NISHIMURA & ASAHI

西村あさひ法律事務所

Indonesia - The Personal Data Protection Law is finally Issued

Asia / Data Protection Newsletter

December 28, 2022

Author:
E-mail Tomonobu Murata
E-mail Ikang Dharyanto
E-mail Made Grazia Valyana Ustriyana

1. Background

Until recently, Indonesia relied on a patchwork of provisions from various laws and regulations to ensure personal data protection. However, after much delay, on 17 October 2022 the President of the Republic of Indonesia finally ratified the Indonesian Personal Data Protection Law (i.e. Law No. 27 of 2022 on Personal Data Protection; "**PDP Law**") to increase the effectiveness of personal data protection in both electronic and non-electronic systems.

Like the European Union's General Data Protection Regulation ("**GDPR**"), the PDP Law's 16 chapters and 76 articles provide strict regulations that domestic and foreign companies operating in Indonesia must understand in order to implement appropriate compliance measures. While methods similar to those used for compliance with the GDPR may be applicable, the PDP Law has novel aspects, such as the introduction of alternative dispute resolution mechanisms (e.g., mediation), that warrant close attention. As such, key points of the PDP Law are set out below to support businesses' compliance efforts.

2. PDP Law Key Points

Definition of Personal Data

The PDP Law defines "personal data" as the data regarding individuals who are identified or can be identified separately or in combination with other information, either directly or indirectly, through an electronic or non-electronic system.

According to the PDP Law, personal data shall consist of:

a. specific personal data, which includes:[1]

- health data and information, e.g., individual records or information related to physical health, mental health, and/or health services;
- biometric data, e.g., data related to an individual's physical, physiological, or behavioral characteristics that enable unique identification of an individual, such as facial images or dactyloscopy data (biometric data also shall describe the uniqueness and/or characteristics of an individual that must be safeguarded and maintained, including but not limited to fingerprint records, eye/retina, and DNA samples);

[1] Article 4(2) of the PDP Law.

- genetic data, e.g., all data of any kind concerning the characteristics of an individual that are inherited or acquired during early prenatal development;
- crime records, e.g., a written record of a person who has committed an illegal or unlawful act or is in the process of being judged for the committed act, including police records and inclusion in the prevention or deterrence list;
- child data;
- personal financial data, e.g., data on the number of deposits at banks including savings, deposits, and credit card data; and/or
- other data in accordance with the provisions of laws and regulations; and

b. general personal data, which includes:[2]

- full name;
- gender;
- citizenship;
- religion;
- marital status; and/or
- combined personal data to identify a person, e.g., cellular phone numbers and IP addresses.

The definition of "specific personal data" above is analogous to "sensitive personal data" under the GDPR, with a few exceptions. Under both laws, companies must consider the basis for processing.

The PDP Law has introduced six lawful bases for data processing,[3] and it does not differentiate between sensitive and general personal data requirements, save for the particular obligations of (a) conducting a data protection impact assessment ("**DPIA**")[4] in processing specific personal data, and (b) having a Data Protection Officer ("**DPO**")[5] for large-scale specific personal data processing. Also notable is that there are special cases in which the PDP Law requires certain procedures; for instance, the processing of personal data of children and persons with certain disabilities requires the consent of the data subjects' parents and/or legal guardian.

Parties Involved in Personal Data Processing – the Data Controller and the Data Processor

The PDP Law introduces the concepts of:

a. personal data controllers, i.e., every person,[6] public agency, and international organization that acts individually or jointly in determining purposes and exercising control over the processing of personal data; and

b. personal data processors, i.e., every person, public agency, and international organization that act individually or jointly in personal data processing on behalf of a personal data controller.

2 Article 4(3) of the PDP Law.

3 See "Lawful Basis for the Personal Data Processing" section below.

4 See "Data Protection Impact Assessment" section below.

5 See "Data Protection Officer" section below.

6 The definition of "person" in the PDP Law includes individuals and corporations.

The individuals to whom personal data is attached are referred to as “data subjects.”

