

The Baker McKenzie logo is displayed in white text on a red rectangular background. The background of the entire slide features a person's hands interacting with a laptop, overlaid with a complex digital network of glowing nodes and lines, suggesting data management and technology.

**Baker
McKenzie.**

Data Protection Laws: Issues involved in regulating data management

Siranya Rhuvattana

15 November 2018



Agenda

- 1 Regional Snapshot

- 2 Data Protection: Current Thai Laws

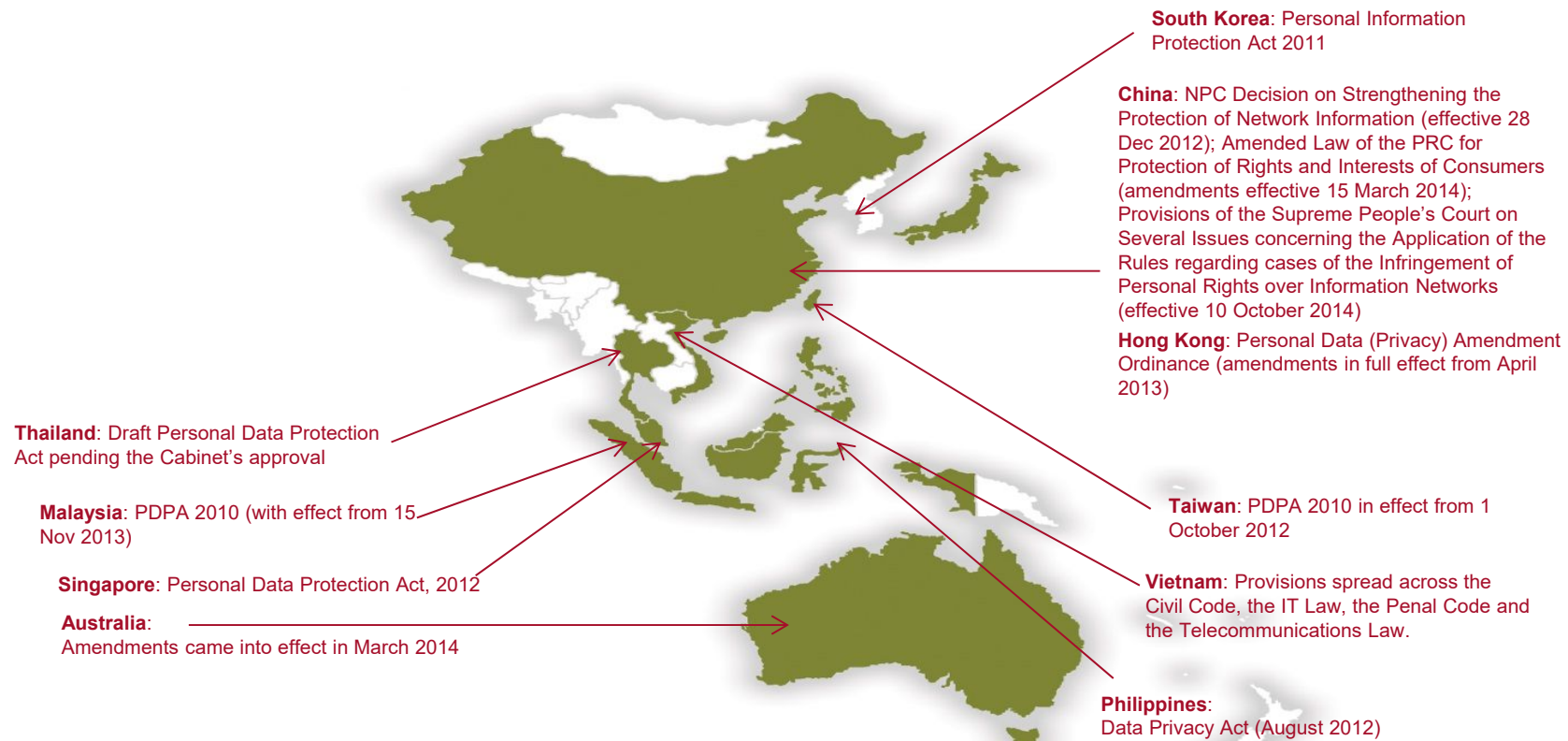
- 3 Draft Personal Data Protection Act (PDPA)

