PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

Asian Data Privacy Laws – Additional countries (2019)

Professor Graham Greenleaf AM
Professor of Law & Information Systems,
University of New South Wales
Asia-Pacific Editor, *Privacy Laws & Business International Report*

30 October 2019, Linklaters, London

What standards are enacted globally? – 'OECD / basic' or 'European'?

1. Must first answer: 'what are *European* data privacy standards?'
2. Approach: What is required by the EU Directive but **not** required by the OECD Guidelines?
3. My 2011 study identified the **10 key differences** as 'European standards' (next slide)
    1. Examined 33/37 non-European laws (as at Dec. 2011) against these 10 criteria
    2. *On average, data privacy laws outside Europe included 6.9 of these principles, in addition to the minimum OECD principles*
4. Now 89 laws outside Europe (not 33) but no significant change to this distribution, globally, is apparent
5. Almost the same for 'top 20 by GDP' countries outside Europe (2017 study: 6/10)
6. Post GDPR (ie from mid-2018) GDPR influence is strengthening adoption of 2nd G standards and adding 3rd G elements –> the 'global standard' is strengthening

3rd G: New EU GDPR requirements (also included in Convention 108+)

1. **Proportionality** required in all aspects of processing;
2. **Stronger consent** requirements ('unambiguous' etc);
3. Greater **transparency** of processing;
4. Some **Mandatory Data Protection Impact Assessments (DPIAs)**;
5. **Limits on automated decision-making**, including the right to know processing logic (was also in EU Directive);
6. Data protection **by design and by default**;
7. **Biometric and genetic data** require extra protection;
8. Right to **object to processing** on legitimate grounds (also in Directive).
9. Direct **liability for processors** as well as controllers;
10. **Data breach notification** to DPA required for serious breaches;
11. DPAs to make decisions and issue **administrative sanctions**/remedies;
12. Demonstrable **accountability** required of data controllers
13. Parties must allow and assist evaluation of **effectiveness.**

3rd G: GDPR innovations not explicitly included in Convention 108+

14. obligations to apply **extra-territorially**, if goods or services offered, or behaviour monitored locally;
15. **local representation** required of such foreign controllers or processors;
16. right to **portability** of data-subject--generated content;
17. right to **erasure/de-linking** (right 'to be forgotten');
18. mandatory Data Protection Officers **(DPOs) for sensitive processing**;
19. data breach notification **(DBN) to data subjects** (if high risk);
20. **representative actions** before DPAs/courts by public interest privacy groups; and
21. maximum administrative **fines based on global annual turnover**;
22. requirement to **cooperate** in resolving complaints with international elements, with any other DPA (as distinct from 108+ members).

Some of these 9 may be implied by 108+.

