MAYER | BROWN

Global Privacy Developments

Europe, Asia and the Americas

Karen H. F. Lee
Counsel - Singapore
+65 6327 0638
karen.hf.lee@mayerbrown.com

Lei Shen
Partner - Chicago
+1 312 701 8852
lshen@mayerbrown.com

Oliver Yaros
Partner - London
+44 20 3130 3698
oyaros@mayerbrown.com

Cristiane Manzueto
Counsel - Rio de Janeiro
+55 21 2127 4235
cmanzueto@mayerbrown.com

Dr. Ulrich Worm
Partner - Frankfurt
+49 69 7941 2981
uworm@mayerbrown.com

Schrems II and Brexit

Dr. Ulrich Worm
Partner - Frankfurt
+49 69 7941 2981
uworm@mayerbrown.com

Oliver Yaros
Partner - London
+44 20 3130 3698
oyaros@mayerbrown.com

MAYER | BROWN

Implications of the so called *Schrems II* decision of the Court of Justice of the European Union ("CJEU") (case no. C-311/18)

- The Schrems II decision concerns data transfers from the European Union (EU) or the European Economic Area (EEA) to third countries.
- Specifically, the decision concerns data transfers from the EU/EEA to the USA on the basis of the EU-US Privacy Shield or Standard Contractual Clauses.
- Data transfers from Europe to a third country are only admissible if they can be based on a safeguard listed in Art. 46 GDPR.
- If none of the safeguards in Art. 46 GDPR is available, transfers may, by way of exception, be based under strict conditions called "derogations for specific situations" (Art. 49 GDPR).
- However, these derogations only serve as exceptions to the rule that transfers must be based on one of the safeguards under Art. 46 GDPR.

Implications of the so called *Schrems II* decision of the Court of Justice of the European Union ("CJEU") (case no. C-311/18)

- In the Schrems II case, the CJEU was asked to ascertain whether the EU-US Privacy Shield is a valid basis for data transfers from the EEA to the USA.
  - The CJEU decided that the EU-US Privacy Shield does not establish an adequate level of protection in the USA, and can thus no longer be used to transfer personal data from the EEA to the USA.
  - This follows the previous Schrems I decision of the CJEU (C 362/14) where it held that the predecessor to the EU-US Privacy Shield, the so called Safe Harbour, also did not establish an adequate level of protection in the USA.
- The CJEU further held that Standard Contractual Clause continue to be an instrument under which transfers of data from the EEA to a third country can be justified.
  - However, parties wishing to rely on Standard Contractual Clauses must verify whether the level of protection in the third country is adequate.
  - CJEU pointed out that appropriate supplementary measures in addition to Standard Contractual Clauses could be implemented in order to protect the data, but only if such measures ensure that foreign domestic law in the relevant third country does not impinge on the adequate level of protection.

Implications of the so called *Schrems II* decision of the Court of Justice of the European Union ("CJEU") (case no. C-311/18)

- Because the CJEU held that no adequate level of protection exists in the USA, the EU-US Privacy Shield can no longer serve as a legal basis for the transfer of personal data from the EEA to the USA. Whether, and under which conditions, Standard Contractual Clauses could still serve as a legal basis remains questionable for the time being.
- What does this mean for companies which have relied on the EU-US Privacy Shield or the Standard Contractual Clauses?
  - Transfers to the USA (and other countries which do not offer an adequate level of protection) need to be suspended immediately, unless and until the transfers could be based on another legal basis; no grace period applies.

Implications of the so called *Schrems II* decision of the Court of Justice of the European Union ("CJEU") (case no. C-311/18)

- Conduct due diligence assessment of the laws in the jurisdiction of the data importer.
- In the case of Standard Contractual Clauses, evaluate whether the implementation of supplementary measures to protect the data would allow to continue to transfer data.
- Closely follow further developments, in particular the announced guidance from the European Data Protection Board on such supplementary measures and transfers post *Schrems II*.
- Evaluate whether the data transfer could be based on another legal basis or derogation.
- Consider switching to service providers, or invest in data processing infrastructure and personnel, in the EEA or a third country that is regarded as being "safe" based on an adequacy decision of the European Commission.

