RPC

Upcoming changes to data protection legislation in Asia

December 2020

ADVISORY | DISPUTES | REGULATORY | TRANSACTIONS

Catching up – data privacy laws in Asia are changing

The data privacy landscape in Asia is varied, complex and evolving. We are already seeing the wheels of change in motion as the data privacy laws of several Asian jurisdictions are being updated to reflect more closely the European data protection regime. This article summarises some of those changes.

Introduction

In Asia, the data privacy landscape is varied, complex and evolving. Many, but not all, jurisdictions have some form of data protection regime, comprising of data protection and/or data security laws (or a combination of both).

To add to these differing approaches, many Asian jurisdictions are in the process of substantially updating their data protection regimes. For example, in 2019 Thailand introduced its Personal Data Protection Act which imposes data use restrictions, civil liability for misuse and sanctions. The Act was due to come into effect in May 2019, but full implementation has been postponed until May 2020.

The tables below provide a brief overview of some of the key changes which companies can expect to see coming into force in Hong Kong, Singapore, Japan and Taiwan in the near future.

Since these upcoming changes are increasing the level of protection afforded to data subjects, organisations operating in Asia markets will need to assess the impact of the changes on their business and take steps to ensure compliance. In the same way that data protection regulation is stringent in the EU market, the Asia market is fast becoming an environment in which data is protected with greater care, and mandatory breach notification obligations. Failure to follow the updated requirements could result in substantial penalties and reputational damage.

Hong Kong

Key amendments to the Personal Data (Privacy) Ordinance (PDPO)

ISSUE	CURRENT LAW (PDPO)
Definition of personal data	◦ Information relating directly or indirectly to an "identified" living individual
Data retention policy	◦ No specific requirement (retention no longer than necessary)
Regulation of data processors	◦ No direct regulation
Data breach notification (privacy regulator)	◦ No requirement (but recommended)
Data breach notification (data subjects)	◦ No requirement (but recommended)
Sanctioning powers	◦ Fine/imprisonment only if breach of PDPO continues after enforcement notice
'Doxxing' (non-consensual publication of personal data)	◦ Fines/imprisonment "on conviction"

Hong Kong's PDPO originally came into force in 1996, and was amended in 2012, largely to introduce restrictions on direct marketing. It was designed in a previous era of data use.

In January 2020, the Hong Kong SAR Government has proposed to update the PDPO to adopt a harder regulatory approach. The Privacy Commissioner for Personal Data (PCPD) will obtain powers to impose direct sanctions. It is expected to take on more of an enforcement role, particularly in light of the PCPD's new MoU with the Information Commissioner's Office in the UK this year to collaborate on joint investigations and enforcement actions.

PROPOSAL	IN FORCE
Information relating directly or indirectly to an "identifiable" living individual	TBC
Mandatory requirement for a "clear" retention policy	TBC
Direct regulation of data processors or sub-contractors	TBC
Mandatory notification to PCPD within specific timeframe (timing TBC)	TBC
Mandatory notification within specific timeframe (timing TBC)	TBC
PCPD power to impose direct administrative fines linked to annual turnover	TBC
Wider powers for the PCPD, eg removal requests and investigation/prosecution	TBC

The proposed amendments to the PDPO, which are still being considered by the Legislative Council, would give the PCPD the power to impose direct administrative fines linked to annual turnover of the data user. It is not yet known how fines would be calculated but the Legislative Council papers refer both the current positions in Singapore (where a maximum fine of SGD1 million can be imposed) and under the GDPR (a maximum fine of EUR 20 million or 4% of a company's global annual turnover in the preceding year, whichever is higher).

The new rules would also impose mandatory breach notifications to both the PCPD and relevant data subjects within a specific timeframe when a data breach has occurred which presents a real risk of significant harm. The Legislative Council papers recommend that the timeframe for notifying should be as soon as practicable and, in any event, within five business days of becoming aware of the data breach. This amendment would not be as onerous as under the GDPR (which requires notification within 72 hours of knowledge) but steps up the obligations on data users that fall under the Ordinance.

