Asian Data Privacy Laws
New & Updated Laws & Bills (2022)
Part 2: ASEAN & S.Asia

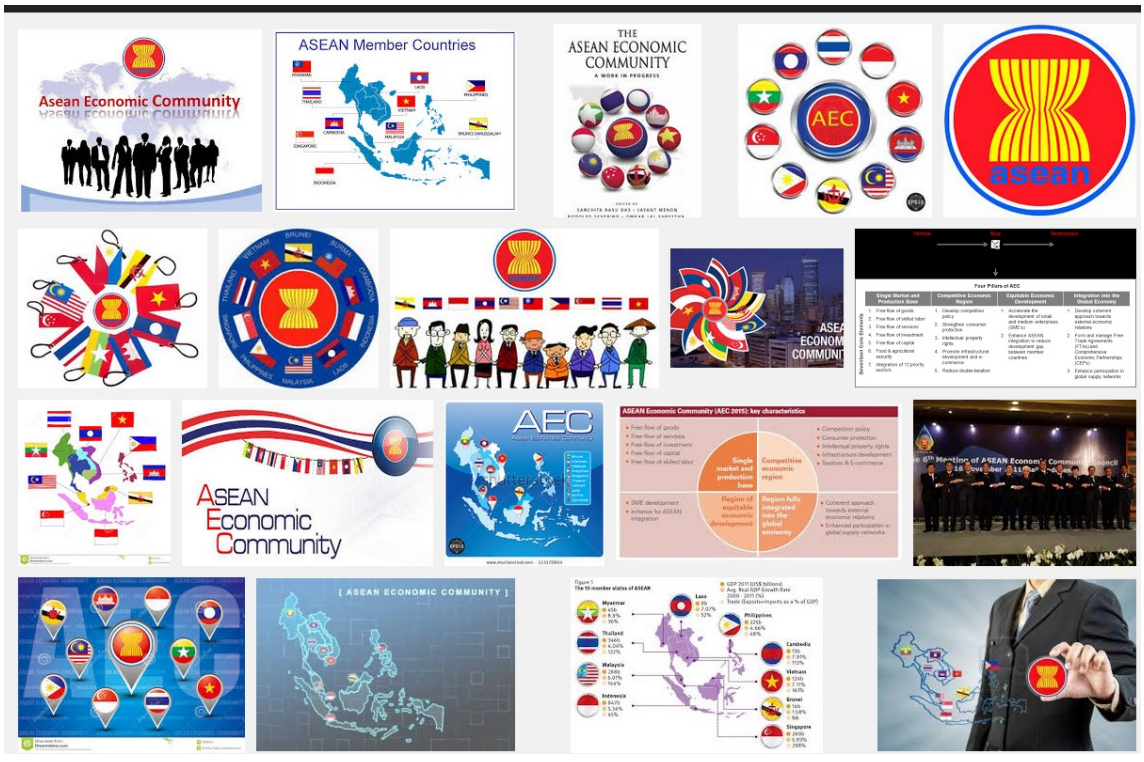
Professor Graham Greenleaf AM

Professor of Law & Information Systems,
University of New South Wales

Asia-Pacific Editor, *Privacy Laws & Business International Report*

UNSW EDGE, 3 March 2022, Law Faculty, UNSW City Campus

1



Many faces of ASEAN (Association of South-East Asian Nations)

2

ASEAN – a growth area again

3

ASEAN & privacy commitments

- *Context:* ASEAN could have become a major driver of privacy laws BUT
  - majority of 10 members are **undemocratic** or quasi-democratic;
  - Most privacy laws did not cover the **public sector** (except Philippines); now, Thailand does, and Bills for Indonesia & Vietnam propose to
- APEC: 7 of 10 members, also in APEC (not Cambodia, Laos, Myanmar);
  - APEC-CBPRs is not significant (only Singapore fully; Vietnam & Philippines notional)
- ASEAN *Human Rights Declaration* (Dec 2012)
  - First human rights instrument many ASEAN countries have entered; **toothless**
  - A21: 'Every person has the right to be free from arbitrary interference with his or her privacy, family, home or correspondence including personal data' (similar to ICCPR)
- ASEAN Economic Community (AEC) established (2015)
  - E-commerce framework includes data protection (**no commitment to legislate**)
- ASEAN *Framework on Personal Data Protection* (2016) is similar to APEC Framework + a deletion-like principle; **no enforcement obligations**
- ASEAN *Data Protection and Privacy Forum* (2019) – first met Aug. 2019
- ASEAN Data Management Framework & Model Contractual clauses (2021)
  - Singaporean initiative; useful tools but no legal significance [recent article on request]

Result: **No regional data protection agreements of legal significance as yet.**

4

Free Trade Agreements & ASEAN

See Materials – final article on 'Trade agreements'

- *CPTPP* - Comprehensive and Progressive Agreement for Trans-Pacific Partnership ('APEC FTA')
  - In force; 2/7 *ratifications* from ASEAN (Sing; Vietnam)
  - Strong limits on data export restrictions & localisation, arguably stronger than GATS (General Agreement on Trade in Services, 1995) Art. 14(c)(ii)
- *RCEP* – Regional Comprehensive Economic Partnership
  - Signed but not in force; all 10 ASEAN members are signatories, plus 6 countries with FTAs with ASEAN, including China and (potentially) India
    - Potentially much larger than CPTPP
  - 'necessity' for export limits or localisation is left entirely to State concerned; therefore very weak limitations

5

ASEAN overview: Renewed progress

- **Philippines**: Act (with DPA) 2012, finally in force in 2016
- **Malaysia:** Act (with DPA) 2010, in force 2013 – no enforcement
  - Dept has prepared Bill for major changes
- **Singapore**: Act (with DPA) 2012, in force 2014 – with enforcement
  - Amending Act passed 2020.
- **Indonesia**: new Regulations 2013 and 2016 under IT law;
  - New GDPR-influenced Bill introduced to Parliament – timing unknown.
- **Thailand**: new GDPR-influenced Act 2019 – most important change
- **Vietnam**: e-commerce & consumer laws, in force
  - Cybersecurity (data localisation) law 2018
  - Comprehensive draft Decree introduced 2021 – not yet enacted
- **Brunei** – draft Bill based closely on Singapore's law (private sector only)
- **Other countries:** No draft Bills in other 3 members (Cambodia, Laos, Myanmar)

Result?: *Progress rapid 2012-13; had slowed but increasing again in 2019-21*

- *Soon, perhaps only Singapore and Brunei will not cover the public sector*
- *Transparency: Reporting of cases in Singapore and Philippines is very valuable*

6

Thailand

[2019 Update; Materials: 'Thailand – Asia's strong new DP law' (2019)

- *Context:* Unstable alternation between military regimes and democracy since WWII; Military and Bangkok elite coup 2014; military junta held elections mid-2019; large-scale protests 2020-21
- APEC and ASEAN member, not OECD; CPTPP and RCEP signatory
- Pre-2019 protections negligible
  - Constitutional protection since 2007 of 'a person's family rights, dignity, reputation, and the right of privacy' - ineffective
  - Official Information Act, 1997 – Only covers State; administered by Official Information Commission (OIC); *Unenforceable* privacy principles. Sidelined
  - Succession of failed data privacy bills 2005 – 2014.
- 2019 Bill enacted by Junta weeks before election of Junta/Party
  - First strongly GDPR-influenced law in Asia; only one in ASEAN as yet
  - in-force date delayed to 01/06/2021; **now delayed again to 01/06/22; 3 year delay partly due to disputes over appointment of DPA membership**