- 4 Key Issues

Regional Snapshot



Overview of data regulation in Asia Pacific



Regulations for Sensitive Data

- Distinction is made in some countries:
 - Malaysia and Australia, for example - Australia has comprehensive regulation of sensitive information and State Health Privacy legislation
- In some jurisdictions, health data would be considered “sensitive data” and subject to certain additional protections
- **No overarching definition of “sensitive data” in Thailand**



Data Protection: Current Thai Laws



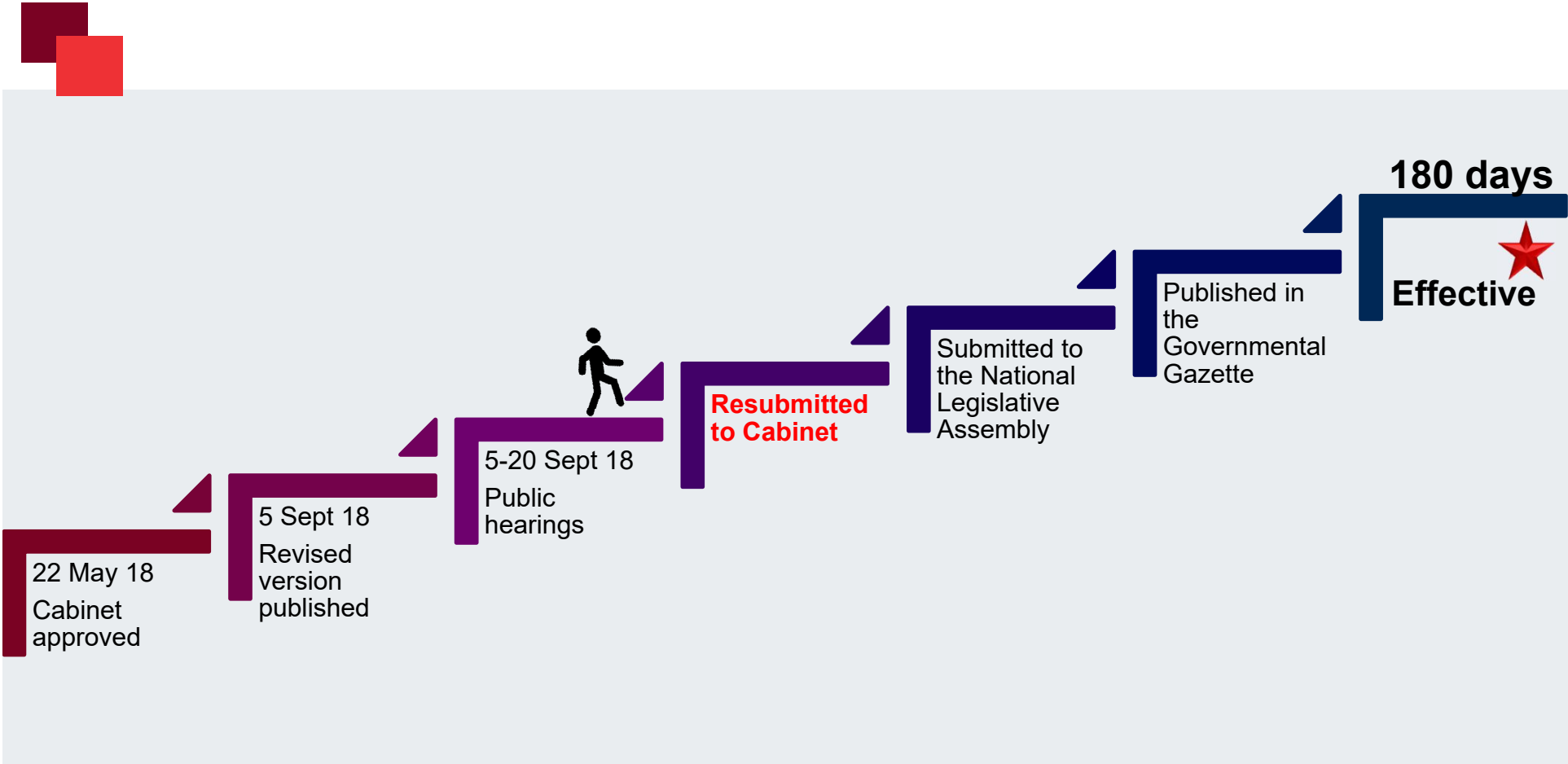
Data Protection: Current Thai Laws