Due to the introduction of this new concept, companies will need to be aware of their status in data processing activities, whether they are acting as the personal data controller or the personal data processor, since this will impact their compliance requirements and liabilities. For instance, among other things, based on the PDP Law, the personal data processor **must only process** the personal data based on the instructions of the personal data controller, the personal data controller is responsible for the processing of personal data by the personal data processor, and the personal data processor must obtain written approval from the personal data controller before engaging other personal data processors. This shows that the obligations of the personal data controller are significantly greater than those of the personal data processor, unless the personal data processor conducts personal data processing beyond the orders and purposes set by the personal data controller, in which case the responsibility for the personal data processing shall shift to the personal data processor.

In addition, the PDP Law neither clearly stipulates that a controller is required to enter into a written data processing agreement (“**DPA**”) with a processor nor what must be provided therein, unlike the GDPR. It can be, however, interpreted that a controller is required to enter into some written agreement with a processor to ensure that the processor processes personal data in accordance with instructions from the controller. Further, the DPA also is important proof of controller compliance, under Article 47 of the PDP Law, as the controller is required to be responsible for the data processing and to demonstrate accountability in fulfilling the obligations of implementing the personal data protection principles.

Applicability and Transitional Period

The PDP Law stipulates that it applies to every person, public agency, and international organization that processes personal data:

a. within the jurisdiction of the Republic of Indonesia; and/or

b. outside the jurisdiction of the Republic of Indonesia but with a legal consequence: (i) within the jurisdiction of the Republic of Indonesia; and/or (ii) on the personal data subjects of Indonesian citizens outside the jurisdiction of the Republic of Indonesia.

The framework of the requirements for extraterritorial application is different from that of the GDPR. It is determined based on whether there is a “legal consequence.” It is, however, unclear in the languages of the PDP Law what a legal consequence is and how to determine if one exists, a matter which will be at issue in practice without further guidelines. In addition, the PDP Law does not require appointment of a local representative even if it applies to an overseas entity, unlike the GDPR.

The PDP Law shall not apply to the processing of the personal data by individuals in personal or household activity.

Further exemptions apply for the processing of personal data for the following purposes, in the context of implementing the provisions of the law:

a. national defence and security interests;

b. law enforcement interests;

c. public interest in the context of state administration; or

d. in the interest of the supervision of the financial services sector, and monetary, payment system, and financial system stability carried out in the context of state administration.

The PDP Law does not provide any further explanation regarding the above exemptions.

The PDP Law has a transitional period of two years (from its enactment on 17 October 2022), within which all parties that do personal data processing must adjust their personal data processing practice in line with the PDP Law.

The term "personal data processing" is not defined in the PDP Law, but Article 16.1 of the PDP Law states that personal data processing includes acquisition and collection; filtering and analysis; retention; fixes and updates; display, announcement, transfer, dissemination, or disclosure; and/or deletion or destruction.

Principles of Personal Data Processing

As the general rule, based on the PDP Law, any personal data processing must be based on the following principles:[7]

a. personal data collection shall be limited and specific, legally valid, and transparent;
b. personal data processing shall be carried out in accordance with its purpose;
c. personal data processing shall be carried out by ensuring the rights of the personal data subject;
d. personal data processing shall be carried out in an accurate, complete, not misleading, up-to-date and accountable manner;
e. personal data processing shall be carried out by protecting the security of personal data from an unauthorized access, unauthorized disclosure, unauthorized alteration, misuse, destruction, and/or loss of personal data;
f. personal data processing shall be carried out by notifying the purpose and processing activities, as well as failure of personal data protection;
g. personal data shall be destroyed and/or deleted after the retention period ends or at the request of the personal data subject, unless otherwise stipulated by laws and regulations; and
h. personal data processing shall be carried out responsibly and can be clearly proven.

