Deloitte.

Hermawan Juniarto & Partners
Members of Deloitte Legal Network
Client Alert
July 2022

Client Alert July 2022
Data Protection Management and Technology Platform

Overview

Albeit the urgency of Indonesia to have a personal data protection, there is no specific laws and regulations relating to personal data protection until today. Provisions related to personal data protection are stipulated in various laws and regulations, including (i) Law No. 11 of 2008 on Electronic Information and Transaction as amended by Law No. 19 of 2016; (ii) Government Regulation No. 71 of 2019 on Administration of Electronic Transaction and System ("**GR 71/2019**"); (iii) Minister of Communication and Informatics Regulation No. 5 of 2020 on Private Electronic System Providers; (iv) Minister of Communication and Informatics Regulation No. 20 of 2016 on Personal Data Protection on Electronics System ("**MoCI Reg. 20/2016**").

MoCI Reg.20/2016 requires the collection of the data from the owner to observe the following rules:

a. The electronic system operator should obtain and collect the personal data based on the approval of the owner of the data when collecting the data; and
b. The personal data that was obtained and collected by the electronic system operator must be directly verified with the owner of the data. If obtained and collected indirectly, the personal data must be verified based on the result of processing from various resources.

The Indonesian Government is currently preparing a draft of the Personal Data Protection Law ("**PDP Bill**"), which specifically regulates on personal data protection to ensure that the personal data protection right can be effectively protected and guaranteed, as well as to encourage the growth of the digital economy and the information and communication technology industry, and to support the improvement of the competitiveness of the domestic industry. This PDP Bill will be drafted by taking into account the provisions under the EU General Data Protection Regulation 2016/679 which applicable as of May 2018 issued by the European Union ("**EU GDPR**").

The PDP Bill applies to every person, public entity, and organization or institution that carries out legal actions as regulated in the PDP Bill, both inside and outside the jurisdiction of the Republic of Indonesia which has legal consequences within the jurisdiction of the Republic of Indonesia and/or for Indonesian Data Owners outside the jurisdiction of the Republic of Indonesia.

A. Data Protection Management

1. General Overview on Personal Data

In the PDP Bill, personal data refers to any data regarding a person that is identified or may be identified (separately or combined with other information, both directly and indirectly through electronic and/or non-electronic systems. There are 2 (two) classifications of personal data:

a. General, which consists of: (i) full name; (ii) gender; (iii) nationality; (iv) religion; and/or (v) combined personal data used to identify someone.
b. Specific, which consists of: (i) health data and information; (ii) biometric data; (iii) genetics data; (iv) Life/sexual orientation; (v) political views; (vi) Criminal record; (vi) Children's data; (vii) Personal financial data; and/or (viii) Other data in accordance to the laws and regulations.

Every individual who has any personal data attached to him/her is defined as Data Owner. The PDP Bill provides 11 (eleven) rights to Data Owners including the right to access; request data processing/ usage information; complete; update/ correct; revoke consent; limit processing; delete data; refuse decision-making actions that are only based on automatic processing of a person's profile (profile creation); and sue for breaching personal data.

2. Key Principles on Data Governance

The key principles on Data Governance in the PDP Bill are as follows:

- Data Processing Principles
  1) Collection of Personal Data is limited and specifc, legally valid, appropriate and transparent.
  2) Processing of Personal Data is accurate, compete, not misleading, current, accountable and can be clearly proven; fit for purpose and failure to protect Personal Data; guarantee the rights of the data owner; and is done by protecting the security of personal data.
  3) Personal Data is destroyed and/or deleted after the retention period ends or at the request of the Data Owner

- Key Roles in Data Processing
  1) Data Controller is the party that determines the objectives and controls the processing of Personal Data;
  2) Data Processor is a party that processes Personal Data on behalf of the Personal Data Controller;
  3) Data Subject is an individual as a data subject who has Personal Data attached to it.

3. Data Storage

Under the GR 71/2019, personal data is prepared, collected, processed, analyzed, stored, displayed, announced, transmitted, and/or disseminated with a series of devices and electronic procedures called electronic system, which provided, managed and/ or operated by an Electronic System Provider ("**ESP**"), which categorized into the following categories.

a. ESP in the public sector, Government institutions and other agencies which are appointed by government institutions in order to organize electronic systems for them and on their behalf ("**Public ESP**"); and
b. ESP in private sector, Individuals (Indonesian or foreign citizens), business entities (incorporated or unincorporated), as well as any public entities which organize electronic systems ("**Private ESP**").

Public ESP must conduct management, processing and/ or retention of the Electronic System and Data Electronic in Indonesian territory. Meanwhile, Private ESP may conduct management, processing and/ or retention of the Electronic System and Data Electronic in Indonesian territory and/ or outside of Indonesian territory by ensuring the effectiveness of supervision by the Ministry or Body and law enforcement.

