Baker McKenzie.

PDPA PRINCIPLES, PLANNING AHEAD & PRACTICE FOR THAI UNIVERSITIES

Kritiyanee Buranatrevedhya, Partner
Certified Information Privacy Professional Europe (CIPP/E)
+66 2636 2000 ext 4592
Kritiyanee.Buranatrevedhya@bakermckenzie.com

Data Privacy & Protection

16 August 2021

TODAY'S AGENDA

1. THE NEW NORM
2. EXAMPLE OF DATA-RELATED ACTIVITIES
3. WHERE TO START ?
4. KEY CONSIDERATIONS
5. CASE STUDIES

Baker McKenzie.

THE NEW NORM

NEW WAY OF LEARNING:

- Hybrid Classroom
- Smart Campus

EXAMPLE OF DATA-RELATED ACTIVITIES

Relevant Data Subjects

- Candidates
- Students
- Parents (in case of minors)

- Lecturers
- Staffs
- Researchers

- Examinees / Outside Examiners
- Guest Speakers
- Tenants (e.g. canteen)
- Visitors
- Contestants (other organization's students)

University Application / Admission

Admitted and Enrolled

Other Areas to Consider

- Research conducted by the university
- University hospital
- Collaboration between universities
- Test centers
- Academic events and seminars
- Public Relations & course advertisements
- The use of biometric data (e.g., facial recognition and finger scan)
- CCTV / Parking lots

Lecturers & Assessments

- Attendance check
- Research & assignments
- Exam script & scores

Student Services

- Enrollment
- Scholarships
- Student document requests
- Nursing rooms

Library

- Library assess
- Book reservation & borrowing logs

Others

- Marketing activities
- Surveys
- University representations
- Student Council
- Sport events

Baker McKenzie.

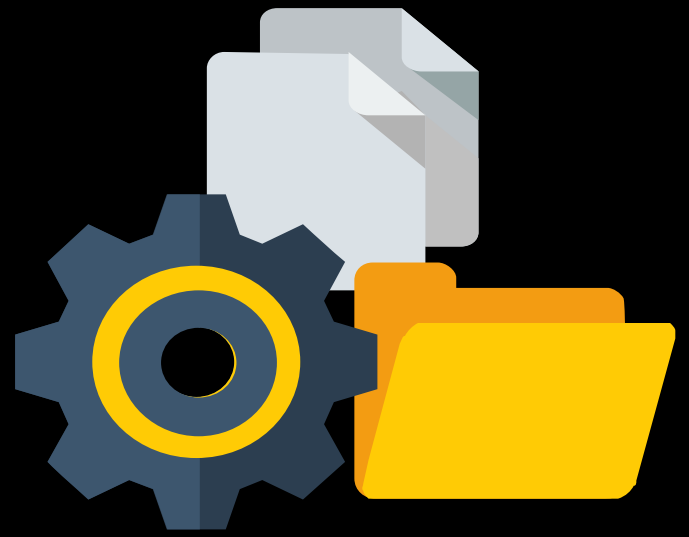
WHERE TO START ?

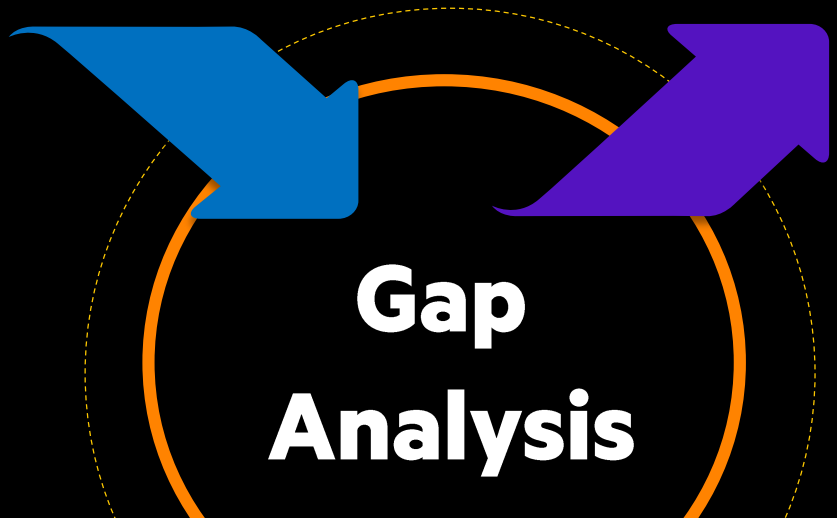
Recommended steps for PDPA compliance

Data Mapping:

