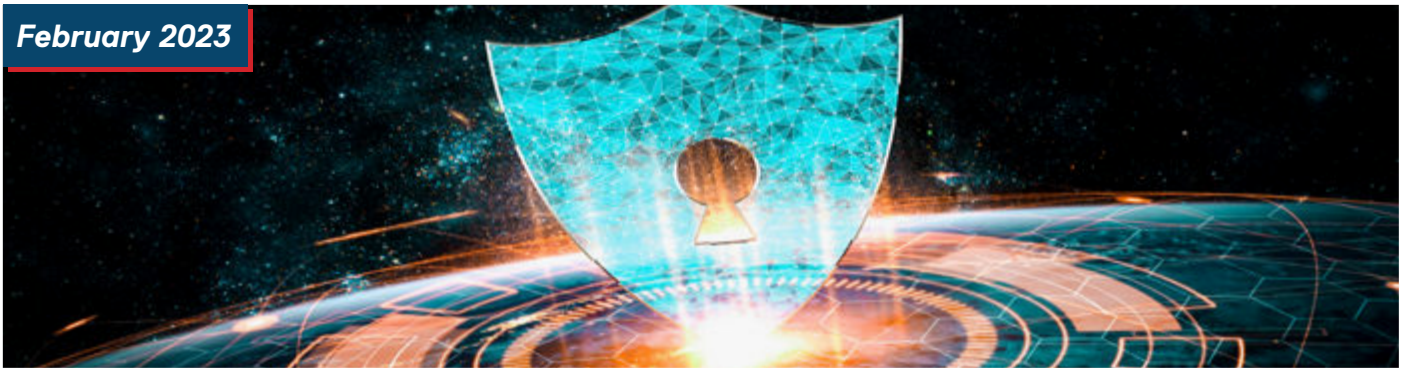
RHTLaw Asia



Year-End Review for Data Protection and Cybersecurity Laws in Major Jurisdictions in Asia for 2022 (Part 2)

Introduction and Overview

In this second part of our Year-End Review for 2022 on data protection and security laws, we look at some of the significant measures taken in major Asian countries and discern a few trends.

Legislative Development Continues in China

The pace of legislation reform on personal data protection continued unabated in China.

After the introduction of the omnibus comprehensive data protection rulebook, China's new Personal Information Protection Law ("PIPL"), on 1 November 2021, the authorities in China did not stop improving and enhancing these new provisions in 2022.

Much of the PIPL has been based on the principles and provisions of the EU General Data Protection Regulation ("GDPR"). The PIPL is neither as prescriptive, nor anywhere near as detailed, as the GDPR. The PIPL instead provides a framework of largely high-level data privacy obligations and is expected to be supplemented by guidance from the Chinese authorities.

One major difference between the GDPR and the PIPL is that while the GDPR is focussed on where the business is established, by contrast, the PIPL is focussed more on where the personal information processing activity happens. If the processing of personal data occurs within China, whether by a company in China or a foreign company without an office in China, the PIPL is applicable. As such, if a company established in China processes personal data of people from overseas, such as in an ASEAN country, the PIPL does not apply to the company's processing activity, as it does not take place in China and it is not processing personal data of people in China.

Under recent administrative rules under the PIPL, personal information can only be transferred outside of China once certain requisite steps are completed and regulatory approval obtained, including, but not limited to clearing a security assessment approved by Cyberspace Administration of China (CAC). On 7 July 2022, the CAC issued the Measures of Security Assessment for Data Export (the "Measures"), which became effective from 1st September 2022. The Measures include specific provisions on the definition of data export, scenarios subject to security assessment for data export, main contents of the security assessment, procedures of the security assessment and responsibilities of the competent authorities.

A Year of Refinement for Hong Kong

Just like in Singapore, legislative refinement of personal data protection seemed to be the theme for Hong Kong in 2022, and there was also a significant court case near the end of the year.

Most of the new developments were to provide more detailed guidance on specific and pertinent nascent areas.

It was telling that focus remained on updating on key areas, such as cross-border transfers and measures to address the Covid-19 virus.

The Office of the Privacy Commissioner for Personal Data, Hong Kong ("PCPD") revised the guidance note for the property management sector in June 2022.

The PCPD also released several new guidance notes:

- Guidance for Employers on Collection and Use of Personal Data of Employees during the Covid-19 Pandemic in March 2022
- Guidance on Recommended Model Contractual Clauses for Cross-border Transfer of Personal Data in May 2022; and
- Guidance Note on Data Security Measures for Information and Communications Technology in August 2022

Hong Kong had also passed a new anti-doxxing law in 2021. In October 2022, a 27-year-old man was the first person to be convicted of this new doxxing offence, by publishing details of an ex-partner without consent and upon his guilty plea and was sentenced to eight (08) months imprisonment on 15th December 2022. This provides an indication as to how serious this conduct is taken by Hong Kong.