Nevertheless, a Public ESP may conduct its activities outside of the Indonesian territory in the event that the retention technology is not available domestically.

4. Data Acquisition and Data Exchange

In the current Indonesian personal data protection laws and regulations, especially the MoCI Reg. 20/2016, any personal data that managed by the Indonesian Data Processor may be transferred to outside the jurisdiction of the Republic of Indonesia with the following requirements:

a. Coordinate with the MoCI to carry out the transfer, by:
    i. Submitting a report on the implementation plan of the personal data transfer, which at least contain the information on the receiving country, the recipient identity, date of implementation, and the transfer purpose;
    ii. Requesting for advocacy (if necessary); and
    iii. Submitting a report on the transfer implementation.
b. Implement any applicable provisions under the Indonesian laws and regulations on the cross-border data transfer.

In the practice, the consent to any cross-border data transfer would be included at the initial consent request in the agreement between the Data Processor and the Data Owner on the data acquisition. Therefore, once the consent obtained from the Data Owner and the personal data has been acquired, the respective Data Processor may carry out a cross-border data transfer, either to any processor's affiliates or any other third-party data processor in other jurisdiction.

Unfortunately, the implementation of the compliance of the requirements under the MoCI Reg. 20/2016 is still quite low, considering that it is still a common case in Indonesia for a Data Processor to carry out a cross-border data transfer without coordinate with the MoCI. Up to the date, there is no further provision on the procedure of such coordination between MoCI and Data Processors, or any sanction on the unfulfillment of such requirements. Furthermore, in the current PDP Bill, Data Controllers may transfer their personal data to other Data Controller within or outside the jurisdiction of the Republic of Indonesia, but they shall obtain explicit consent from the respective Data Owner and the process shall be in accordance with the PDP Bill. In addition to cross-border data transfer, the Data Controllers may transfer their personal data in the following criteria:

a. The rate of personal data protection in the receiving country is equal or higher than the PDP Bill;
b. There is an international agreement between the countries;
c. There is a contract between the Data Controllers with personal data protection standard and/or guarantee in accordance to the PDP Bill;
d. Obtain explicit consent from the Data Owner.

Unlike the MoCI Reg. 20/2016, in the PDP Bill, there are administrative sanctions for the failure in the fulfillment of the criteria for a cross-border data transfer, which consist of:

a. Written warning (warning letters);
b. Temporary suspension of personal data processing activity;
c. Deletion or destruction of personal data;
d. Indemnification of losses; and/or
e. administrative fine.

It is advisable for any Data Owner to protect their personal data protection right with a proper and adequate data personal processing agreement to avoid any potential common fall, especially on the required pre-requisite approval to carry out a cross-border data transfer.

5. Data Retention

Data Processors shall hold into any personal data that processed by them for a certain period of time or retention period. Any personal data will be removed and/or annihilated after the retention period is over or based on the request from the respective Personal Data Owner unless regulated otherwise by the laws and regulations. The current PDP Bill does not set any retention period, however, in the Article 15 of the MoCI Reg. 20/2016, the minimum retention period of personal data is 5 (five) years. Any Electronic Systems Operator shall store the personal data within the retention period as of the date the respective Data Owner is no longer uses the electronic systems.

6. Cybersecurity Compliance

In the current Indonesian laws and regulations on personal data protection, there are potential administrative sanctions for any Electronic Service Providers that failure to comply with the provisions under the personal data protection in relation to the implementation of personal data protection in processing personal data, however the current Indonesian laws and regulations do not provide any criminal sanction on the violation of any provision or prohibition. Nevertheless, PDP Bill and every person who failure to comply with the following provisions will be subject to the imposition of the criminal sanctions, either imprisonment or fine:

a. Intentionally and unlawfully collect personal data that is not their own to give benefit to him/herself or others, or may result losses to the data owner;
b. Intentionally and unlawfully install and/or operate a visual data processing device in a public place or service facility that can threaten or violate the personal data protection;
c. Intentionally and unlawfully uses a visual data processing device installed in a public place and/or service facility to identify a person;
d. Intentionally falsifies personal data to benefit him/herself or others, or may cause harm to others;
e. Intentionally sells or buys personal data.

