



Privacy law in Thailand

Personal Data Protection Act BE 2562 (2019)





PwC contacts



Vunnipa Ruamrangsri
Legal Services Partner
Tel: +66 (0) 2844 1284
vunnipa.ruamrangsri@pwc.com



Chanvit Prachayapipat
Legal Services Director
Tel: +66 (0) 2844 2075
chanvit.prachayapipat@pwc.com

Thailand's Personal Data Protection Act (PDPA) came into effect on 1 June 2022. The PDPA aims to monitor and control the use of personal data.

No matter where the company is established, all business operators who collect, use, process and disclose personal data of data subjects in Thailand can be considered data controllers or data processors and must comply with the PDPA.

So to avoid potential risks associated with any personal data leakage, it's crucial for companies and organisations to prepare themselves for legal compliance in their day-to-day business operations. The PDPA's fundamental principles are quite similar to those of the EU General Data Protection Regulation (GDPR), but there are some differences between them. For example, under the PDPA, a non-compliance could give rise to a criminal offence punishable by imprisonment for up to one year and/or a fine up to THB5m for each transaction of complaint. Also, if the juristic person's violation is conducted by a director, manager or other responsible staff, such person will be subjected to the same penalties.

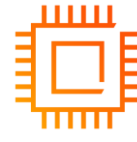
Under the PDPA, the following four main parties have different rights, roles, obligations and liabilities.



Data subject



Data controller



Data processor



Regulators

Business operators will be considered the data controller if they have the power and duties to make decisions regarding the processing activity (e.g. collection, use, disclosure) of the personal data.

As a result, that business owner would need to look carefully at these key elements of compliance.

Identifying lawful basis – the data controller must have a lawful basis for each personal data processing activity. Data subject rights management – the data controller must fulfil the data subjects' requests to exercise of their rights under the PDPA and relevant regulations, e.g. the rights to access, rectify, erase, restrict or object to the processing of personal data. Data breach incident management – in case a data breach occurs, the data controller should have proper procedures and documentation prepared, e.g. policy and procedures, data breach severity assessment forms and data breach notifications, because it may have to notify the authority within 72 hours after having become aware of the incident. Cross-border transfer – unless the transfer falls under an exemption, the data controller can't transfer personal data to any country with inadequate personal data protection or data protection standards as regulated by the regulators. Implementing the required actions and documents – as the data controller must notify data subjects or regulators or obtain consents, it must properly prepare its data processing records and ensure that they contain information such as the data processing activities, procedures and protection measures.



How does PwC help you prepare for PDPA enforcement?

Benefits for you:

Personal data leakage prevention and help in ensuring compliance with all of the PDPA's requirements, including preparing the necessary documents and data processing records

Raised awareness and knowledge of personal data privacy among your management and staff members at all levels in order to maintain the organisation's compliance levels

Advisory

We provide legal advice and explain the PDPA requirements.

Documentation

- We draft and develop templates for legally required documents, such as the privacy policy and notice, consent letter and breach notification form.
- We review agreements related to personal data and make the appropriate revisions.
- We localise the organisation's global privacy policy and documentation and ensure that all local requirements are reflected in them.

PDPA gap analysis

To assess potential legal risks under the PDPA, we conduct a gap analysis through a legal review of your provided information and documents along with interviews with selected stakeholders of each related division, and we give recommendations or advice.

To fill gaps and prevent penalties, we prepare the legally required data inventory and help you to understand data workflow mapping.

After the implementation, we can also conduct a PDPA compliance review to revisit and check whether your current practices are still in line with the PDPA and its subordinate legislations.

PDPA training

We use gap analysis assessments to create a framework to help your employees comply with the PDPA. We design PDPA training courses and conduct trainings to build your employees' understanding of the legal requirements and potential risks of personal data leakage.