End of the EU / Brexit Transition Period (31 December 2020)

- GDPR to be incorporated directly into UK law and sit alongside the Data Protection Act 2018 ("DPA"). New data protection exit regulations have been passed - these make technical amendments to the GDPR allowing it to work in a UK-only context.
- European Commission aiming for an adequacy decision on the UK by 31 December 2020. If the UK does not receive an adequacy decision in its favour EU-UK transfers will need to rely on SCCs, BCRs, codes of conduct and certification or Article 49 GDPR derogations.
- UK government has stated that transfers of data from the UK to the EEA will be permitted after the Brexit Transition Period has ended (to be kept under review).
- Schrems II & UK:
  - If there is not an adequacy decision by the European Commission in favour of the UK, then EU-UK transfers may face similar concerns.
  - UK Investigatory Powers Act, UK-US Bilateral Data Sharing Agreement and further data privacy law divergence post Brexit could create problems

Guidance from the European Data Protection Board on the concepts of controller and processor ("**Guidelines**")

- The Guidelines have been adopted on 2 September 2020, and have been open to public consultation until 19 October 2020.
- Following the consultation period and review of contributions received, the Guidelines will be formally adopted by the EDPB.
- They consist of two main parts, one explaining the different concepts of controllers, processors and joint controllers, the other including detailed guidance on the consequences of these concepts for controllers, processors and joint controllers.
  - A controller is a party which determines the purposes and means of processing, i.e. the why and how of the processing.
  - A processor acts (only) "on behalf of" a controller, i.e. within the boundaries determined by the controller.
  - Joint controllers determine the purposes and means of processing jointly.

Guidance from the European Data Protection Board on the concepts of controller and processor ("**Guidelines**")

- The Guidelines distinguish between the determination of
  - essential means of processing, which is reserved to controllers; and
  - non-essential means, concerning practical aspects of implementation, which can be left for the processor to determine.
- Not every service provider that processes personal data is a "processor". Rather, the role of a processor stems from the concrete activities in the specific context. The Guidelines point out that a service provider which determines the purposes and means of (parts of) processing is a separate controller (or a joint controller), rather than a processor.
- An entity can simultaneously act as a controller for certain processing activities, and as a processor for others.

LGPD in Brazil

Highlights and Key Aspects

Cristiane Manzueto

Counsel - Rio de Janeiro *(Head of Data Privacy and Intellectual Property Practices in Brazil)*
+55 21 2127 4235
cmanzueto@mayerbrown.com

MAYER | BROWN

LGPD: Scope and Applicability

- LGPD is already in full force as of September 18, 2020.
- LGPD is applicable to any processing performed by natural persons or entities, regardless of the means, country or headquarters where the data are located, provided that:
  - the processing operations occur in Brazil;
  - the processing activity is related to the offering or provision of goods and services for individuals located inside Brazil;
  - the processing activity is related to individuals located inside Brazil; or
  - the personal data was collected when the data subject was inside the Brazilian territory.
- Therefore, companies located outside of Brazil — in Europe or in the US, for instance — must comply with the LGPD.

LGPD: Scope and Applicability

- LGDP may be enforced by data subjects, the Brazilian Data Protection Authority (which is still being structured), public prosecutors, consumers' defense organizations and other authorities.
- Penalties of the LGPD (issued exclusively by the Brazilian Data Protection Authority) include:
  - Fine of up to 2% of revenues in Brazil in the prior financial year, up to a total maximum of BRL 50 million per violation;
  - Suspension of the data processing activity related to the infringement for the period of 6 months, extendable for another 6 months; and
  - Partial or complete prohibition of activities related to personal data.
- Law No. 14,010, of 2020, postponed the administrative sanctions above to August 01, 2021.
- Penalties established in Code of Consumers Defense and Internet Civil Framework are also applicable to protection of personal data.