Lawful Basis for Personal Data Processing

Similar with the treatment in other countries, the PDP Law now recognizes lawful bases to process personal data **other than explicit consent** from the data subject which was the primary ground for personal data processing prior to the PDP Law, as follows:

a. Contract: fulfilment of agreement obligations in the event that the personal data subject is a party or to fulfil the request of the personal data subject at the time of entering into the agreement;
b. Legal obligation: fulfilment of the legal obligations of the personal data controller in accordance with the provisions of laws and regulations;
c. Vital interest: fulfilment of the protection of vital interests of the personal data subject;

[7] Article 16(2) of the PDP Law.

d. Public duty: carrying out duties in the context of public interest, public services, or exercising the authority of the personal data controller based on the laws and regulations; and/or
e. Legitimate interest: fulfilment of other legitimate interests by taking into account the purposes, needs, and balance of interests of the personal data controller and the rights of the personal data subject.

It is notable that processing under legitimate interests is allowed, as in the GDPR.

Privacy Notice

While terms like "data protection policy", "privacy notice", and "privacy policy" do not appear in the actual text of the PDP Law, it can be inferred from Article 21 that there is a requirement to notify data subjects of certain information. The PDP Law requires the following information to be provided to data subjects prior to processing personal data:[8]

a. legal justification for the processing;
b. the purpose of processing;
c. the type and relevance of the personal data to be processed;
d. the period for which documents containing personal data will be retained;
e. details about the information collected;
f. period of personal data processing; and
g. rights of the data subject.

The controller must keep data subjects updated in the event of any changes to the information above and provide data subjects with notice before any change occurs.

Forms of Personal Data Subject Explicit Consent

Under the PDP Law, collection of personal data processing consent must be carried out through written or recorded means and identified using clear Indonesian language in order to have legal force.

The PDP Law provides that the consent also may be submitted electronically or non-electronically.

Means of collecting consent that fail to meet the above requirements shall be declared null and void.

Furthermore, the PDP Law also stipulates that an agreement clause in which there is a request for personal data processing that does not contain the **explicit valid consent** of the personal data subject shall be declared null and void.

Rights of the Personal Data Subject

Based on the PDP Law, personal data subjects have the following principal rights towards their personal data:

a. the right to obtain information regarding identity clarity, basis of legal interest, purpose of requesting and using the personal data, and accountability of parties that request the personal data;
b. the right to complete, update and/or correct errors and/or inaccuracies in the personal data regarding themselves in accordance with the purpose of the personal data processing;

[8] Article 21(1) of the PDP Law.

c. the right to access and obtain a copy of personal data regarding themselves in accordance with the provisions of laws and regulations;
d. the right to end processing, delete, and/or destroy the personal data regarding themselves in accordance with the provisions of laws and regulations;
e. the right to withdraw consent to the processing of personal data regarding themselves that has been provided to the personal data controller;
f. the right to object to a decision-making action that is based solely on automated processing, including profiling, which has legal consequences or have a significant impact on the personal data subject;
g. the right to delay or limit the personal data processing proportionally with the purpose of personal data processing;
h. the right to sue and receive compensation for violations of the processing of the personal data regarding themselves in accordance with the provisions of laws and regulations;
i. the right to obtain and/or use the personal data regarding themselves from the personal data controller in a form that is in accordance with the structure and/or format commonly used or readable by an electronic system;
j. the right to use and send the personal data regarding themselves to other personal data controllers, insofar as the systems used can communicate with each other securely in accordance with the personal data protection principles under the PDP Law.

The exercise of personal data subject rights as referred to above shall be submitted through a registered application that is submitted electronically or non-electronically to the personal data controller.

Some of the personal data subject rights above, especially in points (c), (d), (e), (f), (i) and (j), shall be excluded for:

a. the interests of national defense and security;
b. the interests of law enforcement process;
c. the public interest in the context of state administration;
d. the interests of supervision of the sectors of financial services, monetary, payment system, and financial system stability carried out in the context of state administration; or
e. the interests of statistics and scientific research.