Thailand – PDPA 2019

- Scope – Largely comprehensive; potential exemptions
  - Private sector covered (but credit industry exempt);
  - exemptions by Royal decree have no constraints except 'public interest;
  - Normal exemptions: personal uses; media and artistic; 'public interest'
  - Public sector covered – PDPA replaces old OIA – investigations etc exempt
  - Extra-territorial application similar to GDPR
- Principles (explicitly aims at high GDPR compatibility)
  - No 'legitimate grounds for processing' (contra GDPR): emphasis on consent
  - Principles have strong GDPR elements (more so than in Bill): data minimization; strong consent; portability; objections to processing; deletion (incl. RTBF); sensitive data restrictions; DPOs; data breach notification (DBN)
  - Some GDPR elements omitted: 'by design and default'; automated processing; DPIAs; 'demonstrable accountability'.
-

Thailand – PDPA 2019 (2)

- Data exports to countries with 'adequate level of protection'
  - But DPA is to define what 'adequate' means (EU is very strict after Schrems II)
  - Other grounds for exports: consent; other suitable protections (DPA to define)
  - No data localisation provisions (nor in Cyber Security Act 2019)
- Personal Data Protection Committee (PDPC) etc
  - 16 members: Chair + 6 government ex-officio + 9 'honorary' with qualifications
  - 2021: 200 applicants; 10 proposed but protests (lack of qualifications) – reviewed
  - Jan 2022: Govt appointed all members; will now start to make Regs etc.
  - Not independent; byzantine structure (problems with EU)
- Enforcement – civil, criminal and administrative
  - 'Expert Committees' of PDPC *arbitrate* complaints; can issue compliance notices
  - They can issue administrative fines (max US $160K), and enforce via Admin Ct
  - Right to obtain compensation from a court for breaches (not from PDPC)
  - Criminal offences to breach some sections of PDPA
  - Overall, a diverse enforcement toolkit, although max. penalties are light

Thailand – PDPA 2019 (3)

Conclusions

- Potentially stronger than most existing ASEAN/Asian laws
  - will depend a great deal on PDPC's enforcement and delegated rules.
  - 29 draft regulations awaiting approval by newly-appointed PDPC
- EU adequacy will require negotiations & amendments
  - Positive: Has more GDPR elements than Japan's 'adequate' law
  - Dangers: (i) PDPC lack of independence; (ii) data export rules not finalised; (iii) Public sector access exceptions? (*Schrems* dangers)
- In force mid-2022; evidence of adequacy will take longer

Indonesia

[Materials: 'Indonesia's DP Bill lacks a DPA, despite GDPR similarities' April 2020]

- *Context:* Since 1999 and the end of the Suharto era, a successful democracy with improving rule of law. The largest Muslim majority country.
- APEC, ASEAN member; has not signed CPTPP; has signed RCEP
- Implied Constitutional protection (A 28G(1)) has resulted in surveillance requiring legal regulation

•**Complex mix of existing laws**, of little effect because there is no DPA

1. *Public Information Disclosure Law 2010* – right of access (but not correction) to government files
2. *Information and Electronic Transactions Law 2008*
   - Highest form of Indonesian legislation
   - A26 requires consent for use of any person's personal data 'by use of electronic media' – a 'broad brush' right; might apply to all sectors
   - 'Elucidation' implies rights of access and correction
   - A26(2) Courts can award compensation for breaches (No cases yet)

Indonesia – 2012 & 2016 Regulations

3. 2012 Regulation on Operation of Electronic Systems and Transactions A15
   - 2nd highest form of Indonesian legislation; Scope is uncertain:
   - Does 'Electronic Service Organisations' (ESO) apply to both private and public sectors?
   - Definition of 'personal data' is broad; unsure if excludes publicly available data
4. 2016 Ministerial Regulation on Personal Data Protection in Electronic Systems

- Together, 2008 Act + both Regulations go well beyond OECD basic privacy principles:
  1. 'Secrecy, integrity and availability' (2012)
  2. Collection and use based on consent, or legal authority (2012)
  3. Disclosure based on consent, in accordance with purpose of acquisition disclosed at time of acquisition (2012))
  4. Data breach notification requirement (2012): Must notify data subject; + regulatory agency if effects serious (2012)
  5. Security requirements (many provisions); certification of systems required (2016)
  6. Access and correction (2008 Law)
  7. **Right to be forgotten** (2016 amendment to 2008 Law)
  8. Data exports require Ministerial approval; some **data localisation** requirements (2016)
  9. Ministry-based complaints system for data breaches only (2016)

Indonesia – Enforcement of current laws

- Breaches of A15 of 2008 law can result in administrative sanctions (fines) & service suspensions
- A26 of 2008 law provided right to sue for compensation (also perhaps under Civil Code)
- No criminal penalties for A 15 etc breaches
- 2016 Reg complaint system only applied to data breaches
- Data localisation: ESOs must locate 'data centre and disaster recovery centre' on Indonesian territory (A 17)
  - See 2019 Update for details of other current requirements
- 'Reliability Certification Agencies' (A 68) could become relevant to APEC-CBPR

Result: No enforcement known

*Significant principles but **ineffective due to absence of a DPA***

Indonesia – *Protection of Personal Data draft law 2020*

- PPD draft law submitted by President to House of Reps In January 2020
- Comprehensive scope
  - private and public sectors
  - Novel extraterritoriality: (i) processing with legal consequences in Indonesia; (ii) Indonesian processors located outside Indonesia.
- Principles– strongly GDPR-influenced selection of medium strength
  - 'Grounds for legitimate processing': consent or 6 non-consensual grounds (similar to GDPR, but less balancing of individual interests)
  - GDPR-influenced principles: withdrawing consent; data portability; automated processing rights; data breach notification; broad sensitive data categories; can request various processing limitations (enacts RTBF); 'demonstrable accountability' obligations
  - some GDPR principles omitted (uncertain how essential they are for adequacy)
- Data export restrictions
  - Based on 'equal or higher' law of recipient country (regs can include a White List)
  - Other grounds: international agreements; contractual fulfillment; consent (weak notice)

Indonesia – *Protection of Personal Data draft law 2020* (2)

- No DPA created (very surprising)
  - Contrary to previous drafts, GDPR, and international practice
  - Ministry of Comms. and Info. (MCI) holds all enforcement powers in Govt Bil
  - *House of Reps (DPR) is disputing lack of independent DPA as of 11/21 – Bill is blocked*
- Enforcement powers (very weak)
  - No explicit method of making complaints; could be in regs
  - Administrative sanctions for breach of some controller obligations, but none for breach of individual rights; amounts of fines not stated, await regs
  - Compensation is awarded by the Minister, not a court!! Unclear if it includes breach of controller's obligations, or only user rights; appeal rights unclear
  - No criminal offences for breaches of controller obligations, but some general offences
  - Previous Bill included supervising mediation (like Korea); compensation by DPA; administrative penalties up to US$2M; criminal offences
- Result (if enacted with no DPA):
  - Principles – one of stronger Asian laws
  - Enforcement – pathetic, compared with previous Bill. Will not work.
  - Ministry enforcement: has never worked anywhere else.
  - Lack of DPA – no EU adequacy; no Conv. 108+ accession

  Overall, probably a waste of effort until a separate/independent DPA is created

Vietnam

[ADPL Ch 13; Materials article on Vietnam; also 2019 Update.]