- Currently – **no consolidated law**
- The Thai Constitution and **general tort law** apply
- Certain specific data protection laws target **particular business sectors**, e.g.
 - The Credit Bureau Act B.E. 2545 (2002)
 - The Notification of the National Telecommunications Commission Regarding Data Privacy B.E. 2549 (2006)
- Certain specific data protection laws target **particular types of data**, e.g.
 - The Child Protection Act B.E. 2546 (2003)
 - The National Health Act B.E. 2550 (2007)



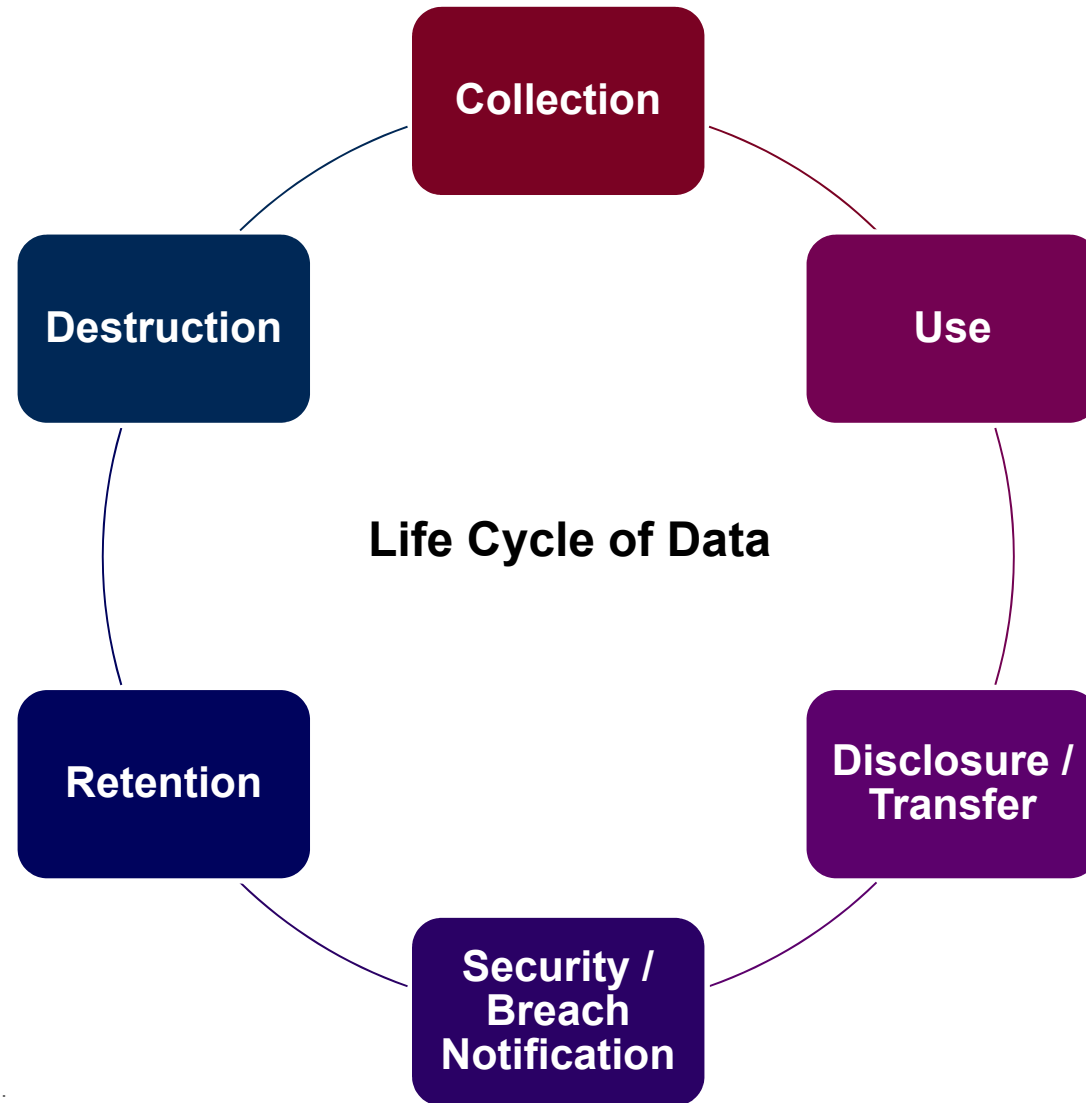
Draft Personal Data Protection Act (PDPA)





