RPC

Changes to data protection legislation in Asia – 2022 update (including Mainland China)

July 2022

ADVISORY | DISPUTES | REGULATORY | TRANSACTIONS

The tide continues to turn – Asian data privacy laws in flux

This update follows on from our original article Upcoming changes to data protection legislation in Asia.

Looking back on the last 18 months, the data privacy laws of several Asian jurisdictions have been updated to incorporate stronger protections for individuals' personal data. This article provides an update on a handful of jurisdictions in Asia and summarises some of those main changes, including the far-reaching implications of the new data protection law in Mainland China.

Hong Kong | Singapore | Japan | Taiwan | Mainland China

Introduction

Many jurisdictions in Asia are in the process of updating, or have already updated, their data protection regimes. Many of these changes were expected developments following a lengthy period of legislative debate, as a part of incremental steps towards strengthening data protection. For example, in Hong Kong, the Personal Data (Privacy) Ordinance has been amended include new provisions regarding 'doxxing'.

Other jurisdictions have made more wholescale changes which represent a shakeup of the data protection regime, with both territorial and extra-territorial effects. For example, the Personal Information Protection Law in Mainland China, which came into effect on 1 November 2021, appears to reflect the European GDPR in its commitments to data protection and introduces a new standard for data protection – it also has broad extra-territorial application.

This article provides a brief overview of some of the key changes made, or expected shortly, in Hong Kong, Singapore, Japan, Taiwan and Mainland China.

Organisations operating in Asian markets will need to assess the impact of these changes on their businesses and take steps to ensure compliance. The data protection regimes in Asia are catching up to the GDPR in the EU, although there is no common data protection regime. Asian jurisdictions protect data differently, but increasingly with greater care and greater pro-active steps needed by those who use and process data. Failure to adhere to these stricter requirements could result in substantial penalties and, perhaps more importantly, significant reputational damage.

Hong Kong

Our previous article listed a number of proposed amendments to Hong Kong's Personal Data (Privacy) Ordinance (PDPO). On 29 September 2021, the Hong Kong Legislative Council passed an amendment bill which focusses largely on only one specific subject matter – 'doxxing'.

Although there is no indication of when, it is expected that some of the other proposed amendments should form part of a larger package of amendments to the PDPO in the future.

Amended PDPO

The amendments to the PDPO took effect from 8 October 2021. They include provisions specifically aimed at combatting doxxing activities. Doxxing is the act of publishing private or identifying information about an individual on the internet, typically for malicious purposes – this has become more common in Hong Kong in recent years, including by protaganists on both sides of the Hong Kong protests. In Hong Kong, between June 2019 and April 2021, the Privacy Commissioner for Personal Data (PCPD) received around 6,000 complaints of doxxing-related activities.

The new provisions fall into three categories:

- the criminalisation of doxxing offences, with more severe sanctions where the doxxing caused actual harm to the victim(s)
- criminal investigation and prosecution powers for the PCPD in relation to such offences, and
- power for the PCPD to direct the removal of doxxing content and issue cessation notices with extra-territorial effect.

Doxxing offences

The new two-tier offences under Section 64 of the PDPO are as follows:

OFFENCE	PENALTY ON CONVICTION
Section 64 (3A): A person commits an offence if they disclose personal data of a data subject without their consent, with an intent to cause specified harm to the data subject or any of their family members, or being reckless as to whether any specified harm would be or likely be caused	A fine of up to HK$100,000 and up to two years' imprisonment
Section 64(3C): A person commits an offence if, in addition to the above, any specified harm is actually caused to the data subject or their family members	A fine of up to HK$1,000,000 and up to five years' imprisonment

"*Specified harm*" is defined quite broadly and includes pestering, harassment, molestation, threats or intimidation, physical harm, psychological harm, harm causing the person to be reasonably concerned for their safety or wellbeing, and damage to property.

Applicable defences include:

- a reasonable belief that the disclosure was necessary for preventing or detecting crime
- a reasonable belief that the data subject gave their consent to the disclosure
- a reasonable belief that disclosure was in the public interest and was made for news activity purposes, and
- where the disclosure was required or authorised by law or a court order.

PCPD powers to enforce, investigate and prosecute

Before the PDPO was amended, the PCPD was required to refer doxxing cases to the Hong Kong Police Force and the Department of Justice for investigation and prosecution. This delayed the handling of cases. Now, the PCPD itself can conduct its own investigations, and has the power to request relevant materials, documents and information and to stop, search and arrest without a warrant any person reasonably suspected of committing a doxxing offence.