- *Context:* Still a one-party state, but since mid-1990s ASEAN membership has become a leading member, with a strong private sector ('socialist market economy'. Structure of legal system similar to China.
- APEC and ASEAN member; not OECD; party to CPTPP; signatory to RCEP.
- A38 Civil Code, 'Right to Privacy' (minor significance)
  - Limited constitutional and treaty possibilities, but A 38 is more relevant
  - 'collection and publication of information and data about the private life of an individual' requires consent or state authority approval
  - 2012 Court decision in favour of a company's right to access and monitor an employee's work email account, on basis of implied consent (p 367)

Vietnam – Existing data privacy laws

Prior to 2016, scattered across consumer, IT and e-commerce laws

- *Law on Information Technology* 2006
  - Covers all entities (including some public sector) using IT applications.
  - A21 & A22 set out obligations on organisations covered by the law in relation to consent, exceptions for processing without consent, notice, use, retention/deletion, security, access (perhaps), correction (including blocking until corrected), disclosure, and compensation.
- Law on Protection of Consumers' Rights 2010
  - Scope of earlier law broadened to apply to all consumers
  - A6 'Protection of consumer information' (Short OECD/APEC code)
  - A10 provisions are also relevant: Misleading or deceptive conduct in advertising; Harassment of consumer through marketing
- Decree 52 on e-commerce and consumer law (2013)
  - Regulation by government as a whole, not a Ministry
    - Prime responsibility to Ministry of Industry & Trade (MoIT)
    - But Ministry of Industry & Communications (MoIC) also has a role
  - Data controller/ processor agreements may allocate who has responsibility for any breaches by processor

Laws still operate but are now subordinate to 2016 & 2018 cybersecurity laws

Vietnam – Existing laws (2)

- *Cyber Information Security Law* (2016) - 2019 Update.
  - now the most detailed data protection law; highest form of legislation
  - Scope limited to online commercial transactions (broadly interpreted)
  - Lacks clarity on enforcement (no DPA)
- Principles are a reasonable approximation of all 'OECD/APEC basics', plus they go further in three areas :
  - Deletion rights (not automatic, only on request)
  - Direct marketing opt-out
  - Data breach notifications (only to notify authorities in the event of attacks)
  - Data exports – no separate provision until 2018 Cybersecurity Law
- *These additions are now a frequent intermediate point in Asian laws between the OECD/APEC basics and 'European' positions*

Vietnam – Enforcement?

- No special DPA established, Ministerial split responsibilities continue
  - Ministry of Trade & Industry has overall supervision of consumer law, but not a complaint resolution function
  - Ministry of Post and Telematics has the prime responsibility for, IT law (A 7(2)), with an 'inspection' function carried out by its Inspectorate (A 10(1)).
- Enforcement – low levels of penalties and compensation
  - General requirements under Consumers law
    - Administrative penalties and criminal prosecutions possible
    - Compensation required for any loss/damage caused
    - 'Social organisations' can take legal proceedings for consumers
    - No regulations or guidelines issued yet, but may occur
  - IT law is now more specific on enforcement due to Decrees
    - Decree 174 (effective Jan 2014) very specific on many breaches which could result in fines of around US1,000 at most
    - Decree 185 similarly detailed on offences by website operators
- Difficult to find evidence of enforcement

Vietnam – Existing Localisation and export limits

- *Cybersecurity law* (June 2018) – 2019 Update.
  - Very contentious, 16 drafts, foreign opposition; final version much more moderate
  - Scope: domestic and foreign companies providing online services to customers in Vietnam ('Providers')
  - Effective 1/1/2019; Regulations needed to fully implement.
- Data localisation/ export prohibition in 2018 law (Not in force – see 2021 draft)
  - Must store in Vietnam data generated by users (localisation #1) for a period of time, but foreign providers are not required to establish own server. Exports then allowed.
  - Prohibition of export of 'critical data' (localisation #2) appears to have been dropped from Bill. Storage in Vietnam' does not seem to imply 'exclusively in Vietnam'.
- No explicit data export restrictions/rules (localisation #3)
  - Consumer Law A6(2)(e) requires consent for any transfers to 3rd Ps, 'except where otherwise provided by law' - but no special 'border control' element. (No new law on this)
- **Bottom line:** Chinese-influenced approach to localisation etc, but not identical
- *Very confusing – needs enactment of 2021 draft Decree to clarify*

Vietnam – comprehensive proposed Decree (2021)

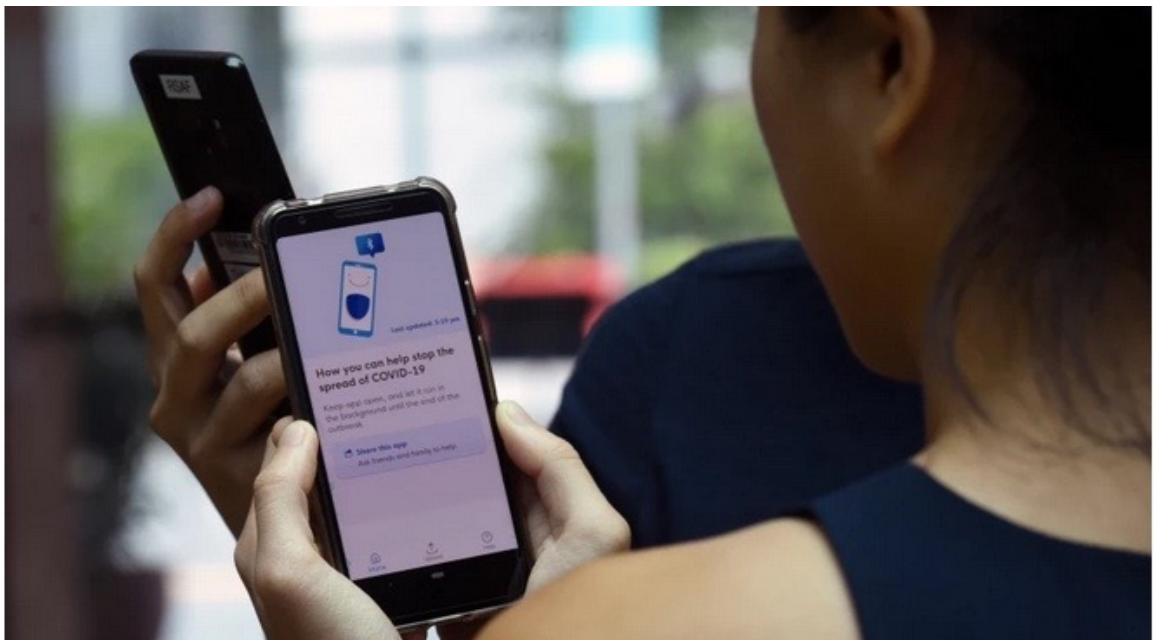
Materials: article on Vietnam's draft Decree (04/21)

- Ministry of Public Security (MPS) draft *Decree on Personal Data Protection* (Feb. 2021)
  - Was aiming for govt. adoption (under *Law on Cyber Security* 2018) and in force by 01/12/21 – but as at 02/22, not adopted. PM has given MPS deadline of 06/22 to complete Decree, and 2024 for full DP Law
- PDP Committee created within MPS; 'no more than 06 comrades';
  - PDPC extensive functions, but all enforcement remains with MPS
- Scope: (similar to China)
  - public sector included (!); processors also
  - anyone 'doing business in Vietnam' (extra-territorial);
- 'Sensitive data' (defined very broadly)
  - processing must be registered; impact assessments required
  - Foreign business concerns: costs; delays; intrusiveness

Vietnam – proposed Decree (cont.)