Status

The Draft Personal Data Protection Act



The Draft Personal Data Protection Act

Personal Data / Sensitive Personal Data

Extraterritorial applicability

Notice

Consent and legal exceptions

Rights of data subjects

Cross-border transfer

Sanctions

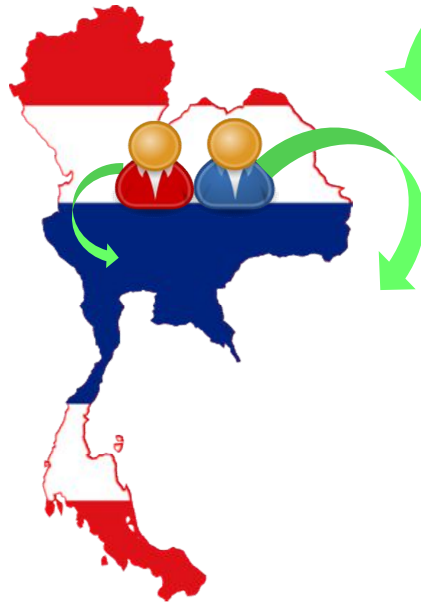
Key Issues



The Draft Personal Data Protection Act

Extraterritoriality: Compliance and data management issue

Data controller or processor
in Thailand



Data controller or processor
outside Thailand



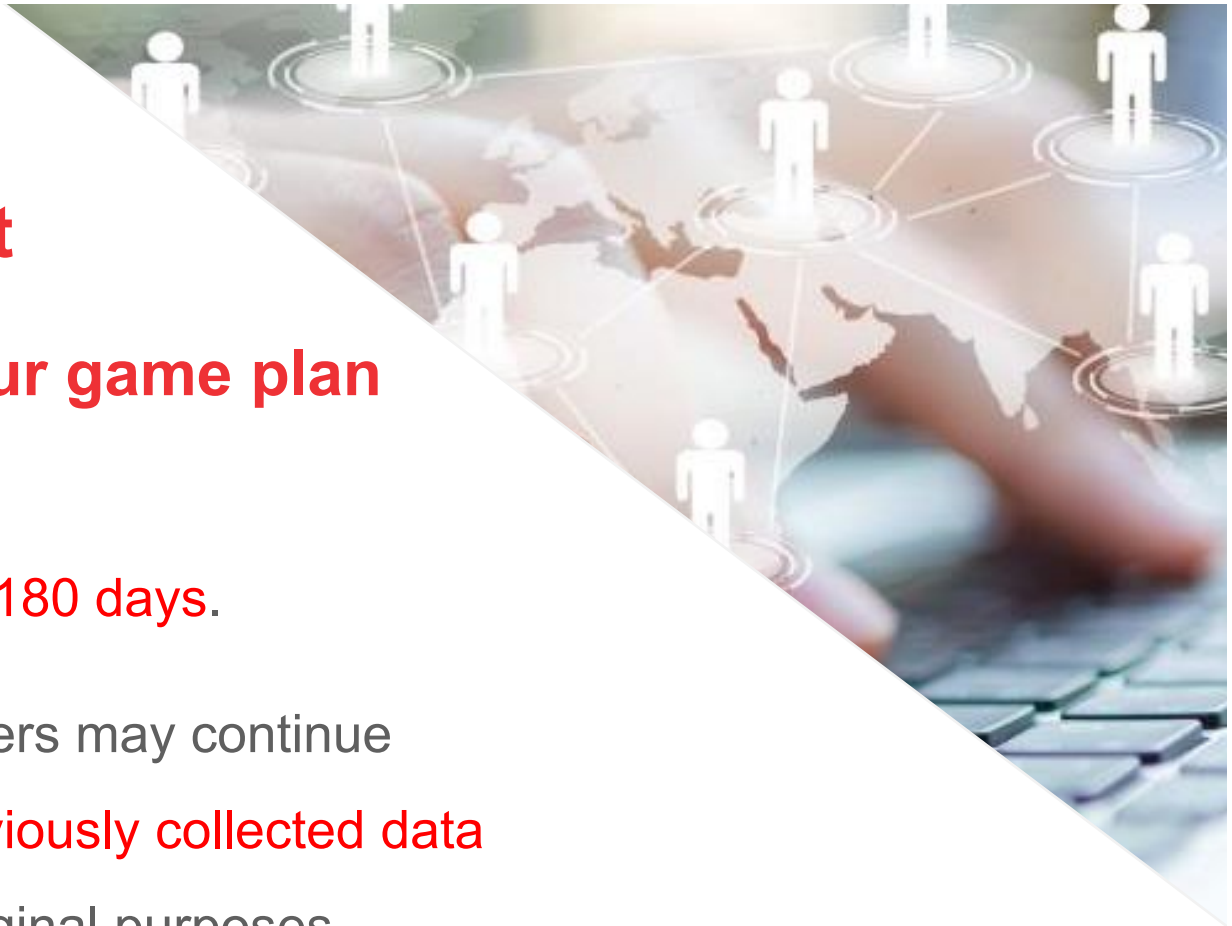
Collection, use, or disclosure of the personal data of data subjects **who are in Thailand**, regarding:

- ✓ **offering of goods or services** (irrespective of payment); or
- ✓ **monitoring** of their behaviour within Thailand.

The Draft Personal Data Protection Act

Transition period: your game plan

- A shorter transition period, from 1 year to **180 days**.
- Personal data controllers may continue to **collect** and **use previously collected data** in accordance with original purposes.
- Must provide and publicize a procedure to allow data subjects to easily revoke consent.
- **Cross-border transfer** and **disclosure** will be subject to the PDPA.



