

What You Need to Know about the Personal Data Protection Law

Prepared by:

Andre Rahadian (Partner), Mika Isac Kriyasa (Partner), Peter Christopher (Senior Associate), Maharani Athina Nelwan (Associate) and Alma Almira (Associate)

The long-awaited Law No. 27 of 2022 concerning Personal Data Protection Law ("**PDP Law**") was finally ratified by the President of the Republic of Indonesia on 17 October 2022, and it is expected to become the umbrella legal framework for the protection and legal certainty of personal data in Indonesia. While the PDP Law strengthens the provisions of previous regulations on data processing and data transfers, it also introduces some widely recognized standard international concepts, such as data controllers, international cooperation, criminal sanctions, and so on, among which the PDP Law has incorporated the principles set forth in the European General Data Protection Regulation ("**GDPR**"). It contains 76 articles which are divided into 16 chapters. This article will focus on the following topics: (1) data processing, (2) personal data controllers and personal data processors, (3) data protection officers and (4) data transmission.

Scope of Personal Data Protection Law

Firstly, it is worth noting that the PDP Law applies to any person, public agency, or international organization that performs legal acts which may be located: (a) within the jurisdiction of the Republic of Indonesia and (ii) outside the jurisdiction of the Republic of Indonesia but having legal consequences within the jurisdiction of the Republic of Indonesia and/or for personal data subjects of Indonesian citizens located outside the jurisdiction of the Republic of Indonesia. This confirms that, similar to the validity of Law No. 11 of 2008 concerning Electronic Information and Transactions as amended by Law No. 19 of 2016, the PDP Law has extraterritorial application since it does not only apply to any person, public agency, or international organization within the Indonesian jurisdiction.

Personal Data Processing

Under the PDP Law, personal data processing must be carried out in accordance with the principle of personal data protection, which includes the requirements for personal data to be collected for a limited and specific, legally valid, and transparent purpose and processed in an accurate, complete, not misleading, up-to-date and accountable manner, in accordance with its purpose and guaranteeing the rights of the personal data subject. personal data must

be secured against unauthorized access, unauthorized disclosure, unauthorized alteration, misuse, destruction, and/or loss. Notice must be given of the purpose and existence of processing, as well as of failures in personal data protection. Further, personal data must 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 the personal data processing must be carried out in an accountable and clearly evidenced manner.

Personal Data Controller and Personal Data Processor

The PDP Law introduces new concepts which are influenced by the GDPR, namely: (a) Personal Data Controller; and (b) Personal Data Processor. In the GDPR, there is a clear distinction between a "data controller" and a "data processor" by which the GDPR aims to highlight that not all organizations participating in personal data processing bear the same level of responsibility. In essence, a data controller determines the purposes for which and the means by which personal data is processed while a data processor merely processes personal data on behalf of the controller.

The PDP Law mandates that the personal data controller must have a basis for the processing of personal data which includes the explicit valid consent of the personal data subject for one or more specific purposes which the personal data controller has notified to the personal data subject. The bases also include the fulfillment of contractual obligations if the personal data subject is one of the parties or at the request of the personal data subject at the time of entering into an agreement, the fulfillment of the legal obligations of the personal data controller under the prevailing regulations, the protection of the personal data subject's vital interest, the execution of duties in the public interest, public services or the implementation of the authority of the personal data controller based on the laws and/or the fulfillment of other legitimate interests subject to purposes and needs, and the balance between the interests of the personal data controller and rights of personal data subject.

Further, the PDP Law provides that, if a personal data controller appoints a personal data processor, the personal data processor must process personal data based on the personal data controller's instructions and carry out such instructions in compliance with the PDP Law. Personal data processing remains the responsibility of the personal data controller, and the personal data processor may involve other personal data processors in personal data processing; however, before involving other personal data processors, the personal data processor must obtain written approval from the personal data controller. A personal data processor is liable for any personal data processing carried out beyond the instructions and purposed determined by the personal data controller.

Data Breach Reporting

The personal data controller must notify (a) the personal data subjects and (b) the institution in writing of any failures in personal data protection no later than 3 x 24 (three times twenty-four) hours after they occur as required in Article 46 paragraph (1) of the PDP Law. The written notification must include at least the following information: (a) disclosed personal data; (b) when and how personal data was disclosed; and (c) efforts made by the personal data controller to manage and recover from the disclosure of personal data.

Further, as stated in Article 46 paragraph (3) of the PDP Law, the personal data controller is required to notify the public of a failure in personal data protection in certain circumstances. The elucidation of the PDP Law specifies that "in certain situations" means, among others, a failure in personal data protection interferes with public services and/or has a substantial impact on the public interest. However, it is still not clear who determines that such a notification ought to be made public.