Starting Over in India

The comprehensive Personal Data Protection Bill 2019 was originally formulated in December 2019, (the PDP Bill), although perhaps not totally unsurprisingly it was withdrawn in August 2022 following consideration of a long list of recommendations for changes tabled by a Joint Parliamentary Committee in December 2021.

In its place, on November 18, 2022, the Ministry of Electronics and Information Technology of the Government of India released a draft of the new Digital Personal Data Protection Bill, 2022 (the DPDP Bill).

The DPDP Bill reportedly reflects a compromise reached on all relevant parties on those contentious elements within the PDP Bill, amongst which includes the removal of, or at least a severe dilution of, a contentious data localisation requirement.

It remains to be seen what will be the final contents of the DPDP Bill.

A Watershed Year for Indonesia

Indonesia had a watershed year in terms of enacting Data Protection Legislation in 2022.

The Indonesian government ratified a draft of the new omnibus Personal Data Protection law ("PDP Law") on 20th September 2022. This PDP Law is intended to unify the protection of personal data into a single comprehensive legal regime for Indonesia. This PDP Law also provides the additional rights for the data privacy subject over and above those from the previous regulations, including the Minister of Communication and Information Regulation No. 20 of 2016 on the Personal Data Protection on Electronic System ("Regulation No. 20/2016") and the Law No. 11 of 2008 on the Electronic Information and Transaction ("EIT Law").

This PDP Law will establish a dedicated institution operating under the President of Indonesia, that would in the future formulate provisions relating to the implementation of personal data protection, supervise the implementation of personal data protection, enforce administrative law, and facilitate dispute resolution.

This PDP Law is due to come into force on a date set by the Ministry of State Secretariat or 30 days. Parties engage in the data processing activities are obliged to comply with the new law no later than 2 (two) years from September 2022.

This important positive development enables Indonesia to level up its laws to protect personal data with some degree of detail and structure. The familiarity of the proposed mechanisms with data protection laws of other countries would only serve to ease harmonisation of the implementation of the concepts for international transfers of data.

Some of the salient features of the new PDP Law include the following: -

(a) Anyone who collects and or uses personal data is either a Data Controller or Data Processor. There must be some recognised basis for data processing by the Data Controllers.

(b) The Data Controller is required to carry out a Data Protection Impact Assessment (DPIA) if the Personal Data processing carries a high potential risk for the Data Subject.

(c) The PDP Law allows the cross-border transfer of Personal Data from a Data Controller to a Data Controller and/or Data Processor outside Indonesia provided certain conditions are met. The implementation of cross-border data transfer is to be further regulated by a Government Regulation.

(d) Data Controllers are required to make notifications of stipulated content within 72 hours of a data breach.

(e) If a Data Controller performs a merger, separation, acquisition, consolidation, or dissolution of a legal entity, it is required to submit a specified notification of the transfer of Personal Data to the Data Subject. The notification must be submitted prior to the aforementioned corporate actions. Further provisions regarding the procedures to deliver a notification shall be regulated in a Government Regulation.

(f) Finally, the PDP Law provides the following prohibitions and sanctions in relation to violations of the law:

- There cannot be unlawful obtaining, collecting or disclosure of Personal Data of others
- There cannot be use of the Personal Data of others in a manner that contravenes the law; and
- No false Personal Data or fake Personal Data must be created with the intention of benefiting themselves or other persons that may cause harm to other persons.

The punishment for such contravention is severe, with hefty fines, administrative sanctions, and even criminal sanctions possible.

Data Protection Comes of Age in Japan

Another country that focussed on refinement of their data protection laws was Japan.

The most significant changes in Japan were

- Laws that were approved in June 2020 ("the 2020 Amendments") to further amend the Act on the Protection of Personal Information ("APPI") came into force on April 1, 2022.
- The separate data protection law for public sector was integrated into the APPI and became effective on April 1, 2022.
- A new data protection law for local governments will be effective after April 1, 2023.

Salient features of the 2020 Amendments are: -

(a) Personal Data Transfer to a Third Party Outside Japan

The Amended APPI requires consent to transfer personal data outside of Japan (the "opt-in principle") and for this opt-in to be effective, a data collector must enable data subjects to furnish informed consent after having provided certain minimum amount of information and or explanation. This explanation must be to the satisfaction of the Personal Information Protection Commission ("PPC").

(b) Person-Related-Information

The Amended APPI introduced a new concept of "Person-Related-Information," which means information related to an individual that does not fall into the categories of personal information, pseudonymous information or anonymous information.