The PCPD also has the power to initiate a prosecution in respect of summary offences at the Magistrates' Court.

For more serious cases, the PCPD can still refer cases to the Hong Kong Police Force or the Department of Justice.

New provisions also empower the PCPD to issue cessation notices with extra-territorial effect to Hong Kong persons or non-Hong Kong service providers where there has been a disclosure of personal data of a data subject (who is either present in Hong Kong or a Hong Kong resident) via a written or electronic message without the data subject's consent (meeting the elements of the first of the two-tier offences). This can be used to target social media users and, potentially, platforms.

The cessation notice may demand:

- removal of the disclosure from the relevant platform, eg websites and mobile applications
- discontinuance of hosting services for whole or part of the platform on which the disclosure was made, or
- restriction of access to the disclosure or the relevant platform.

Failure to comply with a cessation notice may result in a fine of HK$50,000 and two years' imprisonment on first conviction. On subsequent convictions, the fine may increase to HK$100,000.

Comment

The PCPD's *Implementation Guideline* on the amended PDPO states that the new provisions target the disclosure of personal data without consent in a doxxing context only. However, the new two-tier offences adopt wide descriptions without mentioning the term 'doxxing' which could enable the PCPD to use the new investigative powers and offences more broadly, particularly since the PCPD's power to request materials, documents and information appears not to be limited only to the new two-tier offences.

So far, though, the new provisions have been used only in the doxxing context for which they were intended. The PCPD arrested its first two suspects under the new doxxing provisions (for suspected breach of section 64(3A) PDPO) on 13 December 2021 following a victim's complaint and on 26 April 2021. It conducted a joint operation with the Hong Kong Police Force on 11 May 2022 in which another person was arrested (for suspected breach of section 64(3C) PDPO), and issued its first doxxing charges on 20 May 2022 (against the first arrested suspect).

Between October 2021 and the end of February 2022, the PCPD issued "*more than 460 cessation notices to 12 platforms to request the removal of over 2,400 doxxing messages*".

Beyond individuals, this has implications for both employers and services providers/ online platforms:

- employers should update their internal policies to reflect these changes, in particular to avoid an employee committing an offence of doxxing while working, which could subject the organisation to an investigation, and
- online service providers and social media companies should ensure that they are aware of the new provisions of the PDPO, and create a procedure for responding to and complying with any demand received from the PCPD.

As it is an offence not to comply with an investigation, if in doubt, service providers and any companies receiving a demand or cessation notice should seek legal advice.

The PDPO continues to evolve. The 2021 amendments to the PDPO focussed on doxxing, while leaving other expected amendments such as mandatory data breach reporting and a power for the PCPD to impose direct administrative fines. The PCPD has confirmed, however, that she is working with the HKSAR Government to implement these and other amendments to the PDPO. The PDPC has also recently issued guidance on recommended model clauses for cross-border personal data transfers (see Hong Kong data protection: cross-border transfers of personal data). We will cover key developments in separate articles.

The PCPD has also recently issued Guidance on Recommended Model Contractual Clauses for Cross-border Transfer of Personal Data. This Guidance note is explained in more detail in our previous article.

Singapore

Our previous article listed the key amendments to Singapore's Personal Data Protection Act (PDPA) which came into effect on 1 February 2021. As part of the update to the PDPA, follow-up amendments to the Personal Data Protection (Notification of Data Breaches) Regulations 2021 and Personal Data Protection Regulations 2021 have been made, taking effect on 1 October 2021. These include minor clarifications on what constitutes 'significant harm' for mandatory data breach reporting, ways organisations may provide the business contact information of their Data Protection Officers and defences for egregious mishandling of personal data.

The *Advisory Guidelines on Enforcement of Data Protection Provisions* indicate that the increased financial penalties will take effect on a further date to be notified, and no earlier than 1 February 2022. However, there is no update on when the Data Portability provisions will take effect, which will provide an avenue for individuals with an ongoing relationship with an organisation to request for their personal data to be transmitted in accordance with prescribed requirements to a receiving organisation.

We set out below some key updates in Singapore which occurred in the last 18 months.