The Draft Personal Data Protection Act

Cross-border transfer issue

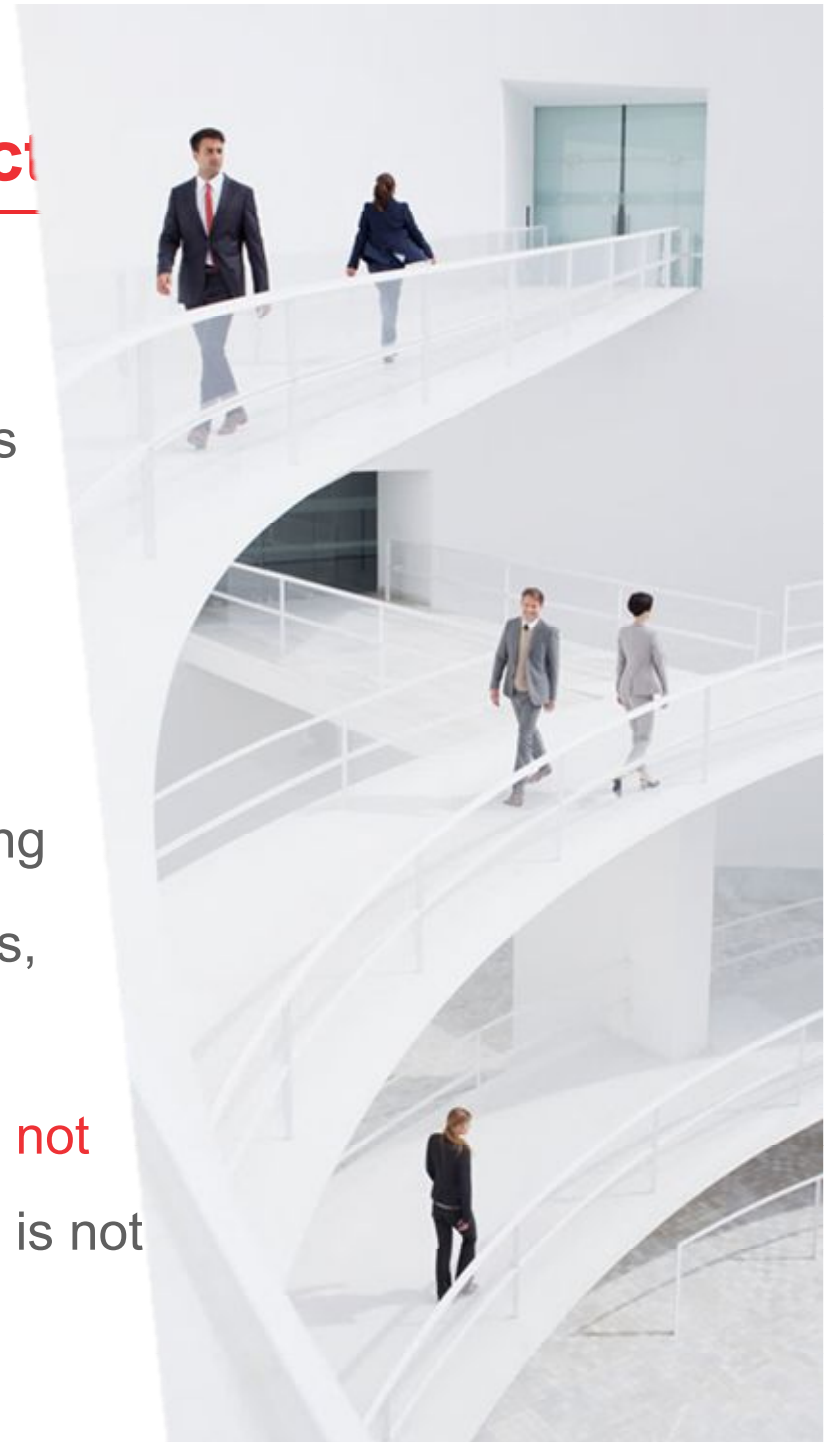
- Data controllers can only transfer personal data to countries
 1. that provide **sufficient personal data protection standards** and
 2. that are in compliance with a cross-border data transfer **guideline** to be later issued by the Data Protection Committee.
 - Unless certain exceptions apply
(e.g. consent, performance of contract)



The Draft Personal Data Protection Act

Consent requirements

- General rule – consent, unless exceptions apply
- Request for consent
 - **explicit**
 - objectives – not deceptive or misleading
 - in writing or through electronic systems, unless not possible by nature
- Consent not in compliance with the law is **not binding**, and collection, use, or disclosure is not allowed.



The Draft Personal Data Protection Act

Sensitive Personal Data



or *any other data as to be prescribed by the Data Protection Committee*

- Processing is **prohibited** unless explicit consent is obtained
- Narrow exceptions include:
 - necessary to prevent harm to life, body, or health
 - necessary to comply with laws for public interest in healthcare or labor protection
- Inappropriate processing subject to heavier criminal penalties

