Data Protection and Privacy - Trends and developments

Charmian Aw, Counsel, caw@reedsmith.com

FIP, CIPP/A, CIPP/US, CIPP/EU

ReedSmith

Driving progress
through partnership

An overview of Asia

- Asia is very diverse
- Rapidly developing data protection landscape

An overview of Asia

Data Protection Regimes in APAC

Overarching Data Protection Legislation

Singapore
Personal Data Protection Act 2012

Malaysia
Personal Data Protection Act 2010

Philippines
Data Privacy Act 2012

Hong Kong
Personal Data (Privacy) Ordinance

South Korea
Personal Information Protection Act

New Zealand
Privacy Act 1993

Australia
Privacy Act 1988

Thailand
Personal Data Protection Bill

No overarching Data Protection Legislation

Cambodia

Myanmar

Lao PDR

Vietnam

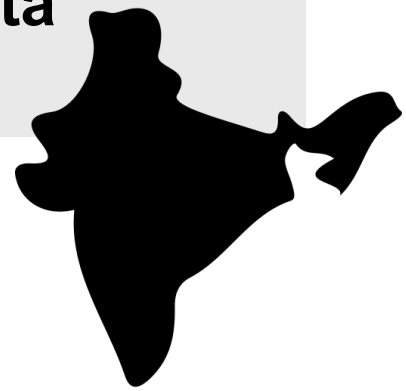
Indonesia

Brunei

India

People's Republic of China

Proposed changes to India’s personal data protection legislation



India

India does not have a dedicated data protection law.

Certain provisions on data protection are found under the Information Technology Act 2000:

- Provides for safeguards against certain breaches in relation to data from computer systems and contains provisions to prevent the unauthorised use of computers, computer systems and data stored in them
- The rules framed permits cross border transfer of data subject to recipient complying with the same level of security standards as prescribed under the rules. The said rules are not mandatory and the parties can by contract choose to exclude the applicability of such rules.

The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 further covers basic requirements which corporate entities must comply with when collecting, processing and storing personal data.

India

Article 21 Constitution:

No person shall be deprived of his life or personal liberty except according to procedure established by law.

Puttaswamy v Union of India (August 2017) held that information privacy was part of fundamental right to life and liberty in Indian Constitution.

Unni Krishnan v State of Andhra Pradesh (1993): The Supreme Court of India recognised the right to privacy under Article 21 of the Constitution as part of the right to life and personal liberty, subject to overriding interests.

India

- In addition, provisions on data protection are found under several sectoral laws:

Company Law

There is a data mirroring requirement for data relating to books of accounts and books and paper of a company that is stored outside India.

Payments

There are data localization requirements on entire data relating to payment systems including full end to end transaction details / information collection / carried / processed as part of the message / payment instruction.

Telecom Law

There are data localization requirements on user information / accounting information relating to a telecom user (except for international roaming / billing information). Even remote access to such data from outside India is not permitted.

Insurance Law

There are data localization requirements on details of insurance policies issued by a company and details related to insurance claims.

India

- Provisions on data protection found under several sectoral laws:

Banking

Credit Information Companies Regulation Act 2005: credit information pertaining to individuals must be collected as per privacy norms. Principles relating to the collection, processing, protection, manner of access to and sharing of data must be adopted by credit information companies and credit institutions (including banks).

Healthcare

Professional Code of Ethics of Doctors requires doctors to keep patient information confidential with disclosure only allowed where a serious risk to the person or community is identified

Banking and Payments Law

– Outsourcing by banks – outsourcing of certain banking functions (which result in data being processed, stored or accessed overseas) is permitted subject to fulfillment of certain conditions, such as, (a) the offshore regulator does not obstruct the arrangement or prevent inspections by the Reserve Bank of India ("RBI") or auditors; (b) the availability of records to the management and RBI is not affected by the liquidation of the offshore provider or the bank in India; (c) the offshore regulator does not have access to the data simply because the data is being processed overseas; (d) the jurisdiction of the courts in the offshore location does not extend to the operations of the bank in India. .