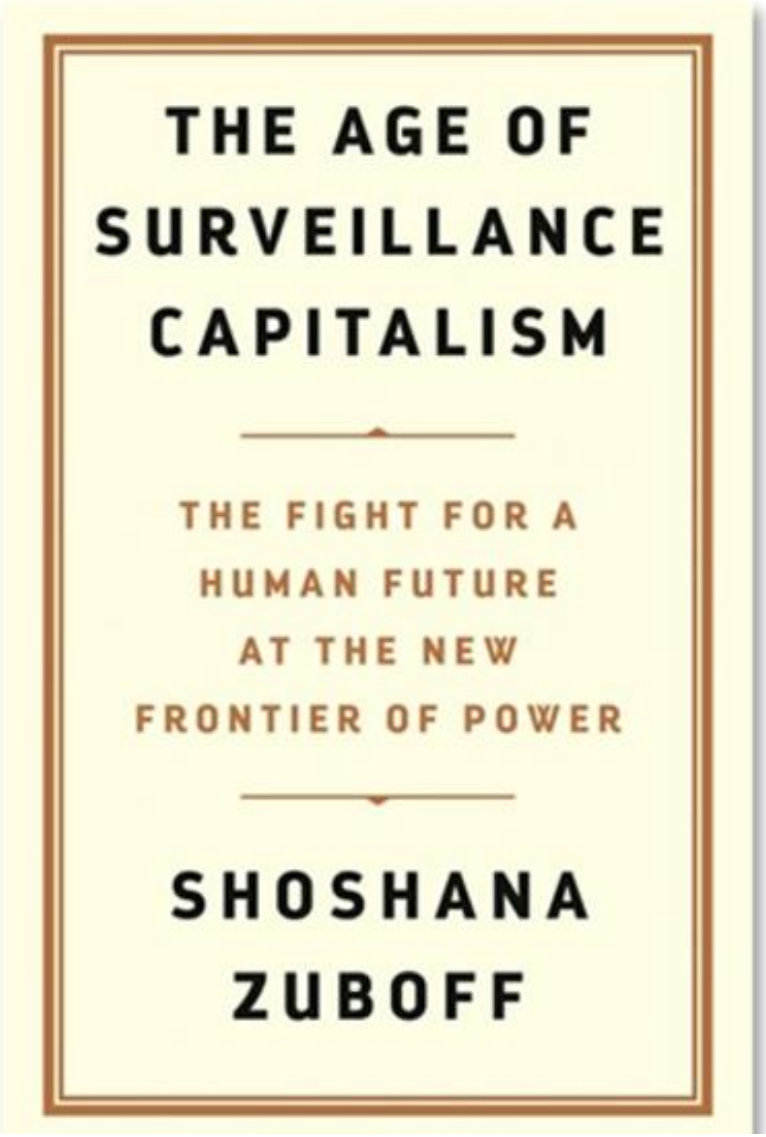
Early effects of the GDPR

Survey of **over 30 countries outside Europe**, shows these 'GDPR principles' enacted by **at least 10 countries**:

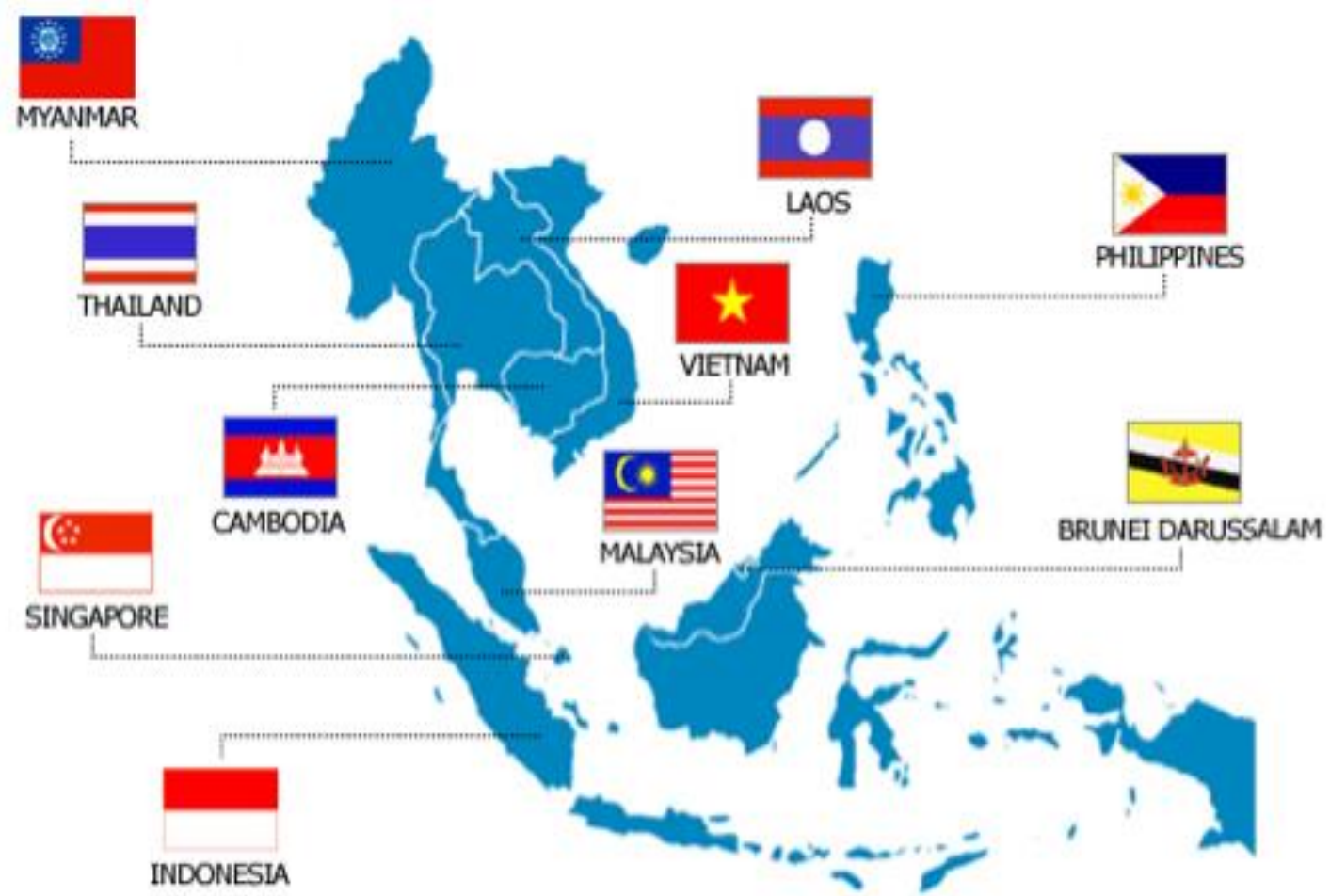
- *DPAs enabled to make binding decisions and issue administrative sanctions including fines;*
- *Right to object to processing based on controller or public interests;*
- *Data breach notification to DPA & to data subjects (+ US);*
- *Stronger consent requirements;*
- *'Sensitive data' to include biometrics and/or genetic data;*
- *Mandatory Data Protection Officers (DPOs) for some processing.*