- Rights & obligations (see article)
  - Relatively strong on data minimisation; consent
  - Weaker on non-consensual processing; de-identification; automated processing
- Data exports and localisation (see article)
  - Detailed baseline export requirements for 1st time
  - All 4 requirement necessary: (i) consent; (ii) local storage; (iii) proof that laws of destination are at least equal to Vietnam; & (iv) written PDPC approval.
  - Alternatively, (i) & (iv), and undertakings at both ends, can suffice (no (ii) local storage). This appears to apply to data on non-Vietnamese data subjects.

Singapore



[ADPL Ch 10 'Singapore – Uncertain scope, strong powers']

23

Singapore

Materials – article on Singapore by Chen & Girot; also 2019 Update; Greenleaf Ch. in Chesterman (ed) DP Law in Singapore *(2018)*

- *Context:* Stable, prosperous, somewhat authoritarian democracy (no changes of government ever); high standard rule of law
- APEC & ASEAN; not OECD; APEC-CBPRs; ratified CPTPP & signed RCEP
- Minimal protections in the general law
  - No constitutional or treaty-based privacy protections
  - No significant tort protections (other than harassment legislation)
  - Some sectoral privacy protections (eg banking law)
- *Personal Data Protection Act* (PDPA) 2012
  - Data privacy aspects in force July 2014
  - Almost all privacy protection in Singapore depends on this Act
  - Personal Data Protection Commission (PDPC) is not independent – a branch of a government department; is largely 'separate' and expert
- 2020 amending Act is first significant update since 2012

24

Singapore
PDPA Scope & exemptions

- Public sector excluded, but boundaries were uncertain
  - Public sector has a privacy code, but content unknown, and unenforceable
  - *Exemption for companies acting for government repealed 2020*
- Private sector scope covered is also uncertain
  - Both regulations and PDPC can exclude any private sector bodies, or any types of activities, from scope of PDPA (has not occurred)
  - Any other law (legislation or other) also overrides PDPA (Many other Singaporean laws have some effect on privacy and confidentiality: at least 161)
  - Lengthy lists of specific exemptions in PDPA (p296)
  - 'Personal data' excludes any publicly available data
  - Some limited exemptions in favour of media
- Result: Scope of PDPA is a 'known unknown' (less so now)

Singapore - PDPA Principles

- Principles cover '1st generation' basics, little else
  - Additions: necessary collection; deletion/de-ID; data exports
  - Omissions: 'sensitive data'; direct marketing opt-out; data breach notification *(now in 2020 reforms)*
- Collection, use & disclosure appear to be based on notice & consent, but are really 'exception based' (more so after 2020)
- 4 factors make exceptions dominate (ADPL p298):
  - i. *Deemed consent* by voluntary provision of data, wherever this is reasonable. (More 'deemed consent' added in 2020 – later)
  - ii. If deemed consent, *no notice* required.
  - iii. Neither consent nor notice wherever lengthy 2nd-4th *Schedules of exemptions* apply
  - iv. *Any other law* can override need for notice or consent

Result: Look at exceptions first, then if out of luck …

Singapore – Data exports (1)

Personal Data Protection Regs. (2014)

- S26(1) requires data exporters to ensure a 'comparable' standard of protection to PDPA
- Exporter must comply with PDPA, wherever data located, if it retains possession/control (R9(1)(a))
- Exporter must ensure recipient also has a 'legally enforceable obligation' to provide comparable protection (R9(1)(b))
  - Can be via legislation (no 'WhiteList' provisions), contracts, BCRs etc:
  - Failure to do so a breach by exporter: PDPC penalties (v. strong)
  - Data subject's remedies against importer will have to arise under this 'legally enforceable obligation' (if aware of it!! – becomes public?)

Singapore – Data exports (2)

Singapore's multi-faceted approach to exports

– 2019 update p. 22; 2018 Update p. 14;

1. PDPC's recommended Standard Contract Clauses [*Article on request*]
   - Now in ASEAN Data Management Framework & Model Contractual clauses (2021)
2. Joined APEC-CBPRs (3rd country fully involved: + US and Japan)
   - Accountability Agent appointed; 2 Singaporean companies accredited (01/21)
   - Singapore deems APEC-CBPRs accreditation is 'comparable' to Singapore: any Sing company can export data to the 20+ US companies accredited in the US; 3 in Japan
3. Data Protection Trustmark Certification Scheme (DPTM Cert)
   - 3 assessment bodies appointed by IMDA (Infocomm Media Development Authority)
   - Some type of joint certification with APEC-CBPRs is possible (but has not occurred)
4. Singapore's *Cybersecurity Act* 2018
   - allows designation of 'critical information infrastructure' (CII); but not data localisation

Result: Singapore is exploring many avenues of 'mutual recognition'

Singapore – 2020 amendments to principles

[Article in Materials; 2019 update; See Greenleaf Ch, in Chesterman (2018) for critique]

2 November 2020 – amending Act enacted, after 5 years; main changes:

1. **Data portability** – to enable consumers to switch to a new provider
2. Mandatory data breach notification **(DBN)**
   - now a global standard, even in APEC Framework
   - Notification to PDPC w/in 30(!) days, if likely to cause significant harm (defined in Regs), or affects more than 500 persons – exceptions stop disclosure / transparency
3. **'Deemed consent' expanded** to include (i) contractual necessity and (ii) notice + failure to opt out (after risk assessed)
   - **Opposite** of stronger consents required by GDPR and most other laws
   - may destroy most limits on use & disclosure (2018 chapter, [14.29])
4. '**Legitimate interests' non-consensual exception** to any processing
   - Supposed to require that public interest outweighs individual interests
5. **'Business improvements' non-consensual exception** to any processing, when to improve any aspect of surveillance capitalism
   - Must be 'what a reasonable person would consider appropriate in the circumstances'

These last 3 exceptions make most of the Act irrelevant; only 'security' remains

Singapore – Enforcement

- Personal Data Protection Commission (PDPC)
  - A government authority, not an independent DPA
  - 6 members as yet – from InfoComm Development Authority) + Advisory Committee
  - Powers to issue Guidelines (does so), as well as enforce Act
- Strong PDPC enforcement powers
  - Can investigate on complaint or own motion
  - Broad powers to direct compliance; **can fine up to S$1M**; fines often S$10K-30K, sometimes S$50K;
  - 2019 fines of SingHealth (S$250K)(a government authority??) & IHIS (S$750K) for data breaches affecting 1.5M people (highest Asian fines except Korea)
  - PDPC cannot award compensation (courts can: next slde)
  - Appeals on all grounds are to 3 person appeal committees of the Data Protection Appeal Panel; then to District Court etc – none known
  - **Transparency**: 2015 Regulations allow publication of decisions, publication is very regular, and respondents are always named ('name and shame')
  - For examples of enforcement action, see See 2017 *Update* pp. 25-26; 2018 Update p. 13; 2019 Update p.21.