India

Draft Personal Data Protection Bill, 2018… ➔

- Likely to be introduced in parliament in June, after the general elections
- Srikrishna Committee was responsible for drafting the bill.
- Proposed a “Fourth Way” of regulating data protection, in addition to the EU, US and China.
- Data subjects/individuals ➔ Data principals.
- Data controllers/organisations ➔ Data fiduciaries (introduces concept of trust).

India

Draft Personal Data Protection Bill, 2018… ➔

- Data protection authority for India, DPAI, will be established under the draft bill.
- Tasked with identifying timelines for response to data principals rights requests, data breach notifications, and enforcing application of provisions of the draft bill.
- For non-compliance, can award fines of:
  - for data fiduciaries: up to 2% of a company's total worldwide turnover or INR 50 million, whichever is higher, and
  - for significant data fiduciaries: up to 4% of total worldwide turnover or INR 150 million, whichever is higher.
- Organizations will be granted a transition period of 12 months after the bill is enacted to ensure compliance.

India

Data principals' rights ⋯⋯⋯⋯⋯⋯⋯⋯➔

Access

Data portability

Correction

Right to be forgotten

Annual data audit required, to be carried out by independent data auditors.

India

Data fiduciary's obligations:

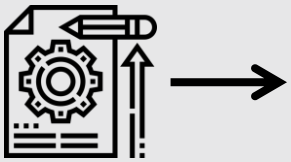
- periodic data audits
- maintaining records of data processing
- performing data protection impact assessments.

Applicable to:

- data fiduciaries established in India:
- data fiduciaries with the systematic activity of offering goods and services to data principals in India; or
- data fiduciaries performing any activity that involves profiling of data principals within the territory of India.

India

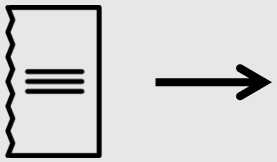
Data fiduciary ⇢



- “Significant data fiduciaries”: high-risk processing activities.
- Required to appoint a data protection officer.
- Also, organizations not present in India but under the scope of the bill are required to appoint a DPO who is based in India.
- But no requirement prescribed under the bill that DPO must be independent.

India

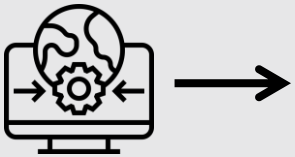
Legal grounds for processing ⇢



- Broadly similar to the GDPR (e.g. consent)
- But narrower than GDPR in some respects e.g. draft bill does not allow processing on basis that it's necessary to perform a contract; DPAI allowed to regulate use of the "reasonable purposes" (akin to legitimate interests) ground for processing (so unclear how this may be relied on in practice).

India

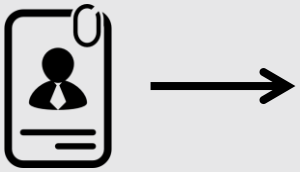
Data localisation



- Data fiduciaries are required to store at least one copy of personal data on servers or data centers located in India.
- Central government has to identify critical personal data, which shall only be processed in a server or data center that is located in India.

India

Personal data breach notification



- Data fiduciaries are required to notify as soon as possible the DPAI.
- If personal data breach is “likely to cause harm to any data principal”
- The DPAI will then determine whether affected data principals need to be notified aswell.
- The DPAI will issue additional guidance e.g. notification thresholds and timeframes.

How these changes may impact on privacy compliance for the rest of Asia?

Potential impact going forward

Many Asian economies including India are focussing heavily on technology and the digital economy. Data is the fuel, so data privacy legislation has increased in importance.

Looking to the EU and GDPR

Data localisation in Asia

India is a large market in Asia, together with China.

May spur larger developing economies in Southeast Asia to implement comprehensive data privacy legislation.

There may be future cooperation with other DPAs on data breach investigations and enforcement.

Key takeaways

Ensure policies and practices comply with Asia data privacy laws, on top of GDPR where applicable.

Data minimisation

Data protection impact assessment.

Privacy by design