notify the Personal Data Protection Committee (**PDPC**) of personal data breaches within 72 hours. The exception to this is where a personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.

Data controllers must also notify affected individuals following a personal data breach. Details on the notification procedure and exemption has been announced under the Notification of the PDPC on Rules and Methods of Personal Data Breach Notification B.E. 2565 (2022).

Data processors must notify personal data breaches to the relevant data controllers within 72 hours of becoming aware of the breach.

Sector specific requirements

The Bank of Thailand's Data Governance Guideline encourages financial institutions to implement measures to prevent data breaches or lessen the potential impacts of a breach, as well as develop a contingency plan in case of a breach.

In addition, the Office of Insurance Commission recently issued Guidelines on Customer's Data Protection to assist insurance companies with the implementation of security measures to protect the personal information of their customers.

Upcoming or recent changes

Under the PDPA, data controllers may be subject to civil liability, criminal liability and/or administrative liability for failing to comply with the PDPA's requirements, including obligations to report applicable data breaches.

The PDPC was established in early 2022, and is expected to publish additional guidelines on the compliance with the obligations under the PDPA.

Insights

Several high profile data breaches occured in Thailand in 2022.

In January 2022, the IT system of the Thai University Central Admission System (**TCAS**) was hacked and personal data of over 23,000 students were exposed. In response to this, the admission database was shut down, and TCAS's website and security system were subsequently upgraded to improve protection of personal data.

In February 2022, Advanced Info Service plc. (**AIS**), one of the biggest telecommunications companies in Thailand, experienced a data breach caused by a ransomware attack. The personal data of approximately 100,000 customers was compromised. AIS explained the incident to The National Broadcasting and Telecommunications Commission, upgraded its security systems, and filed a report with the Thai police to commence legal proceedings against wrongdoers.

Given that the provisions on data protection and penalties under the PDPA were not effective at the time of these incidents, there has been no enforcement action by the PDPC.

Key contacts

Samata Masagee
Partner
samata.masagee@dlapiper.com

Tanadol Rungruengnoravet
Associate
tanadol.rungruengnoravet@dlapiper.com

Thank you