Key Points of the LGPD

- Assuring the lawfulness of processing
  - 10 different legal bases, 08 for sensitive data
- International transfer of personal data
  - 15 different allowance hypotheses
- Informing data subjects in a clear, adequate and ostensive manner
  - 7 minimum standards
- Integrity, security and confidentiality of data
  - Risk assessment + state-of-the-art technology
- Documentation (accountability principle): Records of Processing Activities, Contracts with joint controllers and processors; and Data Protection Impact Assessment.

Key Points of the LGPD

- Main Legal Basis
  - Consent (freely given, unambiguous and informed)
  - Legitimate Interest
  - Comply with a legal or regulatory obligation
  - Necessary for the performance of a contract with the data subject
  - Protection of credit
  - Exercise rights in lawsuits, administrative or arbitral proceedings
  - Prevent frauds or for the safety of the data subject by means of an electronic authentication system (biometric – sensitive data)

Key Points of the LGPD

- Data subject rights, e.g.:
  - ✓ Confirmation of the existence of processing;
  - ✓ Access to the data;
  - ✓ Rectifying outdated or incorrect data;
  - ✓ Anonymization, blockage or elimination of unnecessary, excessive data or processing in violation of the LGPD;
  - ✓ Information of the private and public entities with whom the controller shared data;
  - ✓ Portability.
- Designating a data protection officer ("DPO"), whether a natural person or legal entity.
  - ➢ All controllers are obliged to designate a DPO so far.

Key Points of the LGPD

- Security Incidents (loss, unauthorized access or use, breach, etc.):

  - ✓ Communication to Data Protection Authority and data subjects unless the incident is unlikely to result in a risk or a relevant damage to the data subject.

  - ✓ Communication within a **reasonable term**, to be established by the Data Protection Authority

CCPA and CPRA in the US

Lei Shen

Partner - Chicago
+1 312 701 8852
lshen@mayerbrown.com

MAYER | BROWN

Overview of California Consumer Privacy Act

- **Became effective January 1, 2020, and became enforceable on July 1, 2020**
- Considered to be the **most sweeping privacy law in the U.S.**
- **Applies to for-profit companies doing business in California** that meet certain criteria
- Provides consumers with certain rights to their personal information

Obligations Under CCPA

- **Notice Requirements**
  - Notice at or before the point of collection (also applies to employees)
  - Privacy policy
- **Consumer Rights**
  - Right to Know
  - Right to Opt-Out of Sale of Personal Information
  - Right to Delete
  - Right to Non-Discrimination for Exercising Rights
- **Liability**
  - Fines
  - Private Right of Action

CCPA Regulations

- California Attorney General drafted implementing Regulations for CCPA
  - Provides various supplemental requirements, including for notices, privacy policies, and responding to consumer requests
- California Office of Administrative Law (OAL) approved AG's draft of implementing Regulations on August 14, 2020, with immediate effect
  - OAL made some changes to AG's "final" Regulations
- AG proposed additional changes to OAL's "final" Regulations on October 12, 2020
  - Changes focus on opt-out of sale requirements, authorized agent requirements, and clarifications regarding notices to consumers under 16 years of age

CCPA Enforcement Actions

- **Enforcement of CCPA began July 1, 2020**
- **OAG Enforcement Actions:**
  - Initial letters sent to allegedly noncompliant businesses
    - Businesses identified based in part on consumer complaints using social media
    - Focused on missing privacy disclosures or "Do Not Sell" requirements

CPRA

- **CPRA is new ballot initiative in California that would amend the CCPA**
  - Will be on California's November 2020 ballot
- **Adds new consumer rights and protections**
  - Creates new category of "sensitive personal information"
  - Right to limit use and disclosure of sensitive personal information
  - Right to correct inaccurate personal information
  - Use limitation
  - Data minimization
  - Extends employee and B2B data exemptions
  - New enforcement agency