Before the Amended APPI, unless information falls into the definition of personal information at a data collector transferring the data, it remained outside the scope of the APPI, even when the information is used as personal data at a recipient third party.

To enhance protection for information which may thus be used as personal data after transfer, the Amended APPI requires a Data collector transferring information that does not identify a specific individual to comply with certain specific requirements if it is expected that the recipient of that information will use the information as personal data.

(c) Data Breach Notification

The PPC has enhanced the data breach notification provisions, and now provides for

- Mandatory data breach notification to the PPC under certain situations.
- Two notifications with the PPC, the first being a preliminary notification promptly after becoming aware of the data breach incident and ["promptly" is generally means three to five calendar days] and the second final notification must be filed within a stipulated period of becoming aware of an Incident, after the Data collector has had an opportunity investigate the Incident and to provide a more comprehensive report of the incident. The primary burden of notifying remains with the data collector, even if the handling of the personal data is in the care custody or control of an outsourced third party.

In addition, the Data collector also must give notice of the incident to data subjects "promptly depending on situation" after becoming aware of the Incident.

(d) Pseudonymous Information

Pseudonymous Information is a newly introduced concept under the Amended APPI that allows data collector to use data internally and more flexibly, and without the stress of worrying about mandatory data breach notification amongst other things.

A foreign data collector will be subject to the Amended APPI as long as the foreign data collector processes personal information of data subjects in Japan for its data collector purposes.

The Amended APPI also significantly increases the penalties which may be imposed on businesses, to up to JPY 100 million per violation.

Data collectors that operate in multiple jurisdictions which includes Japan, or if the business holds data of Japanese data subjects, then it must incorporate compliance with the Amended APPI into its broader data management system.

Developments at the OECD

Another milestone was achieved by work done by the Organization for Economic Cooperation and Development ("OECD") in the field of privacy, in 2022.

In December 2022, the thirty-eight (38) OECD countries adopted an intergovernmental agreement on common approaches to safeguard privacy and other human rights and freedoms when accessing personal data for national security and law enforcement purposes ("the Declaration").

The Declaration complements the OECD Privacy Guidelines ("the Privacy Guidelines") and seeks to improve trust in cross-border data flows. It is very important tool to help promote trust in cross-border data flows.

The Privacy Guidelines provide a common reference point for the protection of personal data and aim to facilitate cross-border data flows while upholding democratic values, the rule of law and the protection of privacy and other rights and freedoms, but crucially, these Privacy Guidelines allow for exceptions for national security and law enforcement purposes.

This new Declaration articulates a set of shared principles that reflect common ground of the OECD members' existing laws and practices and complement each other in protecting privacy and other human rights and freedoms.

The principles set out: -

- The legal standards applied when access is sought;
- How access is approved;
- How the resulting data is handled;
- Efforts by countries to provide transparency to the public, including the tricky issues of, such as oversight and redress, which have been challenging to policy discussions.

Significantly, Japan, Korea, Australia and New Zealand are the only named adherents to the Declaration from Asia.

Conclusion

The complete overhaul of the data protection regime in Indonesia in 2022 followed a similar situation in China in late 2021. The significance for both was the enactment of omnibus legislation covering this topic for the very first time.

These changes, coupled with the enhancements and improvements made by the likes of Japan, Hong Kong and Singapore in the last two years, is beneficial for several reasons.

It can help multinational companies who collect and transfer personal data across borders. The harmonisation of laws that carry similar principles will make it easier for them to set up their internal data management systems that can cover broadly most of the jurisdictions in Asia.

Further, it can only but foster better co-operation between Asian countries for a more effective enforcement strategy in the region.

About the Author

Wun Rizwi
Partner
RHTLaw Asia
rizwi.wun@rhtlawasia.com
+65 6381 6818

Rizwi is a founding member of RHTLaw Asia, and is the Acting Head of the firm's Intellectual Property and Technology Practice. He also heads the Firm's Consumer Brands Industry Group, with specific focus on Food & Beverage, Fashion & Luxury, and the Video and Computer Games industries.

About RHTLaw Asia

RHTLaw Asia offers a different perspective on client experience and commercial thinking. As a leading regional law firm headquartered in Singapore, clients can expect intelligent and innovative solutions from a team that is attuned to the nuances of doing business in Asia.

With access to our own ASEAN Plus Group, a network of leading firms comprising over 2,000 lawyers in 16 jurisdictions across Asia and beyond, as well as our membership with The Interlex Group, a global network of leading law firms and HLB a global advisory and accounting network, we help clients understand the local challenges, navigate the regional complexity to deliver the competitive advantage for their businesses in Asia.

In delivering innovative legal and commercial solutions, it collaborates with ONERHT through entities which are not affiliates, branches or subsidiaries of RHTLaw Asia LLP.