Aside from such exemptions, certain rights of data subjects can be refused by data controllers in certain circumstances. For example, Article 33 of the PDP Law provides that data controllers can refuse the request of a data subject to change their personal data, subject to the fulfilment of certain conditions.

Data Protection Impact Assessment

The personal data controller must assess the impact of personal data protection in the event that the personal data processing presents a potentially high risk for the personal data subject.

Personal data processing that has a potentially high risk as referred to above shall include:

a. automatic decision making that has legal consequences or significant impact on the personal data subject;
b. processing of specific personal data;
c. processing of the personal data on a large scale;
d. processing of the personal data for a systematic evaluation, scoring or monitoring of the personal data subject;

e. processing of the personal data for matching or combining a group of data;
f. use of new technologies in the personal data processing; and/or
g. personal data processing which limits the exercise of the rights of the personal data subject.

Further provisions on the DPIA are expected to be issued in a Government Regulation.

Data Protection Officer

Under the PDP Law, the personal data controller and the personal data processor must appoint officials or officers who carry out the personal data protection function in the event that:

a. the personal data are for the benefit of public services;
b. the core activities of the personal data controller have the nature, scope, and/or purposes that require regular and systematic monitoring of personal data on a large scale; and
c. the core activities of the personal data controller consist of personal data processing on a large scale for specific personal data and/or personal data related to crimes.

The PDP Law does not provide further elucidation of the above conditions.

The DPO at least shall have the following duties:

a. inform and provide advice to the personal data controller or the personal data processor in order to comply with the provisions of the PDP Law;
b. monitor and ensure compliance with the PDP Law and the policies of the personal data controller or personal data processor;
c. provide advice on assessing the impact of personal data protection and monitoring the performance of the personal data controller and the personal data processor; and
d. coordinate and act as a liaison for issues related to the processing of personal data.

The functions of a DPO are to be further regulated under a Government Regulation.

DPOs who carry out the personal data protection function shall be appointed based on professionalism, knowledge of the data protection law, personal data protection practice, and ability to fulfil their duties (there are no specific requirements of nationality, location or language skills at least in the language of the PDP Law) and the DPOs may come from within and/or outside the personal data controller or the personal data processor.

Do note that there is already a separate requirement to provide a contact point who can be contacted easily by data subjects as regards to the management of their personal data under Minister of Communication and Informatics ("**MOCI**") Regulation No. 20 of 2016 on the Protection of Personal Data in Electronic Systems.[9] This requirement still applies after the issuance of the PDP Law.

Transfer of Personal Data

The personal data controller may transfer personal data to other personal data controllers within the jurisdiction of the Republic of Indonesia.

[9] This requirement applies to any entity or person providing, managing, and/or operating an electronic system that functions to prepare, collect, process, analyse, store, display, announce, transmit, and/or disseminate electronic information (including personal data), known as an 'electronic system provider'.

Furthermore, the PDP Law also introduces a requirement where a data controller sending personal data overseas must ensure that the receiving nation of the personal data has a similar or higher level of personal data protection ("**Overseas Transfer Requirement**"). However, this requirement can be set aside if: (i) the sending data controller can ensure sufficient and binding personal data protection, or, if (i) cannot be fulfilled, (ii) there is consent from the data subject. It is understood that if the Overseas Transfer Requirement is already fulfilled, there is no need for the data controller to fulfill conditions (i) or (ii). Although the PDP Law does not clearly stipulate how data controllers can make sure that the receiving nation fulfils the Overseas Transfer Requirement or meet requirement (i) above, a written agreement between the sender and recipient, such as a Standard Contractual Clauses (SCC) under the GDPR, or a binding internal policy, such as a Binding Corporate Rules (BCR) under the GDPR, might be admitted as methods to fulfil requirement (i) (i.e., to ensure sufficient and binding personal data protection), which is up to the contents of further guidelines.

Further, do note the above overseas transfer requirement is an addition to the existing requirement of submitting certain reports to the MOCI about the transfer.