Cybersecurity

The Cyber Security Agency of Singapore (CSA) announced, on 5 October 2021, the launch of the updated National Cybersecurity Strategy 2021. In particular, the National Cybersecurity Strategy explains Singapore's plan to advance international norms and standards on cybersecurity in Singapore and to take a proactive stance against cyber threats.

The National Cybersecurity Strategy sets out the numerous ways in which Singapore (and businesses in Singapore) can adopt a robust infrastructure against cybersecurity threats. This is important in light of the increased levels of cyber activity that have been recorded in Singapore. As part of our cyber incident response service work, we have seen an increasing number of Singaporean companies become the targets of cyber incidents such as ransomware attacks.

The first High Court PDPA case

The Singapore High Court handed down its first ever decision under and on the scope of the PDPA on 25 May 2021. In *Bellingham, Alex v Reed, Michael* [2021] SGHC 125, the High Court considered the question of what constitutes "loss or damage", the threshold requirement which data subjects need to satisfy to pursue a right of private action under PDPA.

The High Court held that "loss or damage" must refer only to heads of loss or damage applicable to torts under common law – namely financial loss, damage to property and personal injury including psychiatric illness. Broader concepts of emotional harm (such as humiliation, loss of dignity, injury to feelings and distress) and/or loss of control over personal data are not covered.

Comment

The High Court's decision to adopt a purposive and narrow interpretation of "loss or damage" lowers the potential litigation risk arising from private actions under the PDPA by affected data subjects. Data subjects must now prove that the misuse of personal data results in financial loss, damage to property and personal injury, such as psychiatric illness, in order to pursue a private action.

Of particular importance is the High Court's finding that the purpose of the PDPA was as much to enhance Singapore's competitiveness and position as a trusted business hub as it was to safeguard individual personal data against misuse. The High Court also noted that the position in Singapore differed from the position in other jurisdictions, such as the EU, where the data protection frameworks were driven primarily by the need to recognise the right to privacy of data subjects.

Japan

Our previous article listed the key amendments to Japan's Act on the Protection of Personal Information (APPI) which came into effect on 1 April 2022. That said, stricter financial sanctions had already come into effect, and transitional measures for providing personal data to third parties through an opt-out method had come into effect on 1 October 2021.

Through the latest changes, financial penalties have increased to a maximum fine of ¥100M (approx. USD755k) for companies, and individuals responsible for a breach of APPI may be subject to a fine of up to ¥1M (approx. USD7.5k) and up to a year in prison.

Furthermore, on 24 March 2021, the Cabinet of Japan issued an Order to enforce the amended APPI and the Personal Information Protection Commission (PPC) issued Enforcement Rules for the amended APPI. Together, these documents help to clarify the amended APPI provisions. For example, the Order has provided the following helpful explanations:

- **data breach notification:** the Order has clarified that a notification must be made to the PPC when a breach has or is likely to: (a) involve sensitive personal information; (b) risk property damage; (c) have been committed for an improper purpose, such as a cyberattack; or (d) effect more than 1,000 data subjects. A preliminary report must be made promptly after recognising the breach and a final report must be made within 30 days (or 60 days in the case of (c))
- **pseudonymisation:** the Order has set out processing standards for pseudonymised information (ie processing personal data so that it cannot be used to identify a data subject), which includes the deletion or replacement of the following: (a) descriptions that can identify specific individuals, such as names; (b) individual identification codes; and (c) descriptions that may cause property damage.

Comment

Companies conducting business in or with Japan should be mindful of the stringent nature of the amendments to APPI which will all come into effect in April 2022. Whilst the Order and Enforcement Rules are helpful for companies to understand their personal data obligations when providing goods and services in Japan or handling the personal data of data subjects in Japan, companies should seek legal advice from Japanese counsel if they have any specific queries.

Taiwan

Following our last article, there have been no further updates on the proposed amendments to Taiwan's Personal Data Protection Act (PDPA) and Cybersecurity Act (CSA). Due to the COVID-19 pandemic, the Legislative Yuan's review of both Acts has been on hold.

On 25 May 2021, the Personal Data Protection Office (PDPO) announced that Adequacy talks were still active between Taiwan and the EU. Therefore, as part of Taiwan's pursuit of an Adequacy Decision from the EU, businesses in Taiwan should expect amendments to the Acts to be announced this year. It is expected that the legislative process to amend the Acts will reconvene in the early months of this year.

Mainland China

This article cannot conclude without mentioning the most significant development seen in Asian data protection legislation in the last 12 months – Mainland China's new Personal Information Protection Law.