In light of the aforementioned, the regulations prior to the PDP Law only required an electronic system owner to notify the affected personal data subjects within 14 (fourteen) days; however, there is no deadline for notifying the Minister of Communication and Informatics, only that it must be made immediately.

Data Protection Officer

Data Protection Officer ("DPO") is a concept widely referred to under the GDPR but was not explicitly adopted in the Indonesian personal data protection regulatory framework prior to the enactment of the PDP Law. The PDP Law introduces more stringent requirements regarding DPO whereby the personal data controller and personal data processor **must** appoint an official or person to perform the function of personal data protection, notably for the following circumstances as stated in Article 53 paragraph (1) of the PDP Law:

- a. personal data processing for the interest of public services;
- b. where the core activity of the personal data processor has a nature, scope, and/or objective that requires regular and systematic oversight for large-scale personal data; **and**
- c. the core activity of the personal data controller consists of large-scale personal data processing of specific personal data and/or personal data that is related to criminal activity.

Since the above provision uses the word "and," it is arguable as to what kind of business is required to appoint a DPO. Through a strict legal interpretation, the provision will limit the requirement to a specific type of business that is required to hire a DPO, making this clause not have the same meaning as it does in the GDPR.

Previously, the DPO was not explicitly adopted in the personal data protection regulatory framework; however, Ministry of Communications and Informatics Regulation Number 20 of 2016 on Personal Data Protection in Electronic Systems requires any Electronic System Organizer (PSE) to offer a contact person for the personal data owner in reference to the handling of its personal data. Such a 'contact person' may be considered a DPO, but in a less legal sense.

There is currently no further statutory qualification for a DPO. The PDP Law states that the DPO must be appointed based on professionalism, understanding of the law, personal data protection practice, and capacity to carry out the DPO's duties and the DPO may be appointed from within and/or outside the personal data controller or personal data processor. For this matter, this clause could be interpreted that only a person or firm which has legal/ qualifications

(has an advocate license or has a law degree) could be appointed as a DPO since the above criteria stipulate that appointment as the DPO would be based on their understanding of the law. Given the general qualifications of the DPO under the PDP Law, it is safe for us to say that the appointment of a legal practitioner or law firm would best suit the position. By appointing a law firm as their DPO, data controllers and processors can have a more efficient fee structure and will not need to manage another employee and deal with the implications of the employment law and its implementing regulations.

Personal Data Transmission

Data transmission in Indonesia is another critical feature regulated by the PDP Law. Previously, the regulations only covered the transmission of personal data from the Republic of Indonesia to outside the Republic of Indonesia in a rigid manner. Currently, the PDP Law specifies the circumstances under which personal data may be transmitted from the Republic of Indonesia to outside the Republic of Indonesia.

From the PDP Law perspective, the law asserts that the country of domicile of the personal data controller or the international organization receiving the personal data must have the same or a higher level of security for personal data protection as stipulated in Article 56 paragraph (2) of the PDP Law. If the country of domicile does not fulfil such conditions, the personal data controller must ensure that there is adequate and binding personal data protection as stated in Article 56 paragraph (3) of the PDP Law. If neither condition is satisfied, the personal data controller is required to obtain the consent of the data subjects.

Merger, Acquisition, Spinoff and Dissolution

The PDP Law also now specifies the conditions for personal data transmission when a company is going through a merger, acquisition, spinoff, and/or dissolution. This is a relatively new concept, as it was not covered by the regulations prior to the PDP Law. As stipulated in Article 48 paragraph (1) of the PDP Law, a personal data controller in the form of a legal entity that enters into a merger, acquisition, spinoff, or dissolution of a legal entity must submit a notification of the transfer of personal data to the personal data subject. Notification of the transfer of personal data must be given before and after the merger, acquisition, spinoff, or dissolution of a legal entity. If the personal data controller in the form of a legal entity dissolves or is dissolved, the storage, transfer, deletion, or destruction of personal data must be carried out in accordance with provisions of laws and regulations and notified to the personal data subject as stated in Article 48 paragraph (3) of the PDP Law. Further provisions on the notification procedure will be governed by a government regulation.

Following the implementation of the PDP Law, it is hoped that the Ministry of Communications and Informatics, in conjunction with private and public entities, will take the necessary steps to strengthen and provide opportunities to various stakeholders while maintaining personal data protection, building a digital culture, and taking advantage of the demographic bonus while empowering the Indonesian people in developing the digital world, and harmonizing regulations and increasing funding to advance innovation.

-oOo-

The article above was prepared by Dentons HPRP's lawyers

This publication is not intended to be a comprehensive review of all developments in the law and practice, or to cover all aspects of those referred to. Readers should take legal advice before applying the information contained in this publication to specific issues or transactions or matters. For more information, please contact us at dentons.hrp@dentons.com or Partners listed above.

No part of this publication may be reproduced by any process whatsoever without prior written permission from Hanafiah Ponggawa & Partners.