B. Data Protection Officer

1. The Importance of Data Protection Officer

In 2018, Data Protection Officer role ("**DPO**") was introduced by the EU GDPR to protect the personal data processing activities within the company, however, the current Indonesian personal data protection laws and regulations do not specifically recognize a DPO. Indonesia plan to introduce the role of DPO in the PDP Bill to mitigate any potential risk arises in the personal data protection practice. Any Data Controller, in the following events occur:

a. The personal data processing is for the interest of public services;
b. The main activities of the Data Controller involve a nature, scope and/or purpose that requires coordinated and systematic supervision on the personal data on a large scale;
c. The main activities of the Data Controller consist of large-scale personal data processing for specific personal data and/or personal data relating to criminal offences.

In the current PDP Bill, there are administrative sanctions for the failure to appoint a DPO which consist of:

a. written warning (warning letters);
b. temporary suspension of personal data processing activity;
c. deletion or destruction of personal data;
d. indemnification of losses; and/or
e. administrative fine.

2. Different Model of Data Protection Officer

Even though, the current Indonesian laws and regulations do not specifically recognize the role of DPO, the MoCI Reg. 20/2016 recognize a different role, where Electronic Service Providers must provide a contact person who can be easily contacted by any data owner(s) regarding the management of his/her personal data, so if the data owners want to access their personal data that managed by the Electronic System Providers, the Personal Owners may liaise the contact person. As a reference, the current Indonesian laws and regulations does not stipulate any specific provision on the role of contact person that appointed by the Electronic Service Provider.

3. Roles and Responsibilities of Data Protection Officer

For the purpose of personal data protection, DPO has following responsibilities set up in the PDP Bill:

a. Informing and providing advice to the data controller or processor to observe the provisions under the personal data protection law;
b. Supervising and ensuring compliance with the personal data protection law and the data controller or processor policy, including assignment, responsibility, improving of awareness and training for parties who are involved in personal data processing and relevant audits;

c. Providing advice regarding the assessment of personal data protection impact and supervising the performance of a data controller and processor; and
d. Coordinating and acting as the contact person for the issues related to personal data processing, including conducting consultations regarding the mitigation of risks and/or other matters.

4. Skill and Competency of Data Protection Officer

The Data Controller and the Data Processor must appoint a DPO based on professional quality, knowledge on laws and personal data protection practice, and the ability to perform their duty to protect the personal data. As a reference, the current PDP Bill does not specifically stipulate the provisions on the procedure for the appointment of DPO nor its specific technical requirements, however, further provisions regarding DPO will be stipulated in a Government Regulation upon the enactment of the PDP Bill.

5. Alignment of Data Protection Officer Roles to Other Function

The current PDP Bill does not regulate the specific provisions for the DPO and will be regulated in a governmental regulation as the implementation regulation of the PDP Bill. However, as reference, in the EU GDPR, DPO has an integral position or part in a organization, making them ideally placed to ensure compliance, so DPO should be able to perform their duties and responsibilities independently with following guarantees for their independences:

a. The DPO shall not receive any instructions regarding the performance of their duties;
b. There must not be a conflict of interest between the duties of the individual as a DPO and other duties (if any) and it is recommended that:
    i. the DPO should not also be a data controller of personal data processing activities;
    ii. the DPO should not be an employee, neither with short or fixed term contract;
    iii. the DPO should not report to a direct superior, rather than top management;
    iv. the DPO should have responsibility for managing their own budget.
c. The organization must offer staff and resources to support the DPO to carry out her duties;
d. The DPO should have the authority to investigate and the access to all personal data and data processing operations;
e. A minimum term of appointment and strict condition for dismissal must be set out by the organization for a DPO appointment.

6. Data Privacy Management

Upon the enactment of PDP Bill, every party that conduct personal data processing is obliged to comply their comply their personal data processing policy with the provisions under the PDP Bill within 2 (two) years period. It is advisable for the personal data processing party to consider to liaise with a relevant advisors to give some assistance during the transaction period, to:

a. Prepare the personal data processing framework as the guideline for the Company to comply with the provisions under PDP Bill;
b. Review and record the activities carried out by the Company relating to the personal data processing;
c. Review the existing personal data processing and protection policies within the company to ensure it covers all requirements under the PDP Bill;
d. Review the existing contracts and obtained consents from the Company's Clients relating to the personal data processing;
e. Provide assessment on the gap between the existing personal data processing and/or protection policies within the Company with the provisions under the PDP Bill;
f. Prepare strategy for the Client relating to the data retention.

For further information and/or inquiries related to this alert, you may contact:

Cornel B. Juniarto
Senior Partner
Hermawan Juniarto & Partners
Email: cbjuniarto@hjplaw-deloitte.com

Stefanus Brian Audyanto
Partner
Hermawan Juniarto & Partners
Email: saudyanto@hjplaw-deloitte.com

Maulana Syarif
Senior Managing Associate
Email: msyarif@hjplaw-deloitte.com

Hardy Salim
Senior Associate
Email: hsalim@hjplaw-deloitte.com