Singapore – Enforcement (2)

- Offences usually require dishonest intent to be shown
- Actions before courts for compensation, injunctions or other remedies for breaches of Principles
  - PDPA requires any appeals against PDPC completed first
  - Plaintiffs will bear risks of 'costs against' in Singapore's expensive courts – unrealistic to expect many such actions
  - No such actions known
- Personal & vicarious liabilities increase risks
  - Employers have vicarious civil liability for acts of employees
  - Company officers have personal liability for offences involving their consent, connivance or neglect (like Korea).

Singapore – 2020 amendments to enforcement

Materials – Chen & Girot article; For critique, see 2019 update; See Greenleaf Chapter in Chesterman (2018)

- 2 November 2020 – amending Act enacted, after 5 years
- **Maximum fines** for breaches increased (was SGD 100K)
  - **10% of annual turnover in Singapore**, or SGD $1M, whichever higher
- Criminal offences for **egregious mishandling** of personal data
  - Individual knowing or reckless misuse of an organisation's personal data
- **Voluntary undertakings** to PDPC in lieu of full investigation
  - May avoid very large fines
- **Compulsory mediation** can be required by PDPC
- **Right of private action** for breaches of PDPA, in civil court
  - Not only for compensation, but for any remedy when rights are breached

Result: Singapore now has a very diverse 'enforcement toolkit' – possibly strongest in Asia other than Korea.

Singapore –
Result of 2020 amendments

Still half-way between 1st and 2nd generations

- GDPR has had limited effect, 'data sovereignty'/localisation no effect
  - Singapore goes its own way
- 'Minimalist' model of Asian data protection (even Japan has stronger principles)
- But within the limits of its law, enforcement is serious (contra Japan) – but in effect is limited to security breaches

Easy for businesses to comply, dangerous not to

Malaysia

[ADPL Ch 11 'Malaysia – ASEAN's first data privacy law in force']

Malaysia

- *See 2019 Update p. 19; 2017 Update pp. 26-28*
- *Context:* Since 2018 first democratic change of government; legal system previously abused for political ends, might now be reformed. 'Wait and see'.
- *General law provides no protections*: No constitutional or civil law protections of privacy; Malaysia has not even signed the ICCPR.
- *Personal Data Protection Act* (PDPA) 2010, in force Feb 2014
  - covers private sector only, and only 'commercial transactions'
  - Principles are pre-GDPR EU-influenced, with many weaknesses.
  - Commissioner lacks independence ; does not have international accreditation
  - 3rd PDPC appointed 2017 but died; first two had no impact; 2nd re-appointed
  - No effective enforcement by DPA, only prosecutions for offences
- 'Whitelist' approach to data exports, with over-broad exceptions
  - 2017 draft Whitelist (2017 p. 27) is unjustifiable; appears to be forgotten.
- Following 2018 election, new Minister claimed PDPA under review
  - 14/2/20 PDPC released 22 proposed amendments, called for submissions
  - As at 28/8/20 Minister said amendments were "still in the discussion stage'.

Result: No reforms yet to a weak and un-enforced law

Malaysia – Privacy principles

- All basic OECD principles included, and some others (p324-).
- Only covers data in 'commercial transactions' (broadly defined) 'whether contractual or not'; extent of exception of non-profit bodies is uncertain
- Requires consent to processing of data
  - Processing (collection, use and disclosure) must be directly related to a lawful activity of user and not excessive; Many exceptions (s6(2), s39, s40, s45)
  - Allows withdrawal of consent to processing (s38, s42)
- Other non-OECD principles include written notice (s7), retention limitations (s10), opt-out from direct marketing; sensitive data
- Weaknesses of principles
  - notice of intention to disclose can circumvent limitations;
  - broad and discretionary exemptions possible from many principles
  - a complex and somewhat weak 'media exemption' (p323)
  - danger of State abuse of selective 'sensitive data' provisions

Malaysia – Enforcement

- **Registration** - Minister may require registration of specific classes of data users
  - Most data users required to register – fund raising purpose
- (Only) if **PDPC finds contravention** of Act is *continuing or likely to be repeated*, can issue enforcement notice (s108)
  - Offence for data user to fail to comply with enforcement notice (US$60K fine possible)
  - No remedies where breaches are unlikely to recur
  - Same defects as Hong Kong and pre-2011 UK laws (UK fixed; HK proposed)
  - Rights of appeal by either party to Appeal Tribunal (Pt VII)
- Any breach of a Principle is an **offence** (s5(2)), prosecuted by decision of the Public Prosecutor, before Supreme Court
  - Unusual to have offences as the principal form of enforcement
  - Other offences for 3rd parties collecting, or disclosing without consent, data held by a data user (s130)
- PDPC has **no power to award damages** or role of conciliating
- **No individual rights** to seek compensation or proceed in court

Result: No enforcement known, except for failure to register. Law is useless.

Malaysia – rumoured Bill (Feb 2022)

- Rajah & Tann law firm article 11/2/22 says Dept. of PDP has prepared a Bill as follows.

1. Direct obligation on processors re security
2. Mandatory data breach notification to DPA
3. Mandatory Data Protection Officers (DPOs)
4. Data portability
5. Data exports to be OK to any country not on Black List
6. Governments (Fed & State) to come under Act
7. (If 6 enacted) DPA to be made independent
8. Civil remedies for breaches

These changes would be seismic – close to a modern law

Philippines

[ADPL Ch 12 'The Philippines … ASEAN's incomplete laws']

39

Philippines

- See 2019 Update, p. 19; 2017 *Update* pp. 28-30
- *Context:* Since Marcos dictatorship (1986), stable but low quality democracy, emphasizing spoils of office; current President supports extra-judicial executions
- APEC & ASEAN; not OECD, nor CPTPP; not APEC-CBPRs; RCEP signatory
- Very limited general law rights
  - Constitutional protections of privacy, used periodically
  - Right of 'Habeas data' (constitutional right of access and correction) adopted by Supreme Court (2008) - No known uses as yet
- *Data Privacy Act 2012,* is finally fully in force since August 25 2017
  - National Privacy Commission (NPC) appointed 2016 by departing Aquino
  - NPC made Implementing Rules & Regulations (IRRs), to bring Act into effect; Business was given 1 year (to 25/8/2017) to comply (s42)
- NPC is extremely active in promoting Act; first enforcement step was to recommend prosecution of head of Electoral Commission (p. 29)

40

Philippines – Principles

- Covers both public and private sectors, all data
- *Collection* limited to 'not excessive' data (not 'minimal')
- Subsequent *use/disclosure* requires consent (express/implied) or a broad exception requiring balancing of necessary interests of controller/ 3rd P against constitutional rights of data subject (ie weak protection)
- Processing of *sensitive data* generally prohibited, and very broadly defined - much stricter than elsewhere (Caution!)
- *Data breach notifications* to both Commission & individuals
- *Deletion or blocking* of data required after use completed
- Novel 'right to *data portability*' not found elsewhere