5W (who what where when why) & 1H (how)

- Who do we collect personal data from?
- What personal data are collected, used, and disclosed?
- Where is the data collected and stored?
- When do we disclose personal data and to whom?
- Why do we collect these personal data?
- How long the data is kept?





KEY CONSIDERATIONS

Legal Bases

- Contractual Basis
- Legitimate Interest
- Legal Obligation
- Vital Interest
- Historical, research or statistics
- Public interest or official authority power
- Specific Bases for Sensitive Data

Example

The collection of necessary personal data in relation to the enrollment of a student could rely on the contractual basis.

Consent

- Method of requesting for consent
- When to obtain consent
- Parental consent
- Consent management

Elements of Consent

1. in writing or via electronic system
2. freely given
3. unconditional
4. clearly distinguishable
5. intelligible and easily accessible
6. clear and plain language
7. not deceptive or misleading
8. informed

Privacy Notice

- How many privacy notices to prepare?
- Method of notifying privacy notices
- Data collected from sources other than the data subjects

Example

Consider relying on the disproportionate effort exception?

Baker McKenzie.

KEY CONSIDERATIONS

Operational Procedure → Compliance Audit → Training and Awareness

Cross Border Transfer

- Appropriate legal mechanisms
- E.g. Exchange students / lecturers from partner universities abroad

Security Measures

- Administrative, technical, and physical measures
- E.g. Anonymization of personal data used for research

Personal Data Breach

- Notification to the authority and the data subjects
- Security Breach Reporting and Privacy Incident Response Procedure

Data Right Management

- 8 data subject rights
- Data Subject Rights Policy/Procedure

Data Storage

- Maintain RoPA
- Data Retention Policy and Procedure
- Off-Board / Erasure

Agreements / Legal Documents

- Roles of related parties as a data controller or data processor
- DPA (Insourced and Outsourced) & DTA
- Notice to Supplier
- Vendor due diligence checklist

Data Protection Officer

- Appoint appropriate persons
- Conflict of Interest?
- Data protection work flow within the university

Baker McKenzie.

CASE STUDIES FROM THE GDPR

Medical University of Silesia: fine of €5,500 (Approx. THB 246,000)

- **Violation:** Insufficient fulfilment of data breach notification obligations
- It was found that the university failed to notify the Polish data protection authority and the affected data subjects of a data breach relating to examinations conducted in the form of videoconferences on a special e-learning platform
- The breach occurred due to employee's failure to close access to the virtual room where the exam took place. Thus, the recordings of students were available to other people who had access to the system, and any third party could, by using a direct link, have access to the exam recordings and the data of the examined students presented during identification.

Cork University Maternity Hospital: fine of €65,000 (Approx. THB 2,580,000)

- **Violation:** Insufficient technical and organisational measures to ensure information security
- Personal data of 78 of its patients (6 of which are special category personal data) was discovered as improperly disposed of in a public recycling facility elsewhere in the county
- The case arose from a complaint was raised with the Irish Data Protection Commission (DPC) after a member of the public discovered the documents and brought the matter to the Health Service Executive's attention. The executive then reported the data breach to the DPC.

Anderstorp High School (Sweden): fine of €18,630 (Approx. THB 732,200)

- **Violation:** Insufficient legal basis for Sensitive Data / Purpose limitation and data minimization / Lack of DPIA
- The case concerned with the use of **biometrical data (i.e., facial recognition)** for a disproportionate purpose to keep track of attendance **even with consent**.
- There was **no data protection impact assessment** on risk and proportionality of data process to its purpose.

Baker McKenzie.

THANK YOU !

Baker McKenzie.