What is Thailand PDPA and How to Comply

IT Pattana

Mr.Sakul Tunboonek
IT Pattana Co.,Ltd

Certification#CV516492 PDPA Law for Practitioners
Chulalongkorn University Learning Innovation Center

What is Thailand PDPA

PDPA stands for Personal Data Protection Act.

The key principles and requirements of PDPA are based on Europe GDPR.

Thailand PDPA has been effective on July 1st, 2022

PDPA sets forth requirements for data controllers and data processors, including both public and private entities, on how to receive consent from data subjects before processing, collecting or disclosing

Understand PDPA high points

1. Territorial Scope

- Data Subjects refer to persons who stay in Thailand and makes no explicit reference to their nationality
- Data Controllers and Data Processors refer to persons or organizations both are located in Thailand or outside Thailand, regardless of whether the collection, use or disclosure of personal data takes place in Thailand or not

Understand PDPA high points

2. Understand Different between Personal Data and Sensitive Personal Data

- **Personal Data** refers to information relating to a person, which enables the identification of such person, whether directly or indirectly, but not including the information of deceased person

- **Sensitive Personal Data** include racial, ethnic origin, political opinions, cult, religious or philosophical beliefs, sexual behaviour, criminal records, health data, disability, trade union information, genetic data, biometric data, or of any data which may affect the data subject in the same manner

Understand PDPA high points

3. Does every company need to have a DPO (Data Protection Officer)

No, not every company need to have a DPO

But if your company has appointed PDPA team, then you should also

appoint a DPO

*The act has described characteristics of data and activities for those organizations that need to have DPO

Understand PDPA high points

4. Does PDPA specify the Security standard to protect the data

No, PDPA does not expressly provide for DPIA (Data Protection Impact Assessment)
However, PDPA requires the Data Controller to provide appropriate security measures and review them when it is necessary, or when the technology has changed in order to effectively maintain the appropriate security and safety standard

Understand PDPA high points

5. What is the PDPA penalty

PDPA enforcement outlines both criminal penalizes, non-criminal penalties, and also administrative penalties

- The maximum fine is not exceeding THB 5 million baht
- The maximum imprisonment for a term not exceeding 1 year

FAQ : Data Classification

Q: Does video from CCTV a personal data ? And if it is how should we take care of it ?

A: Yes, video from CCTV is personal data. We need to evaluate the legal basis for recording the video, normally based on legitimate Interest. Data Controller need to post a Privacy Notice at the CCTV

Q: Does the faces CCTV records the sensitive data ?

A: No, normally faces in CCTV records is not sensitive data.

However, it the Data Controller use a technology such as face recognition to identify the faces, or to identify from person behavior then that data is considered sensitive data.

FAQ :

Q: Company A requires a copy of Company B's Board Citizen ID for the partner contract. Does Company A need to request for a Consent ?

A: No need for consent because Company A's request is based on "contractual basis"

Q: Does HR data the sensitive personal data ?

A: Yes, and No.

Please be careful in classify sensitive data. The Act defines "races", "heath information", " religious", "political belief", etc to be sensitive data.

FAQ :

Q: Can a company take the visitor photo before allowing the visitor entry?

A: Yes, the company can refer to its 'legitimate interest' in order to provide safeguard to its Company and employees. However, the company will be held responsible as the 'Data Controller' in protecting the visitor sensitive data (picture is considered sensitive data)

Q: A company has to send its employee personal data to its HQ in another country for a business purpose. Does the company need to ask for employee consent every time?

A: No need to ask for consent every time. However, the consent should state the business need in order to send the personal data regularly and how long it needs to send the data

FAQ :

Q: Are Staff fingerprints in Time Attendance system sensitive data ?

A: Yes, fingerprints are sensitive data. The company will need to ask for consents from its staffs.

Q: Can staffs be ‘Data Controller’ or a ‘Data Processor’ ?

A: No. Staffs are Company’s employees.
Staffs cannot be ‘Data Controller’ or a ‘Data Processor’

FAQ :

Q: What are penalties for Staffs who are responsible for taking care of personal data?

A: There is no penalty for staffs according to this PDPA. However, if the staffs are irresponsible to their job description. The company can consider penalty according to the employment contract.

Q: What are penalties for DPO (Data Protection Officer) ?

A: There is no penalty for DPO according to this PDPA. However, if the DPO is irresponsible to their job description. The company can consider penalty according to the employment contract.