All OECD basic principles covered; last 3 principles go beyond OECD

Strong influence of EU Directive throughout – except for data exports

Philippines – Data exports

- No express data export limitations (s9A 'Accountability')
  - Makes controller 'responsible' for international transfers, 'subject to cross-border arrangements and cooperation';
  - Also 'accountable for complying with the … Act' and for 'using contractual or other reasonable means to provide a comparable level of protection while the information are being processed by a 3rd party'
  - Unknown what this means in practice
- Outsourcing exemption explicitly provided
  - excludes all personal information originally collected from residents of foreign jurisdictions in accordance with their laws, being processed in Phil. (s4(f))
  - Intended to exempt all outsourced processing but may fail to exempt call centres operated from the Philippines
  - Also a Pyrrhic victory, if it succeeds in attracting US outsourcing but EU decides it means no 'adequacy' (p348)
  - Pakistan has a more subtle version (see later)

Philippines – Enforcement

- **National Privacy Commission (NPC)** – an activist DPA
  - Exists since 2016; Within the Office of the President; Commissioner + 2 Deputies
  - Oversight and coordination role in both sectors; advice, codes etc
- **NPC orders** and compensation for any breaches
  - NPC has strong powers to investigate (both complaints, and on own-motion)
  - Can 'adjudicate' and 'award indemnity' (compensatory damages)
  - Can make compliance orders and ban processing, temporarily or permanently
  - Specific power to publicise the sanctions it has used
- **Transparency** of NPC actions is very high:
  - NPC Advisory Opinions – 260 to 11/20 since 2017 (equivalent to case notes)
  - Commission-issued Orders – 9 to 11/20 (variety of breaches)
- **Civil actions** (only as a consequence of a criminal breach)
  - Actions for damages ('restitution') under Civil Code possible
- **Criminal** penalties
  - NPC can recommend prosecutions
  - Many criminal penalties for breaches (eg unauthorised processing)
- 2021 consultancy on **administrative fines** – none at present
- Privacy Codes (NPC can approve or reject: consequences uncertain)
- Philippine Privacy **Trust Mark** ('PPTM') (since 11/21) assuring compliance

The other 5 ASEAN states

[ADPL Ch 14 'Privacy in the other five …']

•**Brunei** –

- Public sector Privacy Policy ; 2021 Bill for private sector, based on Singapore's Act

•**Cambodia** – Nil significant

•**Laos** – Nil significant

– but 2017 *Law on Electronic Data Protection* is unclear as to scope

•**Myanmar** – Nil significant

+ **Timor Leste** (candidate member)

– Novel constitutional protection of personal data

Regional pressures are most likely to prompt privacy laws:

- *all ASEAN countries are RCEP signatories;*
- *RCEP: Cambodia, Laos & Myanmar have 5 year exemption from obligation to provide some data protection laws (art. 12.8)*
- *development of ASEAN Economic Community*

South Asia

India

[ADPL Ch 15 'India – Confusion Raj, with outsourcing'];

India – Overview

2019 Update pp. 15-18; 2018 Update pp.15-20; 2017 Update pp. 33-36
Materials: 'India's data privacy Bill: Progressive principles… (Feb 2020); 'Report keeps India's DP Bill partly within GDPR Orbit' (Jan 2022)

- *Context:* World's largest democracy, with often-functioning rule of law, despite consistent problems of corruption. Huge outsourcing.
- India's legislative privacy protections are still piecemeal; its supposedly general 'Rules' of 2011 are in fact very limited and useless
- India twice failed to obtain an EU adequacy finding (most recent 2013)
- Crucial question: Does the Indian Constitution imply a privacy right?
  - A 21 protection of 'personal liberty' is the basis
  - Was mainly used to limit search and surveillance *Naz Foundation Case* (2009) extended previous case law by holding unconstitutional legislation criminalising homosexuality, based on autonomy; overturned by SC appeal (2013); Supreme Court had not expanded this to 'informational self-determination
  - The Aadhaar ID number system was attacked as being unconstitutional, with Mr Puttaswamy (92 year old SC judge) as one of the petitioners…

47

48

India - *Puttaswamy*'s consequences

- In *Puttaswamy v Union of India* (2017) the Indian government argued there was no constitutional right of privacy at all; in August 2017 a nine judge 'constitution bench' of the Supreme Court found there was an **inalienable fundamental right of privacy** (Chandrachund J, lead opinion)
  - **three main aspects of privacy**: privacy of the body; privacy of information; and privacy of choice.
  - Any legislation/government actions affecting privacy must be (i) for legitimate state interests; (ii) necessary and proportionate [when balanced against privacy interests]; & (iii) authorised by law. (***Puttaswamy* test**)
  - All Indian privacy issues are now in flux because of *Puttaswamy:*
  - *Navtej Johar v Union of India* (6 September 2018) – five judge Constitution Bench held criminalisation of homosexual conduct was unconstitutional (reversing result of 2013 *Naz* appeal).
  - *Puttaswamy #2* – Challenge to constitutionality of Aadhaar biometric ID system was defeated 4/1 by Constitution Bench in Sept. 2018 (Chandrachund J dissenting); held partially unconstitutional but Aadhaar survived; legislation was enacted 2019 to remedy the unconstitutional defects.

India – Personal Data Protection Bill 2019

- *Modi government's imperatives*:
  1. The Aadhaar has been saved by *Puttaswamy #2* .
  2. But many *other government schemes* will still need to show that any invasions of privacy involved are 'necessary and proportionate' through legislation that *sufficiently* protects privacy against abuses.
  3. To obtain a *positive adequacy assessment* from the EU, particularly to benefit its outsourcing industry.

  So, a comprehensive data privacy law may be needed, **meeting Puttaswamy requirements** …
- *Personal Data Protection Bill 2019*
  - Srikrishna Report (July 2018) recommended draft *Bill 2018*
  - Indian government (DeitY) called for submissions in 2018.
  - Government Bill finally tabled in Lok Sabha Dec 2019
  - Joint Committee of both houses required submissions by 25/2/20
  - Committee hearings complete: **Report delivered 12/2021 (later**).

India – Personal Data Protection Bill 2019 (2)

- **Srikrishna Bill 2018** compared with GDPR:
  - See 2019 Update; 2018 Update pp. 17-18
  - More prescriptive than the EU's decentralisation of responsibility/liability to controllers
  - Many key GDPR features were included:
    - Some GDPR obligations only apply to 'significant' controllers
    - GDPR elements excluded may not be vital
  - Potentially very strong enforcement by a national DPA, including up to 4% administrative fines
  - Combined with strong data localisation requirements (other Asian influences?) and data export limitations
- Most of these features are *retained* in 2019 Govt. Bill

India – Personal Data Protection Bill 2019 (3)

Materials: 'India's data privacy Bill: Progressive principles, uncertain enforceability' (Feb 2020) – critique based on my submission to Committee

- Comprehensive of both private & public sectors
  - Any agencies can be exempted by Executive Order (contrary to Srikrishna; possibly unconstitutional); broad security/enforcement exemptions
  - Extra-territorial application similar to GDPR
  - Possible 'outsourcing exemption' of data of foreigners not present in India (eg could apply to USA-sourced data but not EU-sourced data)
- Data Protection Authority of India (**DPAI**)
  - Chair + up to 6 full-time members; dominated by govt.
  - No guarantee of **independence**, can be given (secret) policy directions (disastrous for EU adequacy)
  - Can investigate, issue reprimands and order – appeal to Tribunal
  - DPAI cannot issue fines or award compensation
  - **Adjudicating Officers (AOs)** appointed by DPAI can decide both
  - Unusual for a DPA to be able to award compensation (Australia is another)
  - Fines up to US$2.1M **or 4% of worldwide turnover**

India – Personal Data Protection Bill 2019 (4)

- Categories of data
  - Sensitive data: defined, but special protections *to be added* by regs
  - Anonymous data: DPAI can define standard, effect uncertain
- Categories of data fiduciaries (DFs) have different obligations
  (Controllers are called 'fiduciaries' (as in 'trustees') but this means little)
  1. 'Significant' DFs: designated by DPAI, higher obligations
  2. 'Small' DFs: annual turnover (eg under US$30K)
     - Exempt from many obligations
  3. 'Normal' DFs: those without higher or lower obligations

  See article for *many* differences in obligations of the three
  - This is **uniquely Indian**: may be a model (if EU is happy)
- Rights & obligations
  - Article: **Almost all GDPR elements included** (+ registration with DPAI!)