The Draft Personal Data Protection Act

Notification requirements

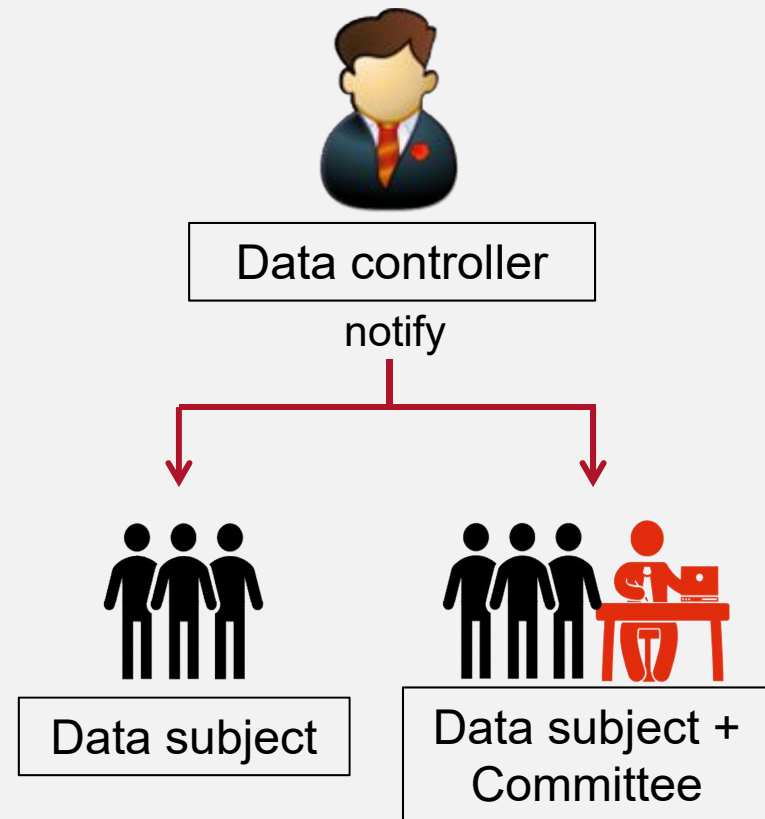
The personal data controller shall notify the data subject **before, or at the time of collection** about various items, e.g.

- the purposes of collection;
- **the personal data that will be collected** and the retention period;
- the types of persons or organizations to which the personal data may be disclosed;
- the information about the personal data controller, contact place, and methods;
- rights of the data subject



Data breach

- Data controller - notify **data subject** of the breach without delay.
- If the breach impacts a number of people exceeding that prescribed in the notification of the Committee, the breach and remedies therefor must be notified **to the Committee** without delay.
- Rules and procedures of the breach notification: to be later announced by the Committee.
- Violations can be subject to civil liability and administrative fines.



*** if exceeds the number of people prescribed*

Response to data breach

Do's

- ✓ Do understand legal requirements – who to notify?
- ✓ Do implement procedures for announcing data breach incidents, apologies, and practical remedies to the public - to calm public anxiety
- ✓ Do implement procedures to deal with accuracy of personal data, access/correction requests, and complaints
- ✓ Do implement procedures and processes to handle data subject's requests/complaints within an appropriate timeline
- ✓ Do implement plans/resources to deal with a large number of data subject's requests/complaints at the same time, especially if the data breach has affected data subjects on a large scale

**Baker
McKenzie.**

Key Takeaways



Key takeaways

- Conduct data mapping - 5Ws (who, what, where, when, why) and record your data processing activities
- Revisit privacy policy/terms and conditions regarding personal data
- Ensure processor/supplier contracts contain adequate provisions
- Prepare procedures to handle data subjects' requests when they exercise their rights
- Implement measures/procedures to detect and provide notice of data breaches
- Name a Data Protection Officer/responsible person within the organization to deal with data protection issues directly
- Check whether cross-border transfer practices meet the requirements under the PDPA
- Train employees on requirements under the PDPA



Q&A





Thank you

siranya.rhuvattana@bakermckenzie.com

Baker & McKenzie Limited
5th Floor and 21st–25th Floors, Abdulrahim Place
990 Rama IV Road, Bangkok 10500, Thailand
Tel: + 66 2 636 2000
Fax: + 66 2 636 2111
www.bakermckenzie.com

Baker & McKenzie Ltd. is a member firm of Baker & McKenzie International, a global law firm with member law firms around the world. In accordance with the common terminology used in professional service organizations, reference to a "partner" means a person who is a partner, or equivalent, in such a law firm. Similarly, reference to an "office" means an office of any such law firm. This may qualify as "Attorney Advertising" requiring notice in some jurisdictions. Prior results do not guarantee a similar outcome.

© 2018 Baker & McKenzie Ltd.

