AN INTRODUCTION TO THE PERSONAL DATA PROTECTION ACT, B.E. 2562 (PDPA)

Phiraporn Nakeiam

R.W.T INTERNATIONAL LAW OFFICE

RWT
INTERNATIONAL LAW OFFICE

An introduction to the Personal Data Protection Act, B.E. 2562 (PDPA)

In Thailand, the Personal Data Protection Act (PDPA) is a critical and relevant law that has basically gone unnoticed although it directly or indirectly is part of everyone's life here in Thailand. This includes an individual's personal data along with all businesses from a small startup all the way up to the largest companies due to various hacks and data leaks which continue to pose a serious problem both here in Thailand and Globally.

Currently, most people are interested in and consider PDPA vital because of the rise of digital technology or online platforms that consumers frequently and openly share personal data to register on these online platforms as well as phone apps before gaining access to them. At this point, personal data is a valuable resource for numerous reasons and that are sold because of it. Due to the reasons listed above, the enforcement of the PDPA Act should be used to protect and address these concerns.

What is the PDPA?

The PDPA, or Personal Data Protection Act, protects individuals from the unauthorized disclosure or misuse of their personal data, including instances where personal data is collected or used without the owner's informed consent.

Additionally, this Act applies to the collection, use, or sharing of Personal Data by anyone who controls or processes data in Thailand including for personal data controllers or evaluators located "Outside Thailand" who sell products or services to people in Thailand or monitor their behavior within Thailand, the rules still apply.

Who must comply with the PDPA Act?

- Data subject

The data owner, also known as the Data Subject, refers to the individual associated with a specific set of personal data that can be linked back to their identity. Essentially, this pertains to us. According to the PDPA (Personal Data Protection Act), the data owner is entitled to protection and various rights concerning their personal data.

- Data Controller

A Data Controller is a person or company with the authority and responsibility to decide how to collect, use, or share personal data. When dealing with personal data, the Data Controller usually needs to get permission from the person the data belongs to unless there are exceptional circumstances where consent is not needed, but these need careful consideration.

The Data Controller must also let the person know why their data is being collected before or when, but only to the extent necessary. They should not use or share personal data without the person's permission unless there is a specific situation where consent is not required.

- Data Processor

A Data Processor is someone or an entity tasked with handling personal data based on instructions from a Data Controller without making independent decisions on data processing. For instance, messenger platforms that handle personal data to deliver messages operate as Data Processors on behalf of users. Similarly, when companies utilize cloud services and the service provider stores data for them, the service provider acts as a Data Processor.

- The Rights of Data Subjects Under the PDPA:
- The Right to be informed: You must know how your data is collected and used.
- The Right of Access: You can request and obtain your data within 30 days.
- The Right to rectification: Your data must be accurate and updated promptly.
- The Right to erasure: You can request data deletion under certain conditions.
- The Right to restrict processing: You can limit data usage in specific cases.
- The Right to data portability: You can receive your data in an accessible format.
- The Right to object: You can object to data usage in certain situations.
- The Right to complain: You can complain to the Expert Committee.

In the case of minors, before any legal action or approval for data to be obtained, the collector of data would first need consent in order to collect and maintain use of the data:

- Ages 0 to under 10: Parental consent is always required.

- Ages 10 to under 20: Parental consent is needed if the minor isn't able to give consent themselves.

The (6) Exceptions to the PDPA:

Collection, use, or disclosure of personal information by individuals for personal gain or within their family is exempt.

Government agencies can handle personal data for purposes such as maintaining national security, fiscal stability, public safety, and combating money laundering and cyber threats.

Individuals or organizations involved in media, arts, or literature can use personal data if it adheres to ethical standards or benefits the public interest.

The House of Representatives, the Senate, and the National Assembly, along with their appointed committees, can collect, use, or disclose personal information as part of their official duties and powers.

Courts and officials involved in legal proceedings, including property management and criminal justice operations, have exemptions regarding personal data handling.

Credit information companies and their members are allowed to process personal data in accordance with the laws governing credit information businesses.

Penalty

The Personal Data Protection Act (PDPA) allows authorities to fine those who break the rules. The fines can be significant, dependent upon how severe the violation may be in each instance. If it is a minor breach, companies may be defined as a percentage of their yearly earnings up to a specific limit. However, they may face daily fines for more severe offenses until the breach has been found to be compliant.

In addition to fines, there are also criminal penalties in place. People who are found to intentionally misuse personal data could go to jail for up to a year and/or include fines. Moreover, those who ignore the orders of the Personal Data Protection Committee could face the same punishment.

If the rights of a person(s) are violated under the PDPA, they can seek reparations in the form of compensation for any harm they have suffered. This could include the filing of personal injury in the form of financial losses or emotional distress caused by their data being mishandled. Courts can decide how much compensation is fair in each case.

These penalties have been put in place to make sure everyone takes data protection seriously. Organizations must follow the rules to avoid hefty fines and damage to their reputation. They should implement robust measures to protect data and train their staff. Moreover, individuals should know their rights and take steps to keep their data safe.

Case Example: The Facebook-Cambridge Analytica scandal

This case involved the unauthorized access and misuse of personal data from millions of Facebook users for political purposes. Cambridge Analytica, a political consulting firm, obtained this data through a third-party app that collected information from users who installed it and their Facebook friends without their explicit consent.

This scandal highlighted the significance of data protection and privacy regulations like the Personal Data Protection Act (PDPA). Even though the scandal primarily unfolded on the Facebook platform and involved users from various countries, including the United States and the United Kingdom, the PDPA principles are relevant.

Under the PDPA, organizations that handle personal data must obtain consent before collecting, using, or disclosing personal information. They must also ensure that personal data is securely stored and used only for legitimate purposes. In the case of the Facebook-Cambridge Analytica scandal, the unauthorized access and exploitation of personal data would likely constitute a severe violation of the PDPA if similar circumstances occurred within a jurisdiction governed by such regulations.

Additionally, the scandal emphasized the importance of transparency and accountability in data processing practices. Organizations must inform individuals about how their data will be used and provide mechanisms for individuals to exercise their rights, such as the right to access their data or request its deletion.

In summary, while the Facebook-Cambridge Analytica scandal did not directly involve the PDPA, it underscored the critical need for robust data protection laws and enforcement mechanisms to safeguard individuals' privacy rights and prevent unauthorized access and misuse of personal data.