Employers Brace Themselves as New Personal Data Protection Act Looms

by Pimvimol (June) Vipamaneerut, partner, and Gvavalin Mahakunkitchareon, attorney-at-law, Tilleke & Gibbins

The draft Personal Data Protection Act (PDPA) was approved by the National Legislative Assembly in February 2019, raising concern among business entities over the need for increased diligence to ensure adherence to the provisions. Running a business often entails handling the personal data of employees, contractors, suppliers, customers, and others. Any personal data collected could be subject to the provisions of the PDPA, and as employee data falls under the PDPA, all businesses, should be prepared to deal with the impact of the PDPA.

Although this final version of the PDPA has not yet received Royal Assent and been published in the *Government Gazette*, the endorsement and publication is expected soon.

The majority of the provisions in the PDPA will only come into force a year after its publication in the *Government Gazette*. This transitional period will allow any entity subject to the PDPA to review and adjust their personal data–related activities.

What is Personal Data?

Personal data is broadly defined as any data about a person that enables the identification of that person, whether directly or indirectly, but specifically excluding data of the deceased. This can include a person's name, identification card number, email address, mobile phone number, health information, payroll information, or bank account number.

Data Controller or Data Processor?

The PDPA sets out different duties and obligations for a data controller and a data processor. A data controller is defined as any person or legal entity that has the power and duty to make decisions on whether to collect, use, or disclose personal data. In contrast, a data processor is defined as any person or legal entity that collects, uses, or discloses personal data on behalf of, or pursuant to, the instructions of the data controller. Since employers have the power to determine which categories of personal data should be collected and retained, they are therefore acting as data controllers.

Obtaining Consent

Collection, use, or disclosure of personal data is generally prohibited unless consent from the data subject has been obtained or unless it falls within an exemption prescribed under the PDPA. The exemptions include, among others, when it is necessary to comply with a contract to which the data subject is a party, or pursuant to the requests of the data subject prior to entering into a contract; and when it is necessary for the legitimate interest of the data controller, other person, or other entity, unless such interest is less significant that the fundamental right of the data subject.

Employers, therefore, should carefully consider whether separate consent must be obtained from their employees or the language of the employment agreement is sufficient for the purpose of possessing their employees' personal data in compliance with the PDPA.

If separate consent is required, such a request must
1. be made prior to, or at, the time of collection;
2. be made in writing or via electronic means;
3. be clearly separated from other terms;
4. be in an easily accessible format or use terms which are understandable;
5. be written in plain language; and
6. not be misleading or deceptive.

The PDPA, however, does not specifically require that the consent must be made in Thai language.

Sensitive Personal Data

Most companies require their employees to provide information relating to their health, race, religion, or biometric data (e.g. fingerprints). These categories of personal data are considered as sensitive personal data. The PDPA expressly prohibits the collection of such data unless explicit consent from the data subject has been obtained, or unless otherwise exempted.

One of the exemptions is where the sensitive personal data is collected for labour protection, social security, or national health security purposes, and it is deemed as necessary for the data controller or data subject to satisfy his or her rights or obligations.

It is still unclear whether collecting sensitive personal data of employees would fall within the scope of this exemption. Hence, employers should closely observe the PDPA and its subordinate regulations once they come into force.

Use of Personal Data

Personal data can only be used for the purposes for which the consent has been granted. Therefore, if the purpose of use has changed, fresh consent from the employee must be obtained.

Retention Period

Where a request for consent is required, the employer must inform employees about the period for which their personal data will be retained.

As the longest prescription period for various labour disputes, including unfair termination, is ten years from the date the claim could be enforced, employers should consider retaining their employees' personal data until the period of prescription expires. Regardless of the length of the retention period that the employer ultimately chooses, they must ensure that this retention period is clearly communicated to the employees.

Cross-border Transfer

Companies often transfer employees' personal data within their group of companies, some of which might be located overseas. If such transfer complies with the company's internal policy for sharing personal data in accordance with the requirements of the PDPA, it would be exempt from the general PDPA requirement for transferring data internationally — i.e. the employer would not need to ensure that the destination country implements an appropriate standard for personal data protection, or obtain further consent. Whether or not an internal policy renders such a transfer exempt is likely to be a matter of some dispute, and companies wishing to transfer data internationally should be particularly cautious about this exemption.

Grandfather Provision

As for employees' personal data that has been collected prior to the PDPA coming into effect, employers may continue to use this data without the need to obtain consent, provided such data is used solely for the purpose for which it was originally collected, and that the employer complies with the PDPA when doing so.

Rights of the Data Subject

Employers should ensure that their employees have been clearly informed of their rights under the PDPA, including, but not limited to, right of access, right to data portability, right to withdraw consent, and right to erasure.

Other Obligations

Under the PDPA, the employer, as the data controller, has an obligation to ensure that any other person or entity to whom the personal data is disclosed will not use or disclose such personal data unlawfully or without authorization.

Data processors are also required to implement appropriate security measures to prevent access that would enable the use, alteration, amendment, or disclosure of the personal data unlawfully or without authorisation. Therefore, where there are inappropriate security measures, it may prove difficult for an employer to escape liability in the event of a data breach.

Penalties

Non-compliance with the PDPA could lead to severe civil liabilities, administrative liabilities, and criminal penalties—the latter two including fines of up to THB 5 million, and even imprisonment.

How Should Employers Prepare?

- Review current personal data protection policies, employment contracts, and work rules to ensure the terms will be compliant with the PDPA (and any other relevant laws).
- Review agreements with customers, contractors, suppliers, and any other related parties.
- Ensure that an appropriate, PDPA-compliant system for personal data protection is in place.
- Identify categories of personal data that are required for a business's legitimate purposes, and only collect and retain such data.
- Provide personal data protection training for employees.

It is essential that all employers closely observe and adhere to the PDPA and subordinate regulations once they come into force, and prepare themselves well in advance, in order to ensure their employee personal data–related activities do not violate any applicable laws. Those who fail to do so could find themselves faced with angry employees and severe penalties

Authors: Pimvimol (June) Vipamaneerut, partner and head of the firm's non-contentious employment practice, and Gvavalin Mahakunkitchareon, attorney-at-law; Tilleke & Gibbins. Please send any comments or questions about the content of this article to Andrew Stoutley at andrew.s@tilleke.com.

Series Editor: Christopher F. Bruton, Executive Director, Dataconsult Ltd, chris@dataconsult.co.th. Dataconsult's Thailand Regional Forum provides seminars and extensive documentation to update business on future trends in Thailand and in the Mekong Region.