Seri Manop & Doyle

THAILAND PERSONAL DATA PROTECTION ACT B.E.2562 (2019) ("PDPA") ENFORCEMENT

- EMPLOYER'S OBLIGATIONS UNDER THAILAND PDPA-

LABOUR AND EMPLOYMENT

Key Definitions under PDPA

Data Controller means a (natural) person or a juristic person having the power and duties to make decisions regarding the collection, use, or disclosure of the Personal Data

Data Processor means a (natural) person or a juristic person who operates in relation to the collection, use, or disclosure of the Personal Data pursuant to the orders given by or on behalf of a Data Controller, whereby such (natural) person or juristic person is not the Data Controller

Personal Data means any information relating to a (natural) person, which enables the identification of such person, whether directly or indirectly, but not including the information of the deceased persons in particular

Following a period of delay since 2019, Thailand Personal Data Protection Act (PDPA) is now enacted as of June 1st, 2022 onwards. The PDPA is quite important as it protects a broad category of natural person personal data from any unauthorized collection, use, or disclosure and processing by all organizations that collect, use or disclose personal data in Thailand.

Personal Data Protected under PDPA

The key concept contained in the PDPA is that the Data Controller and Data Processor (as defined above) to inform and request the data owner's consent prior to any collection, use, or disclosure of their personal data. In addition, the consent provided must be clear and explicit and given on or before the collection of personal data. The data owner is also allowed to withdraw such consent at any time.

However, there are certain exemptions to this cost requirement if the data is used for the following reasons including:

i) The fulfillment of contractual obligations;
ii) Public interest (e.g. statistical research to protect the public health); and
iii) Fulfil legitimate interest (e.g. prevention of danger to an individual).

Personal Data Protected under PDPA

General Personal Information i.e. name/surname, telephone no., e-mail, address, ID card no., passport no., driver license no., educational information, financial information, medical information, vehicle license plate no., date of birth, nationality, weight/height and other information available online that could identify a person (username/password, cookies IP, GPS location)

Sensitive Information i.e. race, political thoughts, beliefs in cult/religion/philosophy, sexual orientation, criminal record, personal health information, labor union information, genetic information, biometrics data

Contact Us

Seri Manop & Doyle Ltd.

No. 21 Soi Amnuaiwat, Sutthisan Road, Samsennok Sub-district, Huaikhwang District, Bangkok 10310, Thailand

Tel: (662) 693 2036
Email: info@serimanop.com

In case of a PDPA violation, civil, criminal and administrative penalty would apply as follows:

- Criminal penalty: imprisonment for up to 1 year, or a fine up to THB 1 million or both
- Civil penalty: damages and punitive damages up to the amount of the actual damages
- Administrative penalty: a fine not exceeding THB 1 million/3 million/ 5 million

EMPLOYER'S OBLIGATIONS UNDER THAILAND PDPA

Employers (either as an individual or a company) also have obligations under the PDPA related to making decisions or taking any action with regard to the collection, use, or disclosure of personal data of employees.

The employers shall not collect, use, or disclose personal data of employees, unless the employee has given consent prior to or at the time of such collection, use, or disclosures. The consent can be provided in writing or electronically. It is important to note that in case of Sensitive Information, it must not be collected by the employers without the explicit consent of the employee, unless in the the case of the above exemptions.

In order to comply with the above PDPA requirements (even if a consent is not expressly required) employers should, whenever possible, take actions necessary in order to notify employees prior to collecting their personal data and fulfil the below requirements:

1. The employee consent should be explicit;
2. Employees should be notified of the purpose of collection, processing, retention period and/or disclosure;
3. The collection of personal data should be limited to the extent of its purpose of use;
4. Employees should have the right to withdraw consent at any time;
5. Employers must inform employees of any consequences associated with the withdrawal of consent; and
6. The employee's right of access their own data and right to request their personal data corrected.

Updated on 1st June 2022