Singapore

Key amendments to the Personal Data Protection Act (PDPA)

ISSUE	CURRENT LAW (PDPA)
Data breach notification (privacy regulator)	◦ No general statutory requirement (but recommended, plus sector specific obligations)
Data breach notification (data subjects)	◦ No general statutory requirement (but recommended, plus sector specific obligations)
Sanctioning powers	◦ PDPC able to impose penalty for breach, up to SGD 1 million
Individual accountability for data breach	◦ No provision

In Singapore, the data protection regime continues to evolve and is becoming more robust. Recent amendments to the PDPA, which were passed by Parliament in November 2020 and are likely to come into force in early 2021, will mandate important recommendations from the Personal Data Protection Commission (PDPC) best practice guidelines. Further guidelines will be issued when the new rules come into effect, however it should be noted that there is no transition period, and therefore businesses should take steps to comply with the new rules now.

If the breach is of a significant scale (ie a breach involving the personal data of 500 or more individuals), the amendments will impose mandatory breach notifications to both the PDPC and relevant data subjects within 72 hours of the data user becoming aware that the breach is notifiable. This approach follows the current best practice under the PDPC guidelines.

PROPOSAL	IN FORCE
• Mandatory notification to PDPC within 3 days from the date the data breach is assessed to be notifiable • Breach notifiable if of a significant scale (affecting 500 individuals or more)	Early 2021
• Mandatory notification if breach likely to (or did) result in significant harm	Early 2021
• Financial penalty increased to the higher of: – SGD 1 million, or – 10% of annual gross turnover if such turnover exceeds SGD10 million	Early 2021
• Individuals accountable for "egregious mishandling of personal data", incl. knowing or reckless unauthorised: – disclosure – use for a wrongful gain or causing wrongful loss – re-identification of anonymised data • Fine ≤ SGD5,000/imprisonment up to 2 years/both	Early 2021

Organisations with global policies for data incidents should therefore localise a response plan for the new requirements in Singapore. Having such a plan may also improve an organisation's chances of having a voluntary statutory undertaking being accepted by the PDPC in lieu of it carrying out an investigation into the organisation.

The amendments will also increase the sanctioning powers of the PDPC. Financial penalties will increase to either SGD1 million or 10% of a company's gross annual turnover in Singapore if such turnover exceeds SGD10 million (whichever is higher). This change has major implications for larger organisations which operate in the Singapore market. For example, businesses that engage in telemarketing or the bulk sending of marketing emails will need to comply with the updated requirements or risk being subject to a large financial penalty.

Japan

Key amendments to the Act on the Protection of Personal Information (APPI)

ISSUE	CURRENT LAW (APPI 2017)
Expanding rights of data subjects	◦ Right to *request* access, correction, deletion and cessation of use of personal data that is/is intended to be retained for +6 months ◦ Opt-out: data transfers to 3rd parties allowed unless data subject opts out
Pseudonymisation (processing personal data so it cannot be used to identify the individual)	◦ No specific provision
Extra-territorial application	◦ Applies to foreign entities who obtain personal data of data subjects in Japan
Data breach notification	◦ No requirement under most circumstances
Sanctions	◦ Fines of up to ¥300,000-500,000 (approx. USD2,900-4,800)

Amendments to the Japanese APPI were passed in June 2020 and follow the trend of creating a more robust data protection regime with more authority for the regulatory body, the Personal Information Protection Commission (PPC). The amended APPI, which will mostly come into force within two years, will have a major impact on businesses that operate in Japan (as well as many global organisations that may be affected by its extra-territorial aspects).

The new rules will allow the PPC to order foreign companies, which either handle the personal data of data subjects in Japan or provide goods or services in Japan, to submit information on how that data is being managed. Further, the PPC will be able to publish the

PROPOSAL (APPI 2020)	IN FORCE
• Right to *require* deletion or disclosure where there is a possibility of violating rights/legitimate interests (includes short term data) • Restriction on opt-out: data transfers allowed on opt-out basis only to first level 3rd party recipients	2022
• Consent required to transfer pseudonymised data in certain circumstances	2022
• Commission has authority to supervise and sanction foreign entities (if provide goods/services in Japan, and handle personal data of data subjects in Japan)	2022
• Mandatory notification to the PPC and relevant data subjects, if incident may cause violation of rights/interests • Preliminary report ASAP (no timeline indicated)	2022
• Fines increased up to ¥100M (approx. USD950k) • False submission of reports – fine up to ¥500k • Potential fines for individuals	2022

fact that an overseas company has not followed a PPC order. Penalties imposed by the PPC will also increase, up to ¥100 million for companies. Individuals responsible for a breach may also be subject to individual penalties.