India – Personal Data Protection Bill 2019 (5)

- Data exports and localisation
  - India's v. unusual approach: division b/w 'sensitive' and 'non-sensitive' data results in 3 types of data localisation (see article)
  - DPAI probably has too much discretionary control
- Conclusions
  - Standards generally v. high (GDPR-like) in principle
  - But more prescriptive than GDPR's dispersal of responsibility
  - DPAI is not independent enough; enforcement uncertain
  - Data principals (and NGOs) unable to enforce effectively
  - Unique Indian elements: (i) obligations depend on category of fiduciary; (ii) data localization/export rules differ (from China)

India – Report of Joint Parlt. Committee 12/2021

- Main changes proposed by 32 member JPC:

1. Less DPAI independence – govt. to be able to give directions on anything
2. Bill should cover all data not just personal data!
3. Extra regulation of social media platforms
4. Even more discretionary controls over data localization
5. Attempt to make powers to exempt govt. bodies consistent with Puttaswamy
6. Changing basis of lawful grounds – more Puttaswamy problems?
7. Various changes to user rights, generally positive

Overall, if adopted, India's Bill would still be a GDPR variant

Sri Lanka

Materials: (i) 'Advances in South Asian DP Laws: Sri Lanka, Pakistan and Nepal'; (ii) 'Sri Lanka's latest 'final draft'; (iii) 'South Asian privacy bills move forward'.

- Unstable democracy; no constitutional protections
- Personal Data Protection Bill 2019
  - 2019 'final draft' replaced by two 2021 'final drafts'; few major changes; 3rd draft certified to be tabled in Parliament
- **Comprehensive**: public & private sectors
- **Extra-territorial effect** is similar to GDPR; 2021 draft removes ambiguity about processing occurring in SL
- **Few exceptions**, but dangerous regulatory powers
- Covers deceased persons; extra protection for sensitive data

Sri Lanka – Personal Data Protection Bill 2019 (2)

- Principles in the PDP Bill (little changed in 3 drafts)
  - Lawful grounds for processing similar to GDPR
  - Further processing must be 'not incompatible'
  - Proportional & 'not excessive' processing required
  - Data breach notification (DBN) required
  - 'Demonstrable accountability'?: broad DPO requirements; DPIAs required before processing, and DPA must be consulted if high risk
  - Data subject rights similar to GDPR: incl. withdrawing consent; right to erasure (perhaps not 'RTBF'); very narrow right of review of automated decisions; no data portability
  - appeals to DPA and courts

Sri Lanka – Personal Data Protection Bill 2019 (3)

- **Enforcement**
  - 'Data Protection Authority of SL' to be appointed from existing authorities
    - no independence, can be given instructions by Cabinet
    - Most appeals against decisions go to Court of Appeal
  - Poor drafting re DPA's ability to receive complaints
  - DPA can direct compliance; to suspend licences etc
  - Fines only for failure to follow directions, not simply because of breach (same problem as HK, Malaysia)
  - DPA can issue fines of US$55,000, double if repeated – now very low, even for Asia
    - no '2% of global turnover' found in earlier version
  - No other enforcement methods: eg compensation

Sri Lanka – Personal Data Protection Bill 2019 (4)

- **Data exports & localisation**
  1. **Public sector** data: requires both (I) *local copies*; and (ii) *local processing* (unless in a category DPA says OK for overseas processing, and going to a white-listed country)
  2. **Private sector** data: Minister & DPA can 'white-list' countries, with detailed criteria and review requirements
  3. Otherwise, exporters must ensure compliance with specified sections of Act, via a **binding agreement** (SCC equivalent)
  4. **Extra-territorial scope**: superficially like GDPR, but only if 'specific' targeting, and in DPA-defined circumstances

Bottom line: (i) A reasonable Bill on principles; (ii) weak on DPA independence; (iii) pathetic on enforcement; (iv)complex data export restrictions

Pakistan

Materials: 'Pakistan's DP Bill' (2020); 'Pakistan's … privacy bills move forward'

- Unstable democracy, with periodic military regimes
- World's 5th largest population; largest economy in Asia without a DP law; Few existing privacy protections
- *Personal Data Protection Bill 2020* (PDPB)
  - Draft Bill, from IT & telecoms Ministry; submissions closed
  - Sindh High Court in 04/21 ordered Federal Ministry to report in one month on progress in bringing a Bill to Federal Cabinet (!)
- Largely **comprehensive** of private & federal public sectors, but with scope for Ministerial exemptions
- **Extra-territorial** scope: (all differs from GDPR – b) and c) may be inconsistent)
  - a) Any processor involved in commercial or non-commercial activity in Pakistan;
  - b) If data subject is located in Pakistan, any foreign processing must comply
  - c) Foreigner's data: protected (only) by law of where foreigner lives or data is collected (convenient re USA and EU!!) (adequacy problems?)

Pakistan – *Personal Data Protection Bill 2020* (2)

- **Legitimate grounds for processing** defined
  - Consent + 7 non-consensual grounds, incl. 'legitimate interests' of processor
  - Over-broad definition of 'legitimate interests' undermines whole approach
- **Many GDPR-like principles**, but not comprehensive
  - **Most are included**: automated deletion; data breach notification; blocking and erasure (incl. 'RTBF'); automated processing rights; data portability
  - Omitted: demonstrable accountability, design & default
  - Categories of sensitive data very different from EU
  - Pseudonymised data is excluded from 'personal data' - inconsistent
- **Data exports & localisation**
  - **Exports:** O/S processing must offer protection 'at least equivalent'; DPA may prescribe alternatives (unclear)
  - **Localisation:** (i) A local copy of all data exported no longer required, but only of 'some sensitive data' concerning public order or national security;and (ii) 'critical personal data' (CPD, now defined very broadly!) may only be processed in Pakistan. Will be contentious outside Pakistan.