All other new GDPR principles were adopted by 1-9 countries

Global surveillance context of data privacy laws



ASEAN – a growth area again



ASEAN & privacy commitments

- See 2019 Update pp. 23-24; 2017 Update, p. 9; 2018 Update pp. 10-15.
- *Context:* ASEAN could have become a major driver of privacy laws BUT
  - majority of 10 members are undemocratic or quasi-democratic;
  - privacy laws governing the public sector are unlikely (except Philippines, and – surprisingly – Thailand, probably Indonesia, perhaps eventually Malaysia)
- Of ASEAN's 10 members, 7 also in APEC (only 4 are not: Cambodia, Laos, Myanmar, candidate Timor-Leste); but APEC-CBPRs is not yet significant
- ASEAN *Human Rights Declaration* (Dec 2012)
  - First human rights instrument many ASEAN countries have entered; toothless
  - Similar terms to International Covenant on Civil and Political Rights (ICCPR)
  - A21: 'Every person has the right to be free from arbitrary interference with his or her privacy, family, home or correspondence including personal data'
- ASEAN Economic Community (AEC) established (2015)
  - Harmonised e-commerce framework includes in its targets adoption of best practice on 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
- Result: No regional data protection agreements of significance.

ASEAN overview: Renewed progress

- **Philippines**: Act (with DPA) 2012, finally in force in 2016
- **Malaysia:** Act (with DPA) 2010, in force 2013 – no enforcement
  - May change with new government
- **Singapore**: Act (with DPA) 2012, in force 2014 – with enforcement
- **Indonesia**: new Regulations 2013 and 2016 under IT law;
  - Draft new GDPR-influenced Bill released
- **Thailand**: new GDPR-influenced Act 2019 – most important change
- **Vietnam**: e-commerce & consumer laws, in force
  - Cybersecurity (data localisation) law 2018
- **Other countries:** No signs of Bills in other four members

Result?: *Progress rapid 2012-13; has now slowed but increasing again*

Only the Philippines & Thai Act covers the public sector – 'ASEAN way'

Reporting of cases in Singapore and Philippines
Indonesia's law, when enacted, will be a major development

Thailand

[ADPL Ch12 'Thailand – ASEAN's incomplete comprehensive laws']

- 2019 Update pp. 5-6
- *Context:* Unstable alternation between military regimes and democracy since WWII; Military and Bangkok elite coup 2014; military junta has announced plans for elections mid-2019.
- APEC and ASEAN member, not OECD
- 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
  - First strongly GDPR-influenced law in Asia

Thailand – PDPA 2019

- *Personal Data Protection Act* 2019
  - Explicitly aimed at high level of GDPR compatibility
  - In force 28 May 2020
- Main elements (2019 Update, p. 5):
  - Largely comprehensive coverage, but exemptions possible;
  - Principles have strong GDPR elements, but not all of them;
  - DPA, but complex structure and not independent; lack of appeal;
  - Data export/onward transfer rules are to be set by DPA;
  - Extra-territorial application similar to GDPR;
  - Modest administrative fines (US $100K max. – beats Japan!);
  - Right to obtain compensation from a court for breaches.
- EU adequacy will require negotiations & amendments
  - PDPC independence; finalised data export rules
  - Public sector access exceptions? (*Schrems* dangers)
- Result: Possibly better than other ASEAN laws, but it will depend a great deal on PDPC's enforcement and delegated rules.

