PwC Indonesia Legal Alert

January 2023 / No. 14

The New Era for Personal Data Protection in Indonesia

The Indonesian Government issued Law No. 27 Year 2022 on Personal Data Protection ("**PDP Law**") on 17 October 2022. Promulgation of PDP Law is a major progression for the protection of personal data, where the PDP Law serves as the umbrella law for the application and implementation of personal data protection in Indonesia. The PDP Law provides more significant, stringent and integrated protection compared to previously scattered regulations, which were supervised by several authorities. PDP Law applies to: (a) any Person (including individuals and corporations), (b) Public Entities, and (c) International Organisations residing in Indonesia, or in a foreign jurisdiction, if any legal impact occurred within the territory of Indonesia and/or if the subject of the personal data is an Indonesian citizen.

PDP Law is effective from the date of its enactment on 17 October 2022, but it provides a transition period of two years for the Personal Data Controller, Personal Data Processors and other relevant parties to adjust and comply with the law.

Below we highlight key provisions and major points for you to note and consider as you transition your organisation towards complying with the PDP Law.

I. What's new?

1. New Terms

PDP Law distinguishes the previously known electronic system provider, into Personal Data Controllers (**"Data Controllers**") and Personal Data Processors (**"Data Processors**"). The Data Controllers determine the purpose and control the processing of personal data, while the Data Processors act on behalf of the Data Controllers to perform the processing of personal data. In this case, the obligations of the Data Controller are regulated in Articles 20 to Article 50, wherein those obligations, namely Article 29, Article 31, and Articles 35 to Article 39, also apply to Data Processors.

2. Notification of Data Breach

In the event of a data breach, the Data Controllers must deliver written notification no later than 3 x 24 hours to the personal data subjects and to the authority. This is a much stricter rule, whereas previously the notification period of a data breach was 14 (fourteen) days, under the Minister of Communication and Informatics Regulation No. 20 of 2016 on Personal Data Protection in Electronic Systems ("**MOCI Reg. 20/2016**"). PDP Law states that written notification should at least contain a description of breached personal data, how and when the breach occurred and the mitigation actions and recovery efforts on the breach's occurrence.

In some events, Data Controllers may disclose to the public when the breach interferes with public services and/or has a severe impact to the public. However, the PDP Law does not elaborate and provides a clear understanding of what constitutes disrupting public services and the level of the adverse impact.

3. Data Protection Officer

The Data Controllers and Data Processors are required to appoint a data protection officer. This is a mandatory function of protecting personal data where the processing of personal data is conducted for public services. The core activity of the Data Controllers requires regular and systematic monitoring of large-scale personal data and where the core activity of the Data Controllers is a large-scale processing of specific personal data and/or personal data related to criminal acts.

4. Cross-Border Transfer

Cross-border transfer of personal data is allowed with the condition that the Data Controllers must ensure the recipient country has an equal or higher personal data protection governance than the PDP Law. If these provisions cannot be met, the Data Controllers must ensure that there is adequate and binding protection, or at the very least, consent must be given from the personal data subjects. Failure to comply with this provision will be subject to administrative sanction. Further details on the cross-border transfer of personal data will be elaborated under a Government regulation.

5. Types of Personal Data, Rights of the Personal Data Subjects

Types of Personal Data

PDP Law defines personal data as any data concerning an individual or person, either fully identified and/or who can be identified separately, or data combined with other information directly or indirectly through an electronic and/or non-electronic system.

Based on PDP Law, there are two types of personal data:

a. General personal data, i.e., a type of personal data which consists of a full name, gender, citizenship, religion, marital status, and/or personal data which combines to enable identification of an identity; and

b. Specific personal data, i.e., a type of personal data in which the processing of the data can result in a greater impact on the personal data subjects, among others, acts of discrimination and greater loss to the personal data subjects. This type of personal data consists of health data and information, biometric data, genetic data, criminal records, children's data, personal financial data, and/or any other data in accordance with the prevailing laws and regulations.

Rights of the Personal Data Owner

Below are the notable rights of the personal data subjects based on the PDP Law:

a. Rights of information, the personal data subjects have the right to obtain information on the clarity of identity, the basis of legal interest, purpose of request and utilisation of personal data, and the accountability of the personal data requester;

b. Rights of modification, which includes any conduct to complete, update, and/or rectify any incorrect or inaccurate information in accordance with the purpose of personal data processing;

c. Rights to access and obtain copies of the personal data;

d. Rights of termination, erasure, and/or disposal of personal data;

e. Rights to withdraw consent given to Data Controllers to process its personal data;

f. Rights to object on any decision made which was based on an automated decision making process, including profiling, which may expose the personal data subjects to legal consequences or significant impact;

g. Rights to delay or limit the processing of personal data proportionately in accordance with the purpose of personal data processing; and

h. Rights to claim and receive compensation over personal data processing violations.

