Deloitte.
Legal

PDPA Alert
25 August 2021

Personal Data Protection Act: Be ready for its full enforcement

DATA PROTECTION OFFICERS (DPOs) – WHO ARE THEY?

Prior to the full enforcement of the Personal Data Protection Act B.E. 2560 ("**PDPA**") in 1 June 2022, all business operators are encouraged to be ready and well-prepared to comply with all PDPA requirements and to enhance the awareness of PDPA within the organizations.

A Data Protection Officer ("**DPO**") plays one of the significant roles in helping organization during the PDPA implementation to drive the organization towards compliance.

A DPO is a new position established under the PDPA as the person responsible in helping the organization in ensuring that the data subjects' personal data is processed in the most consistent manner and feasible with the PDPA requirements as well as being a contact point for PDPA issues with authority and the data subjects. The roles and responsibilities of a DPO has been specified in the PDPA, and there is a possibility that more details regarding the DPO may be issued through other notifications by the Personal Data Protection Committee ("**PDPC**").

Experience the future of law today.

WHAT ARE THEIR ROLES AND RESPONSIBILITIES?

According to Section 42 of the PDPA, the roles and responsibilities of a DPO are as follows: -

(1) To provide recommendations regarding the PDPA requirements to the data controller or the data processor, as well as its employees or service providers;
(2) To monitor the performance of the data controller or the data processor, as well as its employees or service providers, with respect to the processing of the personal data to be in accordance with the PDPA requirements;
(3) To coordinate and cooperate with the PDPC in the circumstance when there are obstacles regarding the procession of the personal data undertaken by the data controller or the data processor, as well as its employees or service providers, under the PDPA requirements; and
(4) To keep confidentiality of the personal data known or acquired while performing his/her duties as a DPO.

From the above, the DPO will not be personally liable for any liability that may arise during the processing of personal data, except in the case where the DPO unlawfully discloses the personal data obtained during the course of his/her duties. Therefore, the data controller and data processor must provide the DPO with appropriate support. Such support may include, but is not limited to, providing appropriate tools or equipment, granting authority to directly report any PDPA breach or any circumstance which may potentially lead to the breach to the chief executive of the organizations, and facilitating access to personal data. Resources, either personnel-wise and financial-wise, should be properly considered.

Additionally, the organizations must maintain the independence of DPO, and dismissal or termination of the DPO's employment (if the DPO is the existing employee appointed) as he/she has performed his/her duties under the PDPA is prohibited.

DO ALL ORGANIZATIONS MUST HAVE A DPO?

Some people may believe that all enterprises must have the DPOs in order to legally process personal data under the PDPA, and some may believe that the DPO's designation is solely determined by the size of the organization. Pursuant to Section 41 of the PDPA, the data controller and the data processor shall designate a DPO in the following circumstances: -

(1) The data controller or the data processor is a public authority;
(2) The activities of the data controller or the data processor in processing personal data require a regular monitoring of personal data or system due to a large scale of personal data being processed; or
(3) The core activity of the data controller or the data processor is processing of sensitive personal data.

Furthermore, it is expected that the sub-law regarding the DPO would refer "large scale" to: -

- Holding certain numbers of personal data during a one year period;
- Holding certain numbers of sensitive personal data during a one year period;
- Having certain numbers of its personnel responsible in processing of personal data; or
- Having certain numbers of its branches or locations to process the personal data.

We can see that the PDPA does not require all organizations to have DPOs; rather, the data controller and the data processor must identify the volume of personal data (and sensitive personal data) being processed, the number of related data subjects, the period of processing personal data, and the resources and locations used for processing personal data in determining whether a DPO is required or not. However, all stakeholders should monitor further updates announced by the PDPC as this is still the draft announcement and may be subject to changes.

WHO CAN BE A DPO?

"Who can be a DPO?" is one of the popular issues that we found when performing the PDPA implementation project. Until now, there is no specific qualifications of DPOs officially announced by the PDPC. Generally, the DPO may be an existing employee of company or a service provider under the contract depending on the discretion, as well as other organizational factors (e.g., the readiness of its personnel, budget of the company, etc.). However, to perform his/her tasks effectively, the DPO must be a person who has in-depth understanding in the PDPA requirements as well as in technical and organizational structures of the company. Besides, the DPO should be trustworthy and not be constrained by his/her current duties or those involving the processing of personal data.

DELOITTE'S OBSERVATION

Prior to the full enforcement of PDPA in June 2022, all stakeholders should have a good understanding towards the PDPA requirements as well as its organizational and technical infrastructure. With this regard, the DPO plays a significant role in facilitating the personal data management within the company and in monitoring whether the processing of personal data is in accordance with relevant regulations. Notably, the breach may result in the heavy penalty of up to THB 5 million. This does not include reputation risk that the company may have to spend a huge amount of fund in order to recover.

Although there is no sub-law regarding the DPOs issued by the PDPC at the moment, we recommend all organizations processing personal data to appoint DPOs (whether a person or a team), especially during this time where the PDPA is newly introduced among Thai business operators, so that they could be the company's PDPA expertise and the center of communication regarding the PDPA related issues.

All things concerned, all stakeholders should be aware of the DPO's importance and monitor further announcements by the PDPC regarding the requirement of having the DPO and qualifications of the DPO in order to find the right DPO for your company.

For more information on how Deloitte can help you, please contact:

Sutthika Ruchupan
Legal Counsel
Tel: + 66 (0) 2034 0000 Ext 11473
Email: sruchupan@deloitte.com

Nattarin Kuwiboonsin
Legal Managing Associate
Tel: 66 (0) 2034 0000 Ext 15007
Email: nkuwiboonsin@deloitte.com

About Deloitte Legal

Deloitte Legal means the legal practices of DTTL member firms, their affiliates or their related entities that provide legal services. The exact nature of these relationships and provision of legal services differs by jurisdiction, to allow compliance with local laws and professional regulations. Each Deloitte Legal practice is legally separate and independent, and cannot obligate any other Deloitte Legal practice. Each Deloitte Legal practice is liable only for its own acts and omissions, and not those of other Deloitte Legal practices. For legal, regulatory and other reasons, not all member firms, their affiliates or their related entities provide legal services or are associated with Deloitte Legal practices.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms, and their related entities (collectively, the "Deloitte organization"). DTTL (also referred to as "Deloitte Global") and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more

Deloitte Asia Pacific Limited is a company limited by guarantee and a member firm of DTTL. Members of Deloitte Asia Pacific Limited and their related entities, each of which are separate and independent legal entities, provide services from more than 100 cities across the region, including Auckland, Bangkok, Beijing, Hanoi, Hong Kong, Jakarta, Kuala Lumpur, Manila, Melbourne, Osaka, Seoul, Shanghai, Singapore, Sydney, Taipei and Tokyo.

About Deloitte Thailand

In Thailand, services are provided by Deloitte Touche Tohmatsu Jaiyos Co., Ltd. and its subsidiaries and affiliates.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms or their related entities (collectively, the "Deloitte organization") is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and none of DTTL, its member firms, related entities, employees or agents shall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication. DTTL and each of its member firms, and their related entities, are legally separate and independent entities.

© 2021 Deloitte Touche Tohmatsu Jaiyos Advisory Co., Ltd.