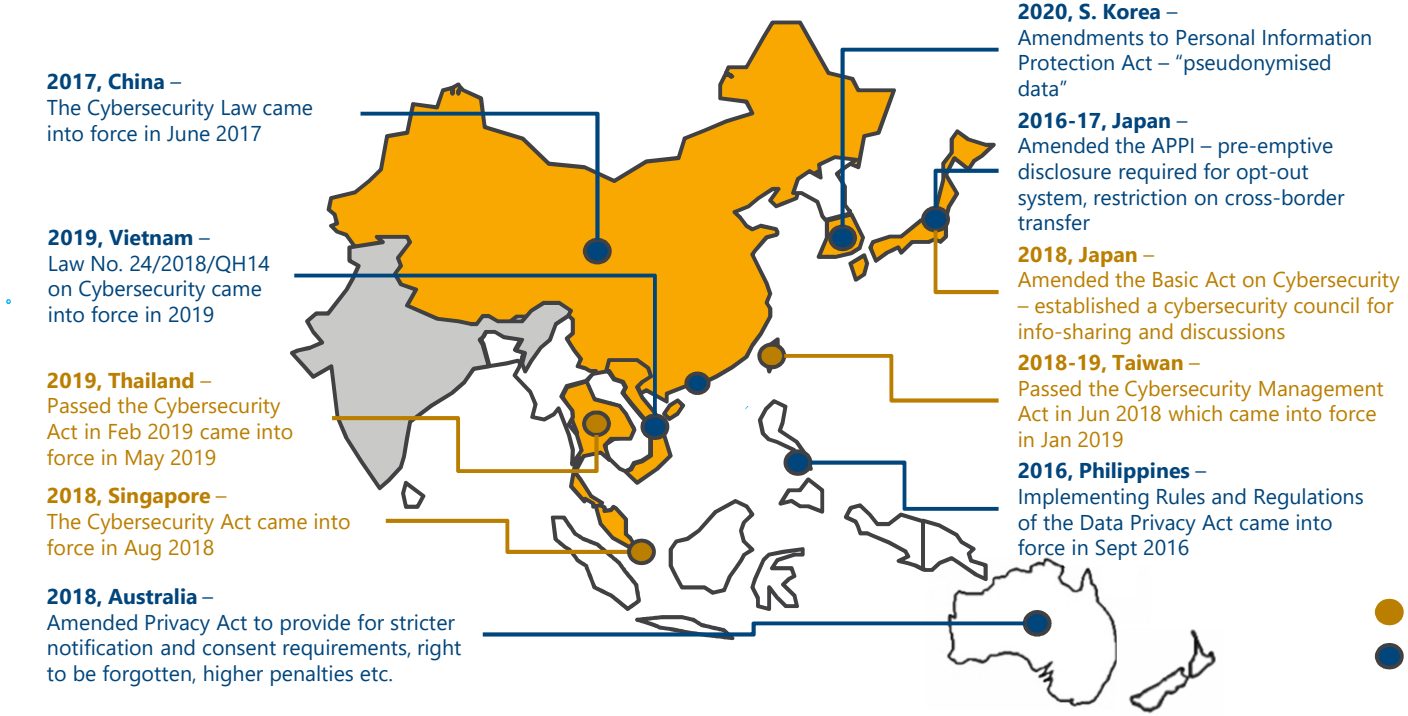
Overview of Data Privacy Regulations in Asia

Karen H. F. Lee

Counsel - Singapore
+65 6327 0638
karen.hf.lee@mayerbrown.com

MAYER | BROWN

Evolution of Regulatory Landscape in APAC



2017, China –
The Cybersecurity Law came into force in June 2017

2019, Vietnam –
Law No. 24/2018/QH14 on Cybersecurity came into force in 2019

2019, Thailand –
Passed the Cybersecurity Act in Feb 2019 came into force in May 2019

2018, Singapore –
The Cybersecurity Act came into force in Aug 2018

2018, Australia –
Amended Privacy Act to provide for stricter notification and consent requirements, right to be forgotten, higher penalties etc.