6. International Cooperation

The Government can enter into international cooperation with the government of other countries or international organisation concerning personal data protection. This arrangement must be implemented based on the applicable laws and international law principles.

II. Introduction of Data Privacy Protection Authority

PDP Law mandated the establishment of a personal data protection authority to carry out government affairs in personal data protection. The data privacy protection authority is instituted and responsible for the President of Indonesia. The authorities' duties are, among others, to formulate and stipulate policies and strategies for personal data protection, conduct supervision on the implementation of personal data protection, to enforce administrative law on any violation to the law, and to facilitate alternative dispute resolutions.

III. Stringent Rules on Sanctions

1. Impact Assessment

Data controller is required to perform an impact assessment for any personal data processing, which is potentially high-risk for the personal data subjects. High-risk personal data processing includes: (a) automated

decision making that has legal consequences or significant impact on Personal Data Subjects, (b) personal data processing of a specific nature, (c) large-scale data processing, (d) data processing for the purpose of a systematic evaluation, scoring, and monitoring of personal data subjects, (e) matching or merging a group of data, (f) use of new technologies for personal data processing, and (g) any personal data process limiting the enforcement of rights of the personal data subjects.

2. Notification on Corporate Actions

Data Controllers in the form of a legal entity must inform personal data subjects prior to and after the completion of the following corporate actions: merger, spin-off, acquisition, consolidation, or dissolution. In case of dissolution, the Data Controllers in dissolution must disclose any retention, transfer, erasure, or disposal of any personal data to the personal data subjects.

3. Prohibitions in the Use of Personal Data

PDP Law restricts any person to:

(a) unlawfully obtain/collect personal data that does not belong to them, with the intention to benefit themselves or other persons which will be disadvantageous to the Personal Data Subject;

(b) unlawfully disclose and use personal data that does not belong to them;

(c) create false personal data with the intention to benefit themselves or other persons which may result in the loss of other persons.

4. Administrative Sanctions

Administrative sanctions under this PDP Law can be in the form of a written warning, temporary suspension of personal data processing, deletion, or disposal of personal data, and/or administrative fines. Imposition of an administrative fine is newly adopted in this PDP Law, which was not included in the sanctions for personal data violation in the MOCI Reg. 20/2016. The maximum amount for an administrative fine that can be imposed is 2% (two percent) of the annual income or annual revenue of the violation variables.

5. Criminal Sanctions

Imposition of criminal sanctions for personal data violation is also newly adopted by the PDP Law. Corporations can be imposed for criminal fines with a maximum amount of 10 (ten) times of the criminal fines that it is subject to. In addition, corporations may also be subject to (i) confiscation of profits and/or wealth obtained or the proceeds of criminal actions; (ii) freezing of all or part of the business; (iii) permanent prohibition of certain conduct; (iv) closure of all or part of the place of business and/or corporate activities; (v) carrying out obligations that have been neglected; (vi) payment of compensation; (vii) license revocation; and/or (viii) dissolution of the corporation.

IV. Actions to Take

Data Controllers, Data Processors, and other parties relevant to personal data protection are given two years to adjust and comply with the PDP Law. Any organisation must perform a legal and compliance assessment of its existing system and business operation and identify any gaps and areas for improvement to adhere with the PDP Law. The legal and compliance assessment must be made to this PDP Law and any other personal data protection obligations under specific sector regulations, such as OJK Regulations for financial services businesses, to ensure full compliance of personal data protection rules.

This Legal Alert is only intended to give an overview of several provisions and may not cover all of the provisions in PDP Law. Please do not hesitate to contact us if you need more detailed advice or have specific questions.

Your PwC Indonesia Contacts:

Please feel free to contact our Legal Specialists.

Melli Darsa
Managing & Senior Partner
Melli Darsa & Co., Advocates & Legal Consultants
melli.darsa@pwc.com

Indra Allen
Partner
Melli Darsa & Co., Advocates & Legal Consultants
indra.allen@pwc.com

Danar Sunartoputra
Partner
Melli Darsa & Co., Advocates & Legal Consultants
danar.sunartoputra@pwc.com

Puji Atma
Director
Melli Darsa & Co., Advocates & Legal Consultants
puji.atma@pwc.com

Indra Natakusuma
Director
Melli Darsa & Co., Advocates & Legal Consultants
indra.natakusuma@pwc.com

Fifiek Mulyana
Director
Melli Darsa & Co., Advocates & Legal Consultants
fifiek.mulyana@pwc.com

www.pwc.com/id

PwC Indonesia

@PwC_Indonesia

If you would like to be removed from this mailing list, please reply and write UNSUBSCRIBE in the subject line, or send an email to **id_contactus@pwc.com**.

pwc