In 2021, the National People's Congress of the PRC passed the Data Security Law (DSL) and the Personal Information Protection Law (PIPL). Along with the Cyber Security Law (CSL), which was enacted in 2016, the three pieces of Chinese legislation present the three pillars of Mainland China's data protection system which forms an overarching framework for governing data processing and cybersecurity issues.

PIPL

PIPL received a lot of attention around the time it came into effect on 1 November 2021, and with good reason. PIPL provides a robust data protection system which is similar in many ways to the EU's GDPR. Of particular importance to multi-national corporates, PIPL has extra-territorial effect.

Our key takeaways from PIPL are as follows:

- **extra-territoriality:** PIPL applies to companies that process the personal information of Mainland Chinese individuals inside or outside of Mainland China for the purposes of offering products or services to them or analysing and assessing their behaviour. Article 3 of PIPL is very similar to Article 3 of GDPR, both of which set out the extent of their extra-territorial application
- **more rights for data subjects:** PIPL provides more rights for data subjects and appears to emphasise the need for consent before processing personal information. PIPL requires personal information to be processed under one of seven legal bases, which include where the individual has voluntarily and explicitly provided consent to such processing, and where it is necessary to conduct human resources management in an employment context. Separate consent from data subjects must also be obtained when processing sensitive personal information such as biometric data, medical and health data and financial accounts. Data subjects have the right to access and copy their personal information, correct and delete personal information, restrict or refuse the processing of their personal information, and find out the ways in which their personal information is being used. Data subjects can also opt out of targeted marketing, including push notifications and pop-ups
- **restrictions on cross-border transfers of data:** PIPL stipulates that firms with

critical information infrastructure and large amounts of personal information must store this data within Mainland China. If they wish to transfer it out of Mainland China, they will first need separate consent from individuals. Then, they will have to meet certain requirements, such as passing a security assessment of the state cyberspace authority and obtaining the required certification, or entering into a standard contract with the overseas recipient of the data (which will be made available by the cyberspace authority in due course)

- **sanctions/penalties:** companies that contravene PIPL may face a maximum fine of RMB 50m (about HK$60m) or 5% of their annual turnover. Other penalties can include suspension of operation or loss of license. Individuals responsible for a breach may also be subject to a fine of up to RMB 100,000 (about HK$120,000). Other penalties can include disqualification from acting as a director, supervisor, senior manager or data protection officer.

Comment

When PIPL came into effect, it was still subject to implementing regulations that had not been issued. Some of those are still awaited. PIPL therefore presents both uncertainty and an aspirational challenge to companies – the Chinese authorities will expect companies to work towards complying with PIPL while the precise implementing rules are finalised. In the context of personal data, however, it can often be cumbersome to change data compliance and governance processes once they have been implemented.

Companies with businesses or customers in Mainland China need to consider the impact of the new legislation on their operations and data processing activities. Due to the extra-territorial effect of PIPL, companies outside Mainland China that are impacted by the law should already have taken or be taking appropriate steps towards compliance. In many cases, companies may need to conduct a full review of their data processes in order to make the changes necessary to comply with this new 'Chinese GDPR'.

Given the business ties between China and many countries around the world, the new law will pose challenges for many businesses around the globe, particularly those in the retail and e-commerce sector which collect and process consumer data. That said, businesses which already comply with the EU's GDPR should be used to data consolidation and compliance projects and may not need to alter too many of their processes and practices.

Given the potential financial penalties for non-compliance, businesses in any doubt should at least try to comply and seek legal advice from PRC counsel (to whom we would be happy to make introductions).

Conclusion

The costs of data security compliance are part of the modern-day cost of doing business. In the same way that businesses are required to comply with anti-corruption standards and labour rights, data protection is now firmly another spoke to the wheel of operating in the any market, including in Asia.

This article provides just a short summary of recent changes in a handful of Asian jurisdictions. The laws in many Asian jurisdictions continue to change regularly.

As data protection regimes continue to change, with more onerous data protection obligations, it will become important for multi-national corporations to keep abreast of key developments or to face the risk of significant financial penalties (and perhaps more costly reputational damage).

We will continue to follow the legislative developments and provide further updates on key changes in the future.

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

Yuankai Lin
Partner
T +65 6422 3070
M +65 8798 7124
yuankai.lin@rpc.com.sg

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

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

rpc.asia