2020, S. Korea –
Amendments to Personal Information Protection Act – "pseudonymised data"

2016-17, Japan –
Amended the APPI – pre-emptive disclosure required for opt-out system, restriction on cross-border transfer

2018, Japan –
Amended the Basic Act on Cybersecurity – established a cybersecurity council for info-sharing and discussions

2018-19, Taiwan –
Passed the Cybersecurity Management Act in Jun 2018 which came into force in Jan 2019

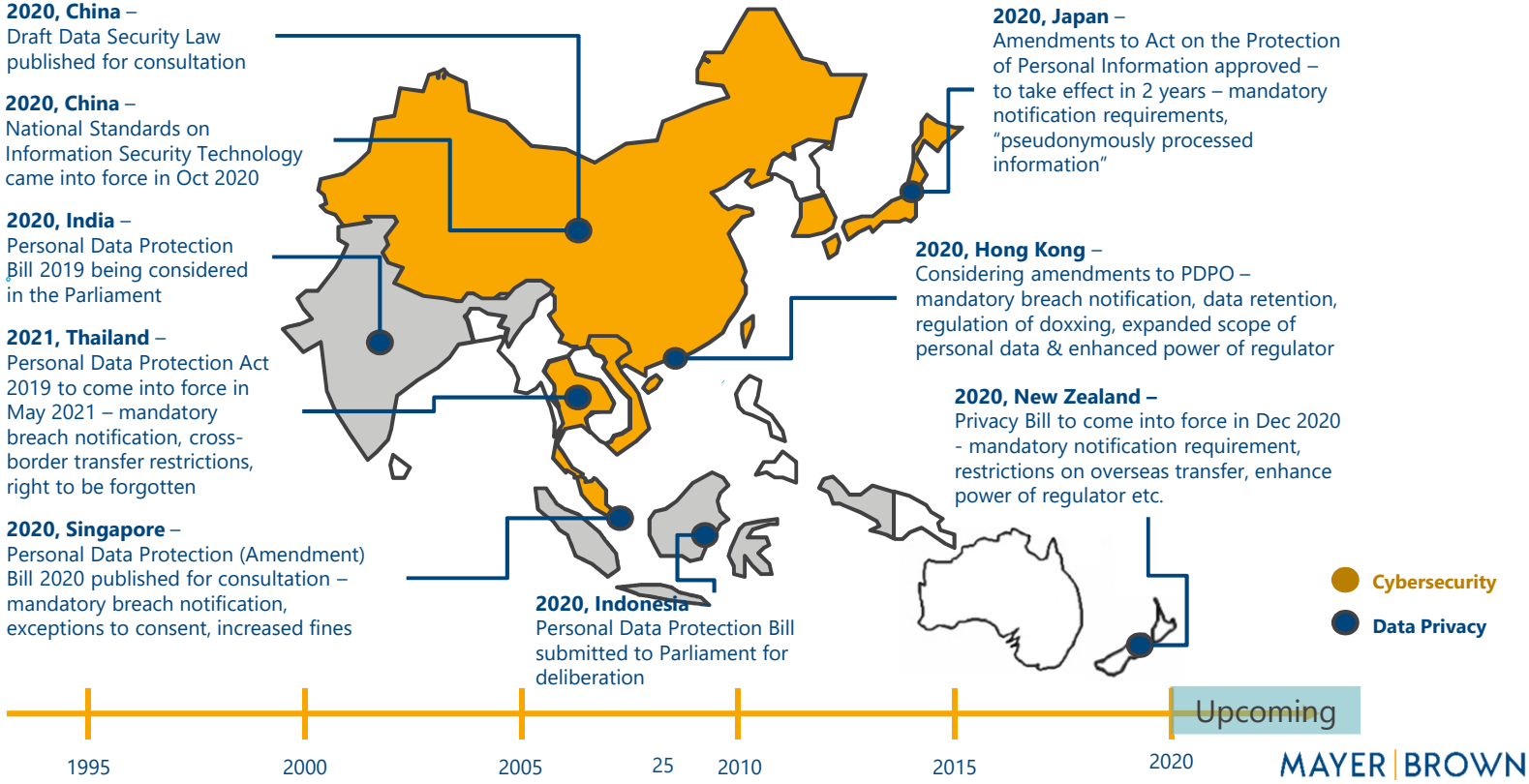
2016, Philippines –
Implementing Rules and Regulations of the Data Privacy Act came into force in Sept 2016

