

Is Your Company Ready for Thailand's PDPA Enforcement in June 2021? Learn more about what it is, and tips on getting started.

After a lengthy process of drafting, consulting the public, and revising, Thailand is finally set to enact their own Personal Data Protection Act (PDPA). Much like the raft of other new data laws which have come along in the past two years, this one takes many of its cues directly from GDPR. Despite disruptions from the COVID-19 pandemic, the PDPA will enter law on **27th May 2021**.



On its face, this is good news for many businesses as the similarities between the GDPR and PDPA mean that a number of the processes, policies, and procedures they already have in place for GDPR can prove equally as sufficient for PDPA. Even so, in much the same way that business owners were left confused in the run-up to GDPR, PDPA's arrival has left many with some serious questions about what exactly Thailand's new data protection law means for them and their companies.

Before we take a look at the key points addressed in the PDPA, let's explore the definitions of the key terminology used:

Data Subject – refers to any individual person who can be identified, directly or indirectly, via an identifier such as a name, an ID number, location data, or via factors specific to the person's physical, physiological, genetic, mental, economic, cultural or social identity. In other words, a data subject is an end user whose personal data can be collected.

Personal Data – refers to any information relating to a "Data Subject" an identifier, such as a name, an identification number, location data, an online identifier, or to one or more factors specific to his or her physical, physiological, genetic, mental, economic, cultural or social identity.

Consent – consent means any freely given specific, informed and explicit indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to "Personal data" relating to them being processed.

Data Controller – The PDPA identifies a data controller as the authority that determines the means and purpose of collecting, using, and sharing personal data.

Data Processor – According to the PDPA, a data processor is any individual or party that gathers, uses, or shares personal information as directed by the data controller.

Key Points of the PDPA

We have identified 4 key points in the PDPA which all businesses should be aware of, and elaborated below:

1. Rights of the Data Subject

As previously mentioned, the PDPA is dedicated on protecting Data Subjects from the illegal or unconsented collection, use, or disclosure of personal data. Therefore, there are clear rights of Data Subjects that have been outlined in the PDPA including:

- The right to be informed
- The right to access
- The right to data portability
- The right to object
- The right to erasure/right to be forgotten
- The right to restrict processing
- The right to rectify

What this means for businesses is that our customers, usually “Data Subjects” will have the right to be informed, access, object, restrict, rectify, and erasure of their personal data at will. This may cause extreme disruptions to businesses that are not fully prepared.

2. Responsibilities of the Data Controllers and Processors

According to the PDPA, both Data Controllers and Processors must carry out their duty of data collection and control that fully always complies with the laws and regulations and must operate within the scope of the consent/purpose given by each Data Subject. Data Controllers and Processors must also notify Data Subjects before collection of Personal Data regarding why and how their data will be used. Data Controllers and Processors must have access to requested Personal Data at all times.

3. Importance of Consent

Under Thailand’s new PDPA laws, data controllers and processors must seek the data owners’ consent in good faith and in an honest manner. Under the same laws, data subjects can revoke consent at any time, applicable to current Thailand laws and other agreements, of course – however, this revocation has no bearing on any data collection, usage or disclosure which the data owner previously legally consented to. Data controllers are also obliged to ensuring that the appropriate security measures are put in place in order to guard against any data loss or modification. In addition, they must ensure that the data used or disclosed (with consent) is completely accurate, complete and up to date.

4. Data Protection Policies, Procedures, and Notices

The PDPA requires the Controller to notify each data subject of the purpose of any collection, use or disclosure of personal data prior to or at the time of data collection so that the data subject is made aware of how his/her personal data will be used and the purpose it will serve. The notice must contain at least the intended purpose of data collection, the retention periods, the consequences of not



providing data, the types of data to be collected, the rights of data subjects, and information about the Data Controller. Data protection systems and measures must be in place to secure Personal Data collected.

Tips to get started

At time of writing, there is less than 4 months remaining before the PDPA will be enforced and all organizations would need to comply with this regulation. We here at VinarcoFormiti would like to stress the importance that businesses start to begin assessing their data processing activities to identify what operational processes that would need amendment, then begin planning on how each process should be changed and/or added. Please see below how we recommend our clients to kick-start their PDPA compliance project:

- Conducting a gap assessment to identify the current level of compliance, key gaps, and where to focus initial efforts
- Conduct organizational Data mapping and Data flow diagram to understand how your company collects, processes, transmits, and stores data, which includes identifying the legal basis to collect and use personal data
- Reviewing internal policies, agreements, and practices related to Personal Data
- Updating existing privacy notices and creating relevant legal documents
- Raise awareness of all employees and ensure that they are fully trained on the relevant requirements of the PDPA in their scope of work

To learn more about the PDPA and how we could support you in your journey to PDPA Compliance, please visit our website: www.vinarcoformiti.com or email vichapat.p@vinarco.com

Name: Vichapat Piyaratn

Position: Director - Operations

Company: VinarcoFormiti

Mini Bio: Vichapat has over 8 years' experience in Human Resource Organizational Development (HROD) field. He is currently working for the Vinarco Group of companies continuously improving internal operating standards, in addition to offering a wide range of HR Solutions/Consultancy and Corporate Compliance to clients.

Website: www.vinarcoformiti.com

Photo of the author:

