NEWSLETTER

November 2022

The New Personal Data Protection Law what you need to know

Key contacts:

Eka Siswani
Partner
ekaws@mkklaw.net

Oka Anantajaya
Senior Associate
oka.anantajaya@mkklaw.net

The Indonesian House of Representatives passed the Personal Data Protection Bill into Law on 20 September 2022 becoming effective on 17 October 2022. Now known as Law No. 27 of 2022 concerning Personal Data Protection (the "**PDP Law**"), it is expected to serve as the foundational regulatory framework in addressing cybersecurity and personal data protection challenges.

Key subjects

The PDP Law is extensive comprising 76 Articles and 16 Chapters encompassing several key provisions, among others:

- personal data;
- data subjects (the owner of personal data);
- personal data processing;
- the roles of the data controller, data processor and data protection officer;
- data protection impact analysis;
- cross-border data transfer notification to data subject in the event of corporate action; and
- criminal and administrative sanctions as well as the creation of a data protection regulatory agency.

Who the PDP Law applies to

The PDP Law applies to every person, entity, public institution and international organization that processes personal data in Indonesia, or outside of Indonesia but with a legal impact in Indonesia and/or on Indonesian data subjects outside Indonesia. The PDP Law does not apply to personal data processing by individuals on private or household matters. Unhelpfully, these exceptions are not discussed in the elaboration, and it is unclear how regulators will interpret such exception

Definitions

Under the PDP Law, "personal data" is defined as a data concerning individuals that can be identified or is identifiable either separately or in combination with other information either directly or indirectly through electronic or non-electronic systems. The PDP Law introduces 2 categories of personal data:

- *General data* comprising of full name, gender, citizenship, religion, marital status and/or combined personal data used to identify a person; and
- *Specific data* consisting of health information, biometric and genetic data, criminal records, children's data, personal financial data and/or other data specific data as set out under the laws and regulations.

Unlike the European General Data Protection Regulation (EU GDPR) which differentiates basic principles of data processing treatment between general data and specific data, the PDP Law only provides rudimentary guidelines for the processing of personal data where the data controller and data processor:

- are required to carry out data protection impact analysis ("**DPIA**") if the processing involves a potentially high-risk for a data subject; and
- shall appoint a data protection officer if the core activities of the data controller include large-scale processing of specific data and/or personal data related to criminal acts.

Data Controller, Data Processor and Data Protection Officer

Similar to the EU GDPR, the PDP Law also adopts the previously unknown concepts under the Indonesian data protection regulation of a data controller and data processor. A data controller (the party that determines the purpose of personal data processing) and data processor (the party that processes personal data on behalf of a data controller) can be either a person, corporation, public agency, or international organization, authorized to control and process the personal data of a data subject.

The PDP Law introduces the concept of a data protection officer which is also found in the EU GDPR. Essentially, the requirement is to appoint a data protection officer to restrict a data controller and data processor if:

- personal data processing is required for public services;
- the nature, scope, and/or purposes of the core activities of the data controller requires frequent and systematic monitoring of large-scale volumes of personal data; and
- the core activities of the data controller encompass the processing of large-scale volumes of Specific Data and/or personal data related to criminal acts.

The PDP Law stipulates bare minimum requirements for a data protection officer, including providing advice for and ensuring that the data protection compliance of the data controller and data processor(s) in connection with personal data processing. The PDP Law does not state the specific qualifications that must be held by a data protection officer, whereby it only stipulates that a data protection officer is appointed based on professionalism, knowledge of law, data protection practices, and an ability to fulfill the duties. An implementing government regulation will be issued to regulate further the role of a data protection officer.

Rights of Data Subjects

The PDP Law sets out the minimum consent requirements from data subjects for the collection and use of personal data including by electronic or non-electronic means. The PDP Law also specifies several rights of data subjects to their personal data including the right to be informed of personal data processing and utilization, right to correct/amend, right to access and right to terminate, delete and erasure etc.

Data Protection Impact Analysis (DPIA)

Under certain circumstances, a data controller is required to carry out DPIA, if the personal data processing has a high potential risk to a data subject such as:

- Personal data processing involves automatic decision making that has legal consequences or significant impact on the data subject;
- Processing specific personal data;
- Personal data processing involves large-scale personal data processing;
- Personal data processing purported for evaluation, scoring or systematic monitoring of data subject;
- Personal data processing in order to match or combine a group of data;
- Personal data processing by utilizing new technologies; and/or
- Personal data processing which restricts the data subject to exercise their rights.

In relation to the above, an implementing government regulation will be subsequently issued to further regulate DPIA.

Transferring Personal Data overseas

As for the cross-border transfer of personal data, under the PDP Law, a data controller or data processor that wishes to carry out a cross-border transfer of data must ensure that the recipient country has an equal or higher level of personal data protection than Indonesia. If the level of data protection is lower than that of Indonesia, then the data controller must obtain the approval of the data subject to transfer the personal data.

Notification obligations for corporate actions

In the event the data controller is a company and performs a corporate action such as a merger, acquisition, amalgamation, spin-off, or dissolution, the data controller is obliged to notify the data of this "transfer" of personal data, prior to and after the completion of the corporate action.

Data Breach

A data controller must also give written notification no later than 72 hours after a data breach is discovered to a data subject and the to-be-established Indonesian Data Protection Authority (see our discussion below on this new institution). This is a significant shortening of time from the current 14 days timeframe under the Ministry of Communications and Informatics Regulation No. 20 of 2016 on the Personal Data Protection within the Electronic System.

Sanctions

The PDP Law introduces both administrative and criminal sanctions for any violation of the PDP Law. Criminal sanctions include imprisonment for up to six years and fines up to IDR 6 billion for performing unlawful:

- collection of personal data;
- disclosure of other people's personal data;
- use of personal data of others; and
- falsification of personal data.

If the criminal act is carried out by corporations, the maximum penalty is 10 times the amount of the fines imposed. There are also administrative sanctions that can be imposed in the form of written warnings, temporary suspension of personal data processing rights, deletion of personal data and fines. In addition, there is also an administrative fine amounting to 2% of the entity's annual revenue.

New Data Protection Authority

The PDP Law stipulates that there will be a newly-established agency to supervise the implementation of personal data protection, issue policies, impose administrative sanctions with respect of implementation of personal data protection, and facilitate any out of court dispute resolution (e.g., mediation, arbitration, and negotiation). The agency is not yet named and will be established by and report directly to the President by virtue of a Presidential Regulation.

Two-year transitionary period

The PDP Law outlines in its transitionary provisions that data controller, data processor and other parties involved in the processing of the personal data to carry out adjustments with the PDP Law at the latest within 2 years since the enactment of the PDP Law. Further, the PDP Law mandates several provisions to be regulated under its implementing regulations and thereby there are still several provisions under the PDP Law that will be regulated further in a Government Regulation. We will keep on monitoring such progress and update in upcoming newsletter series upon the issuance of such implementing regulations.

Should you have any questions or require specific advice relating to the above, please do not hesitate to contact our ICT lawyers who are also personal data protection officers:

Attorneys	Telephone	E-mail
Eka Siswani – Partner	+62-21-5711130	ekaws@mkklaw.net
Oka Anantajaya – Senior Associate	+62-21-5711130	oka.anantajaya@mkklaw.net