Pakistan – *Personal Data Protection Bill 2020* (3)

- National Commission for Personal Data Protection (NCPDP)
  - Has 'autonomy', except govt. can issue policy directions (!) (problems for EU or Conv. 108+)
  - 5 full-time member NCPDP, all described by qualifications (previously, 3 from Ministries)
- Enforcement
  - NCPDP has powers of a 'Civil Court'
  - Powers to order compliance, impose penalties; compensation unclear
  - Many other powers, including licensing, and regulations
  - Fines for breaches: vary b/w maxima of US$15K to 150K; corporate liability can be from US$200K to 1% of local turnover
  - Failure to comply with NCPDP order in 15 days: penalty up to US$1.5M
    - Clarification needed whether civil or criminal penalties
- Result: Like SL, strong on principles, but with weaknesses in DPA independence, scope of 'sensitive data', pseudonymity & data exports

The rest of South Asia / SAARC

[ADPL Ch 16 'Privacy in the other 7 SAARC states'] 2019 Update Materials: 'Advances in South Asian DP Laws' (Dec 2019)]

- If Bills are enacted in India, Pakistan & Sri Lanka, South Asia will be similar to other Asian sub-regions, perhaps stronger than ASEAN
- **Nepal** – has a public sector data protection law within its *Right to Information Act* 2007; *The Privacy Act 2018* (not a data privacy law)
- **Bhutan** – data privacy law within e-commerce Act (2018)
- **Bangladesh** – no Bill known
  - Development of digital ID cards, as in India
  - Often influenced by Indian developments
- No **SAARC** initiatives
  - 'South Asian Area of Regional Cooperation'
  - Unlike ASEAN, no interest shown in data privacy as yet
- As with India, outsourcing is a factor in Pakistan, perhaps others

International /regional standards and Asia

See 2019 Update, pgs 67-71; Materials: 'Will Asia-Pacific trade agreements collide with EU adequacy and Asian laws' (Oct 2020); pages in 2019 update:

1. No significant regional standards (p. 67)
2. 'Data free flow with trust' means? (p. 67)
   - Significant split across Asia over data export & localisation rules
3. CPTPP in force with 6 parties: privacy dangers (p. 69)
   - UK would like to join CPTPP; will Biden's US 'rejoin'?
   - New RCEP treaty with 15 signatories is more privacy-protective
4. APEC-CBPRs has 2 participants (pp. 69) – Table over
   - Now 3 with Singapore
5. Convention 108+ - slim prospects (pp. 70)
6. EU adequacy beyond Japan & Korea? (p. 71)
7. Other EU 'appropriate safeguards' (p. 71)
8. Conclusions on Asian 'convergence' (pp. 72-3)

APEC-CBPRs has 3 participants

(add AAs in Singapore (3 certifications) & Korea (0) 2019)

APEC economy	Approved to join APEC-CBPRs	Accountability Agent appointed	No. of Companies certified
USA	**2012**	**2013**	**26**
JAPAN	**2014**	**2015**	**3**
CANADA	2014	–	0
MEXICO	2014	–	0
KOREA	2016	–	0
SINGAPORE	2017	–	0
TAIWAN	2018	–	0
AUSTRALIA	2018	–	0
OTHER 11 IN APEC	–	–	0

65

2nd Generation principles (EU DPD & revised 108) 1995-2016 – as seen in Asian Acts and *Bills*

	2nd Gen Principles	Asia (/17 Laws or *Bills* @ 06/21)	/17
2.02	***'Deletion'** - Destruction or anonymisation of personal data after purpose completed*	Bhutan, *Brunei, China*, Hong Kong, *India*, *Indonesia*, Japan, Korea, Malaysia, *Pakistan,* Macau, Philippines, *Sri Lanka,* Taiwan, Thailand, Singapore,	16
2.09	*Specialised **Data Protection Authority** (DPA) – only 4 are **independent****	Bhutan, *Brunei,* Japan*, *India*, Korea*, Macau, *Pakistan,* Philippines*, Hong Kong*, Singapore, Malaysia, *Sri Lanka*, Thailand, Vietnam	*14*
2.10	***Recourse to the courts** to enforce & compensate & appeals from DPAs*	Bhutan, *Brunei,* China, Hong Kong, *India*, *Indonesia*, Korea, Macau, *Pakistan,* Philippines, Taiwan, Singapore, Thailand, Vietnam	*14*
2.01	***Minimum collection** necessary for purpose (data minimisation)*	Bhutan, *Brunei, China*, Hong Kong, *India*, *Indonesia*, Korea, Malaysia, Macau, Taiwan, Singapore, Thailand, *Vietnam*	13
2.04	***Legitimate bases for processing defined***	Bhutan, *China*, *India, Indonesia*, Korea, Malaysia, Macau, *Pakistan,* Philippines, Singapore, *Sri Lanka,* Taiwan, Thailand	*13*
2.08	***Restricted data exports required** based on recipient country protections*	*China*, *India*, *Indonesia*, Japan, Korea, Malaysia, Macau, *Pakistan,* Singapore, Thailand, Taiwan, *Sri Lanka, Vietnam*	*13*
2.03	*Additional protections for **sensitive data** in defined categories*	Bhutan, *China, India, Indonesia*, Japan, Korea, Malaysia, Macau, Philippines, Taiwan, Thailand, *Vietnam*	12
2.07	*To **object to processing** on compelling legitimate grounds,*	Bhutan, *Brunei, China*, *Indonesia*, Hong Kong, Korea, Malaysia, Macau, Taiwan, Thailand, *Vietnam*	*11*
2.05	*Additional restrictions on some **sensitive processing** systems*	Hong Kong, India, Japan, Korea, Malaysia, Macau, *Pakistan, Sri Lanka*	*8*
2.06	*Limits on **automated decision-making***	*China*, *Indonesia*, Macau, Philippines, *Sri Lanka, Vietnam*	*6*
	TOTAL	Average over 17 countries is 7/10	*120*

66

3rd Gen. principles (GDPR & 108+) in Asian laws

3rd Gen. Principle	Asia (/12 laws as @0821)	TTL
Data breach notification to DPA for serious breaches	China, Korea, Philippines, Singapore, Thailand, Vietnam	6
DPAs to make decisions and issue administrative sanctions incl. fines	Japan, Korea, Singapore, Taiwan, Thailand	5
Data breach notification to data subjects (if high risk)	Taiwan, Philippines, Korea, Thailand, Indonesia	5
Representative actions before DPAs/courts by privacy NGOs	China, Korea, Philippines, Taiwan, Vietnam	5
Stronger right to erasure incl. 'to be forgotten' (RTBF)	Indonesia, Thailand, Japan, Korea	4
Stronger consent requirements incl. for children	Korea, Thailand	2
Biometric and genetic data require extra protections	Japan, Thailand	2
Right to data portability (UGC / other)	Philippines, Thailand	2
Mandatory Data Protection Officers (DPOs) for sensitive processing	Korea; Thailand	2
Direct liability for processors as well as controllers	Thailand	1
DPAs must cooperate with other DPAs in resolving int. complaints	Japan	1
Extra-territorial jurisdiction over local marketing or monitoring	Thailand	1
Local representatives for extra-territorial controllers or processors	Thailand	1
Maximum admin. fines based on annual turnover, global or local	Korea	1
Data protection by design and by default	–	0
Demonstrable accountability by controllers	–	0
Proportionality required in all aspects of processing	–	0
Data Protection Impact Assessments (DPIAs) for high risk processing	–	0
TOTAL	**Average / 12 countries = 3.2**	38

References

- My home page contains links to most of my papers http://www2.austlii.edu.au/~graham/
- More easily found on my SSRN page at http://ssrn.com/author=57970
- *Privacy Laws & Business* website has links to many Data Protection Authority home pages (please advise omissions) http://www.privacylaws.com/Links/