Indonesia

[ADPL Ch 13 '…Indonesia – ASEAN's sectoral laws']; 2019 Update pp. 13-15

- *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 and WTO member
- 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
- Public Information Disclosure Law (2010) establishes a right of access (but not correction) to government files
- 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

- 2012 Regulation on Operation of Electronic Systems and Transactions A15
  - 2nd highest form of Indonesian legislation; Scope of 'Electronic Service Organisations' (ESO) may apply to both private and public sectors (unclear)..
  - Definition of 'personal data' is broad; unsure if excludes publicly available data,
- 2016 Ministerial Regulation on Personal Data Protection in Electronic Systems strengthens rules – see 2017 *Update* p.31, article by AA Rahmin
- Together, 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 rquired (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 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 p. 14 for details of other current requirements
- 'Reliability Certification Agencies' (A 68) could become relevant to APEC-CBPR

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

Indonesia – 2018 Bill

- Kominfo draft *Data Protection Bill* (April 2018)
  - There are different versions in circulation
  - Little likelihood of 2019 enactment; EU assistance provided
- Major elements of the Bill (2019 Update pp.13-15)
  - Comprehensive scope;
  - All basic principles + some GDPR-influenced (data breach notification; broad sensitive data categories; can request processing limitations; many GDPR principles absent, but uncertain how essential they are
  - Data export restrictions based on 'equal or higher' law of recipient country; White List by DPA; consent; and other grounds;
  - DPA (Commission) reporting to President, but with independence unclear;
  - Strong enforcement powers including supervising mediation (like Korea); compensation; administrative penalties up to US$2M; criminal offences
- Result: Would be one of the stronger Asian laws if enacted, but would require adequacy negotiations, particularly re DPA independence
  - Has to co-exist with localisation requirements, which EU does not favour

Vietnam

[ADPL Ch 13 ‘Vietnam … ASEAN’s sectoral laws’]; 2019 Update, pp. 20-21.

- *Context:* Still a one-party state, but since mid-1990s ASEAN membership has become a leading member, with a strong private sector. Structure of legal system similar to China.
- APEC and ASEAN member; not OECD; signatory to CPTPP.
  - First communist state with such extensive data privacy laws;
- A38 Civil Code, ‘Right to Privacy‘
  - Limited constitutonal 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 – 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
  - 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 – Data privacy laws (2)

- *Cyber-Information Security Law* (2016) - 2019 Update p.20.
  - 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 the Post and Telematics Ministry's 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 new Decrees
    - Decree 174 (effective Jan 2014) very specific on many breaches which will result in fines of around US1,000 at most
    - Decree 185 similarly detailed on offences by website operators

Vietnam – Localisation and exports

- Cybersecurity law (June 2018) – 2019 Update, pp. 20-21.
  - 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
  - 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)
- Other aspects
  - Foreign providers may need local representatives (but only if prior breaches of the law)
  - Providers must control (censor) postings by users
  - Authentication of users required
- **Bottom line:** Chinese-influenced approach to localisation etc, but not identical

[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 fully democratic for 1st time; 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 claims PDPA under review

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 (US$60K fine possible)
  - No remedies where breaches are unlikely to recur
  - Same defects as Hong Kong and pre-2011 UK laws (both now fixed)
  - 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

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

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 and ASEAN Member, not OECD nor APEC-CBPRs
- 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)

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; Strong influence of EU Directive throughout - except 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’
- 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)

Philippines – Enforcement

- National Privacy Commission (NPC) – an activist DPA
  - In existence since 2016, moved swiftly to finalise *Implementing Rules & Regs*.
  - 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 – dozens since 2017 (equivalent to case notes)
  - Commission-issued Orders – 3 in 2018 (primarily data security 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)
- Privacy Codes (NPC can approve or reject: consequences uncertain)

The other 5 ASEAN states

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

- Brunei – Nil significant
  - Public sector Privacy Policy (see Materials)
- Cambodia – Nil significant
- Laos – Nil significant
- Myanmar – Nil significant
- Timor Leste (candidate member)
  - Novel constitutional protection of personal data