Cybersecurity
Data Privacy

1995 2000 2005 2010 2015 2020
2015-2020

MAYER | BROWN

Evolution of Regulatory Landscape in APAC



MAYER | BROWN

Issues Relating to Data Privacy in Asia

- A patchwork of laws
- Different requirements around consent/notification and direct marketing
- Mandatory vs voluntary breach notification
- Cross-border data transfers
- Data processors
- Data retention
- Definition of data (sensitive data; biometric data)
- Data privacy regulators

Trends in Data Privacy in Asia

- Overall greater alignment in standards across Asia - gradual shift towards a GDPR-esque standard
- Mandatory data breach notification requirement
- Increasing penalties for breach (revenue-based penalties)
- Greater emphasis on accountability-based frameworks
- More countries adopting APEC CBPR and seeking (or planning to seek) EU adequacy decisions
- Privacy by design and PIAs

China

- No over-arching data privacy law
- Cybersecurity Law ("**CSL**") – June 2017
  - Applies to network operators and CII operators
  - Data localization restrictions
    - CII operators must store in PRC, personal information and important data generated or collected during operations within PRC
  - Cross-border transfer restrictions
    - Cannot transfer or provide access to personal information or important data offshore, unless e.g. conduct official security assessment, consent, etc.
- Multi-level protection scheme – security requirements depending on level of risk
- PI Specification (amendments came into effect October 2020)
  - "Best practices" standards for personal information security

China

Draft Data Security Law (3 July 2020)

- Important definitions
  - Data: any electronic or non-electronic records of information
  - Data activities: include data collection, storage, processing, usage, provision, transaction and publication
  - Data security: the ability to ensure that data receives effective protection, will be used legitimately and remains in secure condition through the adoption of necessary measures
- Tightens regulations for accessing and sharing data
- Creates new management responsibilities for data entities
- Extraterritorial effect – applies to any overseas individuals and companies whose activities damage China's national security, public interest or legitimate interests of citizens

China

Draft Data Security Law (3 July 2020)

- Protection of important data
  - Multi-level data protection: different security requirements apply to data falling into different levels based on (i) importance to social and economic development and (ii) harm to national security
  - Local governments and industry regulators to draft catalogue of important data
  - Processors of important data to conduct risk assessment; appoint data security officer and designate management department
- Data activities affecting national security – subject to national security review
- Export control, countermeasures against unfair treatment
- No provision of data stored in China to foreign law enforcement authorities, without prior approval of Chinese authorities
- Centralised data security mechanism for assessing and reporting data security risks, sharing relevant information, and providing early-warnings

Hong Kong – Personal Data (Privacy) Ordinance

Background

- One of the oldest regimes in APAC
- Amended once (2012) and due for another amendment in 2021

Features

- Underpinned by 6 data protection principles
- Cross-border data transfers allowed
- No mandatory breach notification

Proposed amendments

- Mandatory breach notification
- Data retention policies
- Direct regulation of data processors
- Expanding definition of “personal data”
- Regulation of doxxing
- Increased penalties

Hong Kong – National Security Law

- Came into effect 30 June 2020
- New offences of secession, subversion, terrorism and collusion with foreign or external forces
  - Offence to aid, abet or assist in commission of such offences, including provision of financial assistance or funds
- Broad powers of law enforcement agencies
  - Require anyone suspected of having info or material relevant to investigation, to provide it or answer questions
  - Search relevant premises and electronic devices that may contain evidence of offence
  - Interception and surveillance (approved by Chief Executive) on person suspected of being involved in committing offence endangering national security
  - Require service providers or individuals to remove info (e.g. takedown posts on social media) and provide assistance

Take Away Points

- Increased awareness of privacy rights
- Increased adoption of overarching data privacy laws – trend towards more regulation
- Increased enforcement through constant updating of laws and regulations (Hong Kong, Australia, South Korea, Singapore, Japan, New Zealand, China, etc.)
- Increased focus on cross-border data transfers
- Those with no overarching legislation will likely have one in years to come
- Regulators leaning towards "privacy by design" and requests for PIAs


Thank you!
MAYER | BROWN

Americas | Asia | Europe | Middle East

mayerbrown.com