Deloitte.
Legal

PDPA Alert
26 September 2022

Notifications and rules issued under the PDPA for data controllers, data processors and data subjects

Experience the future of law today.

Shortly after the Personal Data Protection Act B.E. 2562 (2019) ("**PDPA**") has become fully effective on 1 June 2022, the Personal Data Protection Committee ("**PDPC**") announced additional notifications and rules to further spell out PDPA implementations and compliances.

The notifications and rules were continuously promulgated on the Government Gazette starting in June 2022. Following are a summary of the notifications and rules issued during 20 June 2022 - 11 July 2022.

1. Notification of the PDPC RE: Exemption from the Preparation of Records of Processing Activities for Small Businesses B.E. 2565 (2022)

Under Section 39 of the PDPA, data controllers are required to prepare and maintain a record of processing activities or the so called "RoPA". This PDPC's notification exempts the following small businesses from the application of such provision:

(i) Small or medium sized companies under the laws on promotion of small and medium sized enterprises;
(ii) Community enterprises or community enterprise networks under the laws on promotion of community enterprises;

(iii) Social enterprises or a group of social enterprises under the laws on promotion of social enterprises;
(iv) Cooperatives, cooperative federations, or agricultural groups under the laws on cooperatives;
(v) Foundations, associations, religious organizations, and non-profit organizations; or
(vi) Household businesses or other similar businesses.

This exemption does not apply to small businesses which (i) are service providers collecting information through computer traffic logs in accordance with the laws on offenses related to computers (save for internet café service provider), (ii) collect, use, and/or disclose personal data in manners or forms which might affect the rights and liberties of data subjects, (iii) process the personal data on a regular basis, or (iv) collect, used, and/or disclose sensitive personal data under Section 26 of the PDPA.

2. Notification of the PDPC RE: Criteria and Methods for Preparing and Maintaining Records of Processing Activities for Data Processors B.E. 2565 (2022)

Being effective on 17 December 2022, this PDPC's notification provides the particulars required to be maintained by the data processors in the record of processing activities according to Section 40 of the PDPA. Accordingly, the data processors must prepare and maintain a record of processing activities containing, as a minimum, the following particulars:

(i) Names and details of the data processors, and their representatives (if any);
(ii) Names and details of the data controllers which the data processors operate pursuant to their instructions or on behalf of, and their representatives (if any);
(iii) Names and details of data protection officers, including the addresses and contact methods, (if any);
(iv) Types or details of processing activities conducted on demand/behalf of the data controllers;
(v) In case of cross-border transfer of personal data, the details of the recipients; and
(vi) Explanations of security measures according to Section 40 of the PDPA.

3. Notification of the PDPC RE: Security Measures for the Data Controllers B.E. 2565 (2022)

According to Section 37(1) of the PDPA, the PDPC shall set the minimum standards for the appropriate security measures for preventing the unauthorized or unlawful loss, access to, use, alteration, correction, or disclosure of personal data. This PDPC's notification, therefore, lays out such minimum requirements in more details as follows:

(i) The security measures must cover the collection, usage, and disclosure of personal data in all forms including hard copies and electronic forms;
(ii) The security measures must consist of organizational, technical, and physical measures appropriate to the level of risks and possibilities of breaches which may arise;
(iii) The measures must be accounted for the securities in various aspects such as identifying, monitoring, and preventing risks to personal data breach, responding to personal data breach, restoring damages from the personal data breach, etc.;

(iv) The security measures must take into account the ability to maintain confidentiality, integrity, and availability of personal data appropriate to the risks;
(v) The security measures for the collection, usage, and storage of personal data in electronic systems must cover all related components of the systems;
(vi) The security measures related to the access, usage, alteration, correction, destruction, or disclosure of personal data must consist of the particulars required by this PDPC's notification such as access control, identity proofing and authentication, user access management, etc.;
(vii) The security measures must include privacy and security awareness building;
(viii) The data controllers must review the security measures not only when there are changes in the technology but also when there are breaches to the personal data in their possession; and
(ix) When entering into a data processing agreement with data processors, the data controllers must also ensure that the minimum standard for security measures are met.

4. Notification of the PDPC RE: Criteria for Determining and Ordering Imposition of Administrative Fines for Expert Committees B.E. 2565 (2022)

According to Section 90 of the PDPA, the expert committee shall determine the issuance of an order to impose an administrative fine taking into consideration the severity of the circumstances of the act of offense, size of the business of the data controller or the data processor, or other circumstances according to the rules prescribed by the PDPC. Among other things, this PDPC's notification categorizes the administrative punishments into two major levels as follows:

- Non-severe cases - Possible punishments are such as warning, injunction, restriction of personal data processing
- Severe cases - Possible punishments are administrative fines as prescribed by the PDPC together with the punishments for non-severe cases

5. Rule of the PDPC RE: The filing, refusal, dismissal, consideration, and timeframe for the consideration of the complaints B.E. 2565 (2022)

According to the PDPA, the data subjects have the right to file complaints if the data controllers or the data processors violate or do not comply with the PDPA, or notifications and rules issued thereunder.

The rule spells out the methods for filing complaints whereby the complaints can be submitted to an expert committee in person, through the post, or through electronic channels which are to be further specified by the office of PDPC. Further, the rule lists out the minimum information and documents which are required for a valid complaint, examples of which are:

(i) Identity of the person making complaint;
(ii) Details of the violations or non-compliances; and
(iii) Details of damage or impact that such violations or non-compliances have on the data subject.

Deloitte's observation

From the effective date of the PDPA onwards, there has been significant development in the drafting, hearing, and promulgation of the sub regulations providing a clearer guideline for PDPA compliance as well as enforcement of the law. The PDPC may announce more sub-regulations in the near future to outline the PDPA enforcement, for example, to govern the requisition of consents, to extend the meaning of sensitive personal data, to control cross-border transfer of personal data, etc.

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

Anthony Visate Loh
Country Leader

Tel: + 66 (0) 2034 0112
Email: aloh@deloitte.com

Sutthika Ruchupan
Legal Counsel

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

Narita Sakunchotikarote
Legal Associate

Tel: + 66 (0) 2034 0000 Ext 16053
Email: snsakunchotikarote@deloitte.com