Breach notifications to both the PPC and relevant data subjects will be mandatory as soon as possible following a data breach, in the event of an incident which may cause the violation of individual rights and interests (similar to the notification threshold envisaged in Hong Kong). Businesses would need to provide a preliminary report to the PPC and data subjects as soon as possible, followed by a more detailed report regarding cause and remediation.

Taiwan

Key amendments to the Personal Data Protection Act (PDPA)/ Cybersecurity Act (CSA)

ISSUE	CURRENT LAW (PDPA/CSA)
Definition of personal data (PDPA)	◦ Information/data which may be used to identify a natural person ◦ Directly or indirectly
Protections afforded to children under 13 (PDPA)	◦ No provisions
Definition of 'critical infrastructure provider' (CSA)	◦ Those who maintain or provide critical infrastructure either in whole or in part ◦ To be designated by competent industry authority (and ratified)
Government agency obligations (CSA)	◦ Several cyber security management obligations

Taiwan adopts a 'split' data protection regime, with personal data protected by both the PDPA and the CSA. The PDPA, which primarily concerns data privacy, applies to businesses; whereas the CSA, which is aimed at data security (regardless of whether such data is 'personal data' as defined under the PDPA), applies only to those businesses which are deemed to be critical infrastructure providers, designated by the sectoral regulator and ratified by the Executive Yuan.

Both Acts are currently under review by the Legislative Yuan and the underlying intention to the amendments is to clarify the law, more than to effect substantial change. The PDPA aims to meet EU standards so that Taiwan may obtain an Adequacy Decision from the European Commission. For example, the proposed amendments to the PDPA include increased protections for children under the age of thirteen.

PROPOSAL	IN FORCE
• Specification of which types of web-based data constitute personal information	TBC
• Requiring a legal representative to approve collection and processing • Prohibiting sale or other commercial use of data	TBC
• Clarification by specific examples: government offices, communication networks, national defense and military facilities, and businesses engaged in private energy, transportation, finance, health care, and food and water supply	TBC
• Additional requirement to prepare information security budget	TBC

An Adequacy Decision would allow personal data to flow from the EU (and Norway, Liechtenstein and Iceland) to Taiwan without further safeguards, treating transfers to Taiwan as if they were intra-EU transmissions of data, ie the same guarantees as those under EU law will continue to apply. In Asia, only Japan has so far obtained an Adequacy Decision.

Conclusion

Data protection regimes in Asian jurisdictions are catching up to the GDPR (hailed as a world-leading data protection regime for its extra-territorial application and significant sanctions). International businesses across Asia, often aware of the key requirements of GDPR, will now need to be aware of more stringent rules and regulations applicable in several Asian jurisdictions.

This article has provided just a snapshot of a handful of jurisdictions in Asia. Other jurisdictions' laws (beyond the reach of this short summary) should also be considered carefully, eg the upcoming and expansive changes to the data protection regime in Mainland China.

In summary, any business that is established or operates in locations across Asia (or is looking to set up a presence in Asia) should keep a close eye on the changing legal landscape across the region and the data that the business controls or processes in such a large and diverse market. Thoroughly researching the regulatory regime in each Asian jurisdiction and implementing a robust and compliant data protection policy, data map and data breach plan will be key to navigating the evolving Asian data protection landscape.

RPC frequently advises its clients on all aspects of data privacy and cyber security matters – please do get in touch with us if you would like to discuss how we can help.

AUTHORS

Jonathan Crompton
Partner
T +852 2216 7173
M +852 6822 5016
jonathan.crompton@rpc.com.hk

Summer Montague
Partner
T +65 6422 3042
M +65 9667 6152
summer.montague@rpc.com.sg

Stephanie Northcott
Registered Foreign Lawyer
T +852 2216 7200
M +852 6827 3500
stephanie.northcott@rpc.com.hk

Sumyutha Sivamani
Senior Associate
T +65 6422 3065
M +65 8809 2206
sumyutha.sivamani@rpc.com.sg

Sakshi Buttoo
Legal Manager
T +852 2216 7211
M +852 6977 2312
sakshi.buttoo@rpc.com.hk

rpc.com.hk