Data Breach Notification

Under the PDP Law, in the event of the failure of personal data protection, the personal data controller must provide a written notification by no later than 3 x 24 (three times twenty-four) hours to the personal data subject. Under the elucidation of Article 46 of the PDP Law, "failure of personal data protection" is defined as "failure to protect a person's Personal Data in terms of confidentiality, integrity, and availability of the personal data, including security breaches, whether intentional or unintentional, leading to destruction, loss, alteration, disclosure, or unauthorized access to the Personal Data which are being sent, stored or processed", similar to the GDPR. Therefore, this obligation seems to be wide in scope, adjustment of which is up to the contents of further guidelines. In addition, the same notice must be provided to the authorized agency responsible for supervising the implementation of personal data protection in Indonesia, which will be established by the President. Provisions on the procedures to inform the agency of this and other information will be established by a Government Regulation, which will be issued in the future.

This timing of notification is shorter than the previous regulation where the notification to the affected individual must be provided no later than 14 days after the discovery of such breach.

The PDP Law sets out that the written notification shall at least contain:

a. the disclosed personal data;
b. when and how the personal data were disclosed; and
c. efforts to handle and recover the disclosed personal data by the personal data controller.

In certain cases, for example, where the failure to protect personal data properly would interfere with public services and/or have a serious impact on the public interest, the personal data controller must notify the public of any failure to protect personal data (i.e., a data breach or leak).

Notification on a Corporate Action

Under the PDP Law, personal data controllers that intend to merge, consolidate, acquire, spin-off, or dissolve must notify the personal data subjects on the transfer of their personal data twice, i.e., before and after such corporate action.

The notification can be given either personally to each personal data subject or given through a newspaper announcement. There is no further provision on the notification, or the contents of the notification, though a further government regulation on this requirement is expected.

The implication of this requirement is that parties in, for example, a merger and acquisition transaction will need to pay more attention to personal data, and identify where the personal data will be transferred and who will have access to the personal data once the transaction is concluded.

Sanctions

The PDP Law introduces two types of sanctions, i.e., administrative sanctions and criminal sanctions.

Administrative sanctions will be imposed for violation of the data privacy related requirements, such as the lawful basis requirement, the corporate action announcement requirement, and the DPO appointment requirement. The administrative sanctions will include warning letters, temporary suspension of data processing activities, deletion of personal data, and/or administrative fines (the amounts of which are not yet determined).

Criminal sanctions are imposed for violation of any of the following prohibitions:

- Prohibition on unlawful collection of personal data, with an intention to benefit/enrich oneself or other parties, that causes losses to the data subject;
- Prohibition on unlawful disclosure of the personal data of others;
- Prohibition on unlawful use of the personal data of others.

Criminal sanctions take the form of a monetary penalty of Rp.4-6 billion and/or imprisonment of 4-6 years, depending on the crime.

In addition to the sanctions, additional punishments may be imposed in the form of confiscation of obtained profits and/or assets or proceeds from criminal acts and/or compulsory compensation payments.

In the event that the crimes are conducted by a corporation, the sentence may be imposed on the management, controller, commanding officer, beneficial owner, and/or corporation (only in the form of a fine).

The fine imposed on a corporation shall be a maximum of 10 (ten) times the maximum sentence imposed.

In addition to fines, corporations may be subject to additional sentences in the form of:

a. confiscation of profits and/or assets obtained or proceeds from crimes;
b. suspension of the entirety or part of the corporation's business;
c. permanent prohibition from conducting certain actions;
d. closure of the entirety or part of the corporation's place of business and/or activities;
e. fulfillment of the obligations that have been neglected;
f. payment of compensation;
g. revocation of license; and/or
h. dissolution of the corporation.

3. Actions to Consider

As stipulated in the PDP Law, implementing regulations will be issued to provide more clarity on some of its provisions.

For the time being, during the transitional period, companies whose business involves the processing of personal data may need to conduct an internal assessment to understand what adjustments may be necessary to comply with the PDP Law.

Public Relations Section, Nishimura & Asahi E-mail✉