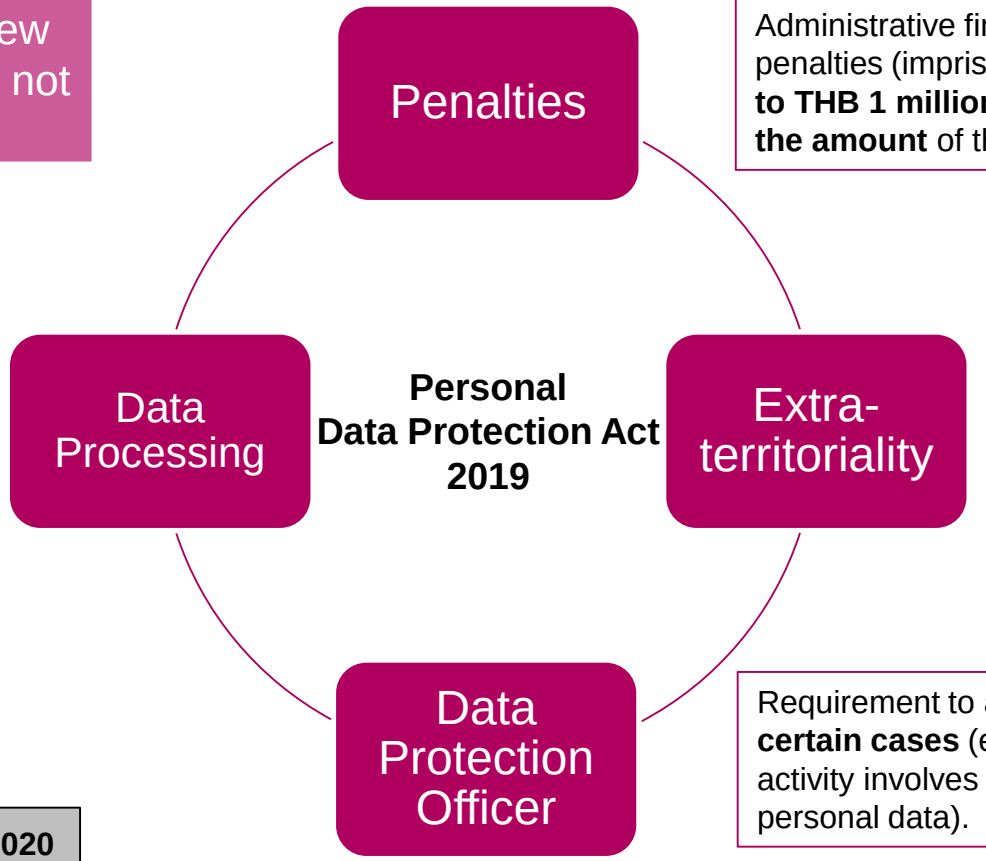
THAILAND

Thailand

Key element of the PDPA relies around **consent**, with only a few exceptions to where consent is not needed.



Administrative fines (**up to THB 5 million**), criminal penalties (imprisonment up to **one year** and/or fines **up to THB 1 million**), and punitive damages up to **twice the amount** of the actual damages.

Follows the **seven core** data protection **principles under GDPR**. However, **consent is the key** legal basis for processing personal data.

Even if entity is outside Thailand, where activities are related to offering goods and services to **individuals in Thailand**, the requirements of the Act will apply.

Requirement to appoint a **DPO in certain cases** (e.g. where main activity involves processing sensitive personal data).

operative provisions effective 27 May 2020

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; not in APEC-CBPRs
- 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 - Scope
  - In force 28 May 2020; see separate article in materials
  - Explicitly aimed at high level of GDPR compatibility
  - Only comprehensive ASEAN Act (other than Philippines)
  - Some exemptions, and others possible, with few controls
- Data exports and related matters:
  - Extra-territorial application similar to GDPR;
  - Data export/onward transfer to 'adequate' countries, but 'adequate' rules are to be set by PDPC;
  - A data processor bound by the PDPA but located outside Thailand must designate an in-country representative who has power to act in relation to all matters concerning personal data, and liability for failure to do so (s. 37(5))

Thailand – PDPA 2019 (2)

- Principles in PDPA have strong GDPR elements:
  - data minimization in collection (s. 22); strong consent requirements in relation to collection (ss. 23-25) perform a similar function to GDPR 'legitimate processing' restrictions; the right to data portability, subject to many limitations (s. 31); the right to object to processing (s. 32); right to request deletion, in terms similar to the GDPR and including the 'right to be forgotten' (s. 33); genetic and biometric data have been added to the categories of 'sensitive' personal data (s. 26); Appointment of data protection officers (DPOs), called 'personal data officers', is required (s. 41); Notification of data breaches to the PDPC within 72 hours, unless no risks, and to data subject if a breach raises high risks (s. 37(3))

Thailand – PDPA 2019 (3)

- GDPR aspects not included:
  - Defined grounds for legitimate processing; privacy by design and by default; protections re automated processing; 'demonstrable accountability', 'personal data impact assessments' (DPIAs)
- Enforcement
  - DPA, but complex structure and not independent; lack of appeals;
  - 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 stronger than other ASEAN laws,
  - will depend a great deal on PDPC's enforcement and delegated rules.