Development of ASEAN Economic Community most likely to cause privacy law developments


AFGHANISTAN
PAKISTAN
NEPAL
BHUTAN
INDIA
BANGLADESH
MYANMAR
SRI LANKA
MALDIVES

South Asia

APEC's CBPRs

APEC-CBPRs has 2 participants

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

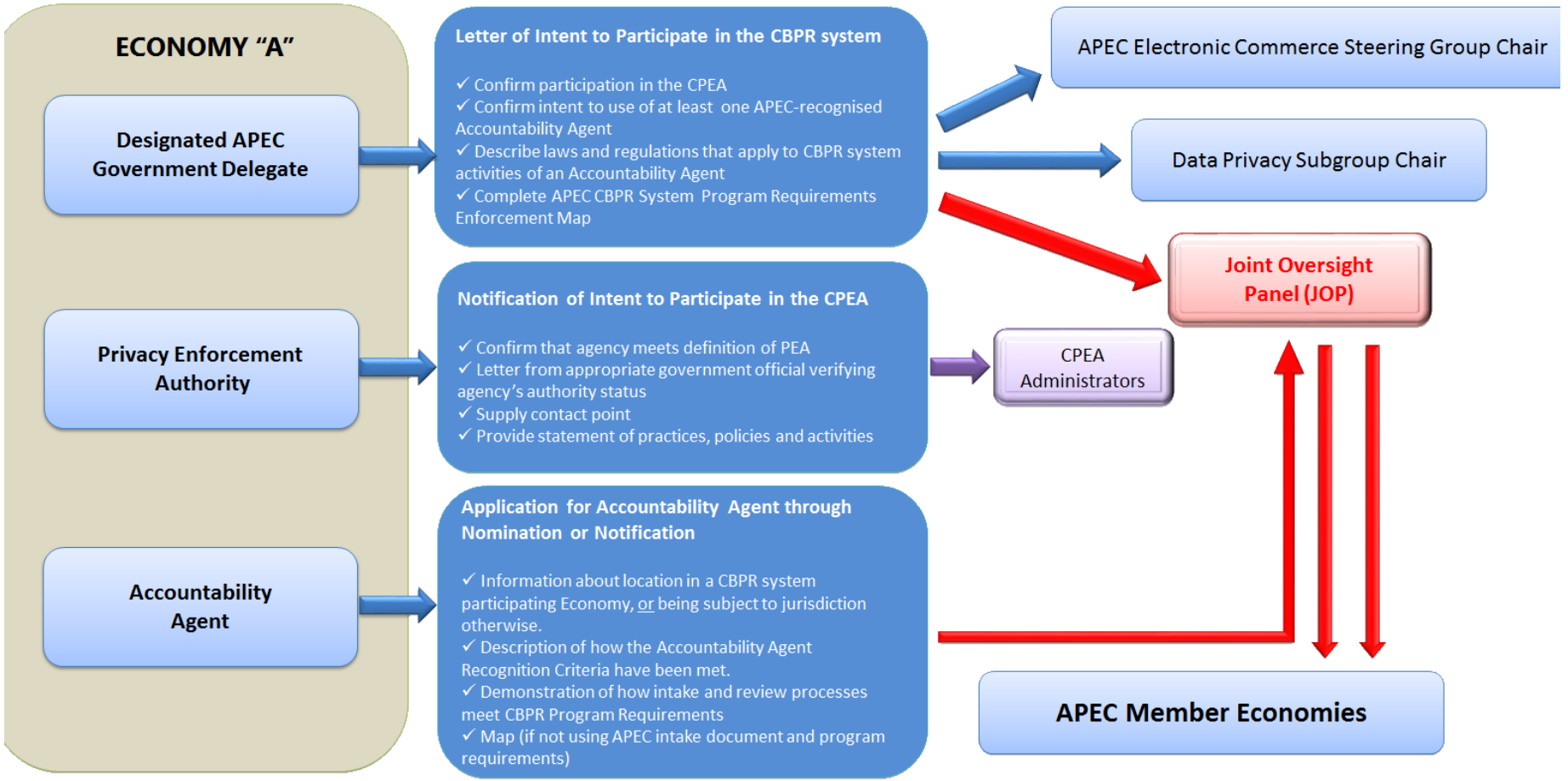
APEC Framework's 9 Privacy Principles

I Preventing Harm
II Notice
III Collection limitation
IV Uses of personal information
V Choice
VI Integrity of Personal Information
VII Security Safeguards
VIII Access and Correction
IX Accountability (includes due diligence in transfers)

The APEC Framework had a minor update in 2016, to make it consistent with the OECD Guidelines: No change to Principles, only data breach notification.

