KUDUN & PARTNERS

Legal Alerts | Data Privacy and Protection

Does Your Company Need a DPO and Who to Appoint?

In many aspects, the Personal Data Protection Act B.E. 2562 (2019) (the "**PDPA**") has posed considerable challenges to organizations. One of the biggest concerns and the most frequently asked questions center around the concept of data protection officer ("**DPO**"). Though the obligations regarding the appointment of a DPO apply to both data controllers and data processors, it is important to note that not every organization needs a DPO.

Who is a DPO?

A DPO may be an individual or an organization. Currently, the PDPA does not specify the qualifications of a DPO, but only sets out its roles and responsibilities. The PDPA also states that the DPO may also perform other tasks, so long as such tasks do not create any conflict of interest of the DPO's responsibilities under the PDPA, meaning that the DPO's roles within your company should not include determining the company's processing of personal data (e.g., determining purposes and method of processing).

Though the PDPA does not yet specify the qualifications of a DPO, we can learn from the DPO's statutory roles and responsibilities as to who would be appropriate for the task. With its advisory and supervisory roles to the company (as the data controller or the data processor) and its employees, a DPO should be independent and have knowledge of data protection compliance under the PDPA. It is advisable that the knowledge level of the DPO corresponds to each organization's risks and complexity of personal data processing.

July 2021

Get in touch

Nattaya Tantirangsi
Senior Associate
nattaya.t@kap.co.th

Panithida Termrungruanglert
Associate
panithida.t@kap.co.th

Pariyakorn Rungrueang
Associate
pariyakorn.r@kap.co.th

Kudun and Partners

23rd Floor, Unit C and F,
Gaysorn Tower 127,
Ratchadamri Road,
Lumpini, Pathumwan
Bangkok, 10330, Thailand
contact@kap.co.th

Does Your Company Need a DPO?

Your company must appoint a DPO if it falls into any of the following categories.

1. **Your company's activities consist of processing operations which require regular and systematic monitoring of a large scale of personal data.**

   What is regular and systematic monitoring? Both the PDPA and the draft PDPA sub-regulations publicly released earlier this year (2021) ("**Draft PDPA Sub-Regulations**") are silent on the meaning of 'regular and systematic monitoring'; therefore, we will refer to the WP29 Guidance on DPOs[1] pursuant to article 37(b) of the GDPR (the "**Guidance**"). The Guidance suggests that the meaning of 'regular' includes ongoing or occurring at particular intervals for a particular period, recurring or repeated at fixed times or constantly or periodically taking place. It further suggests that the meaning of 'systematic' includes occurring according to a system; pre-arranged; organized; or methodical; taking place as part of a general plan for data collection; or carried out as part of a strategy. Consequently, regular and systematic monitoring can include all forms of tracking and profiling, such as location tracking by mobile apps, monitoring of wellness, fitness and health data via wearable devices.

   What is considered 'large scale of personal data'? The Draft PDPA Sub-Regulations suggest that "large scale" means either when the data controller or the data processor has in its possession personal data of more than (1) 50,000 data subjects or (2) 5,000 data subjects in case of sensitive data processing, within any 12-month period.

   Moreover, the Draft PDPA Sub-Regulations also set out some specific activities which shall be deemed as large scale of processing ***regardless*** of the number of data subjects mentioned above, and thus require designation of a DPO. These activities include, but are not limited to, processing of personal data for behavioral advertising by search engine or social media providers and processing of customers' personal data in the regular course of business by insurance companies, commercial banks or other similar businesses that conduct risk assessment of their clients prior to entering into contracts or providing relevant services.

2. **Your core activity concern collection, use or disclosure of sensitive personal data.**

   The PDPA and the Draft PDPA Sub-Regulations are silent on the definition of 'core activity'. Therefore, we refer to the Guidance and the ICO'S Guide[2] on the GDPR for answers. A core activity means the primary business activity of an organization. For example, processing patients' health data is a core activity of a hospital, while other integral activities such as financing or recruitment would be considered secondary activities.

3. **You are a public authority.**

   The PDPA authorized the Personal Data Protection Committee to announce a list of public authorities required to appoint the DPO. Such list is currently absent, while the Draft PDPA Sub-Regulations suggest that public authorities in this case should cover governmental agencies, state enterprises, local administrative agencies and other state agencies.

More Thoughts on DPO

If your company is not required to appoint a DPO, appointing a DPO may however be advisable in order to be prudent and to convey accountability to the data subjects (your clients). Considering that the GDPR-level of personal data protection compliance under the PDPA is a concept recently introduced in Thailand and that the obligations the PDPA imposes could be hugely unfamiliar to your company (including its directors, management and employees), voluntary appointment of a DPO could be a step further to ensure that your company is PDPA compliant.

For more information, please get in touch with our Data Privacy and Protection lawyers or alternatively, please contact the authors.

[1] "Guidelines on Data Protection Officers ('DPOs')." *European Commission,* https://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf?wb48617274=CD63BD9A

[2] "Data Protection Officers." *Information Commissioner's Office,* https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-officers/

About Us

KAP Cloud, a subsidiary of Kudun and Partners, together with various digital and technology solution providers are teaming up to provide a comprehensive solution for our client's PDPA compliance. We believe technology and legal expertise need to come hand in hand to address this issue.

We have a dedicated team who is keen to understand our client's business and in helping them achieve their purpose in navigating the complex regulation of data and achieving their goals and objectives.