Answers to Frequently Asked Questions Concerning Thailand's Personal Data Protection Act (PDPA) Employment

Written by Mike Doyle | Pakdeenad Supradit N Ayudhya | Kanyanat Thuamsiri

Do PDPA Requirements Apply to Thailand Parties only ?

There is a common misconception that only Thailand parties are required to comply with Thailand's Personal Data Protection Act, or for short, PDPA but that is not the case.

The PDPA provides employees and other individuals protection related to their personal data, which means that any data pertaining to an individual that enables the identification of that individual, whether directly or indirectly such as data the individual's name/surname, phone number, address, email address, ID card number, fingerprint, passport number, driver license number, educational information, financial information, medical information, or other information (available online or offline) which could identify such individual.

Consequently, the data protection obligations under the PDPA apply to ALL organizations that collect, use, or disclose personal data in Thailand or of Thai residents, regardless of whether they were formed under Thai law (referred to as Data Controllers), and whether or not they are residents or have a business presence in Thailand.

SERI MANOP & DOYLE Ltd.
Tel: (662) 693 2036
Fax: (662) 693 4189
Email: info@serimanop.com
http://www.serimanop.com
21 Soi Amnuaiwat, Sutthisan Road, Samsennok
Sub-district, Huaikhwang District, Bangkok 10310, Thailand

What Should Companies do the Ensure that They are in Compliance with the PDPA ?

Companies should implement the following policies with respect to the employee data management.

1. Managing Personal Records.

Employee personal data is required to be stored, managed, analyzed and maintained in a standardized manner in order to prevent disclosure, including having a system to update employee data in a secure way.

2. Obtaining Employee Consent.

The company's PDPA policy should, also require the company to obtain employee consent before using, storing or disclosing personal information which clearly specifies the purpose and the duration of the use of personal information.

Is the Employer Required to Obtain Consent from the Employee Each Time the Employee's Personal Data is to be Disclosed ?

There is also misconception that the owner of the personal data is required by law to grant their consent for the use of the data at all times. However, in actual fact, the employee is required to give consent to the Data Controller as stated in the first instance only once. However, if the Data Controller intends to use the personal data in a way that is different from the purposes for which the employee or other data subject has previously given consent, the Data Controller must also notify and obtain consent to the data subject for that purpose again.

What are the Consequences of Violating the PDPA ?

Failure to comply with the PDPA the Data Controller is subject to civil, criminal and administrative penalties. The civil penalty, is that the organization must indemnify the data subject or employee for his/her actual damages incurred. The criminal penalty is imprisonment for not more than 1 year or a fine of not more than 1,000,000 baht, or both. The administrative penalty, is a fine of up to 5,000,000 baht