Generally 'OECD Lite', a slightly weaker version of the OECD Guidelines, plus principles I and V which add nothing of value, and IX which is a dangerous substitute for any real controls on data exports

Structure of the APEC Cross Border Privacy Rules (CBPR) system



See **Update** pp. 6-8; **Further Update** pp. 3-4

APEC's CBPR system (1)

APEC CBPRs in 13 steps [with comments]

APEC finalised its CBPR system in Sept 2011, endorsed by leaders (p531)

0. Economy expresses interest 'someday' *[Australia; Philippines; Vietnam]*

1.To participate in CBPRs, APEC economy must have laws which can be enforced to protect privacy consistent with APEC Framework

- CBPRs Joint Oversight Panel (JOP), from 3 economies, must report on application [*almost like self assessment, on examples so far*]

2.Economy has to have a Privacy Enforcement Authority (PEA) which participate in APEC's Cross-border Privacy Enforcement Arrangement *[Lots - separate]*

3.Economy has an 'APEC government delegate' to nominate the PEA & AA [*Mexico, Canada, Korea & Singapore have got to this stage*]

4.An Accountability Agent (AA) is nominated, and documents how it will meet the CBPR Program Requirements when it (i) assesses companies for certification; (ii) monitors compliance; and (iii) handles complaints

5.JOP reviews AA application to assess whether it meets criteria, and recommends appointment to APEC ECSG (no-objection approval). [*USA's nominee, TRUSTe, has been approved, despite numerous Civil Society claims of non-compliance; Japan's JIPDEC approved:* ***Update*** *pp 6-8*]

APEC's CBPR system (2)

6. Approved AA accepts applications for certification from *companies in its own jurisdiction only*; + only in relation to data 'subject to cross border transfer' (ie imported or to be exported) [***All APEC-CBPR certification is local; no such thing as 'APEC-wide' or even bi-lateral certification***]
7. AA 'verifies' company self-assessment of policy compliance (not public), collects fees, approves and monitors compliance ***[US TRUSTe has certified 19 companies, some with common ownership; Japan's JIPDEC certified 1 but it lapsed]***
8. CBPR certification does not alter company obligations to comply with laws of own country (or any other) – including data export restrictions **['*APEC compliance' is not an explicit basis for data exports anywhere yet, except Japan*]**
9. AA does not certify company's compliance with local laws, only APEC Framework **[*This is not a 'trustmark', it just looks like one*]**
10. AA is supposed to remove certification for breaches, and, if un-remedied, refer to local PEA [***No TRUSTe examples yet known***]
11. AAs are to release anonymised case notes of complaints ***[None]***
12. AA status must be renewed annually [***Civil Society submitted TRUSTe's AA status should be revoked for non-compliance – not sure if renewals continue***]
13. Company certifications, and payment of fees, periodically renewed **[*Many US companies already falsely purport to be CBPR-certified – USFTC fines $100K*]**

APEC's CBPR (3)

- What is the business case for APEC-CBPR certification? (ADPL p534)
  - Application process is onerous, involving 'registration' requirements Asia-Pacific laws avoid; fees are unknown
  - Multinationals would need multi-certifications
  - Benefits for companies in countries with privacy laws elusive
  - EU A29 C'tee has dismissed 'interoperability' with EU BCRs: partly common certification procedures is the best likely
  - **EU Commission has declared that 'Japanese back door' does not work**
  - TRUSTe AA case has reduced CBPR and JOP credibility; US $100K settlement for breaches (***Updat***e p8)
  - ***Can anyone identify a single concrete benefit of certification?***
- Factors favouring APEC CBPR
  - Japan's law (**Update** pp. 6-7) assists exports of Japanese data to US companies
  - Unknown if EU and APEC may still be exploring EU/APEC co-operation)
  - USA is willing to fund any country willing to develop CBPR

Conclusion: Business case for (non-US) companies is unknown; EU 'interoperability' is dead; viability of whole APEC CBPR is still uncertain