HHP Law Firm.

Client Alert

September 2022

Indonesia: The Personal Data Protection Law is Finally Here. What Does That Mean to Your Business?

In brief

The draft of the Indonesian Personal Data Protection Law ("**PDP Law**") was approved to become law (*Undang - Undang*) by the Indonesian Parliament (*Dewan Perwakilan Rakyat Republik Indonesia*) on 20 September 2022. With this approval, we are nearing the end of the process of an ambitious piece of legislation, which took several years to get approval. For several years, Indonesia has only relied on various diverse regulations that contain privacy provisions without one comprehensive umbrella law on personal data protection.

In this issue

The PDP Law is currently waiting to be passed by the President (when it will also be allocated a law number), and then issued to the public. Theoretically, if the President does not sign the PDP Law within 30 days after it is approved by the Indonesian Parliament, the PDP Law will automatically be enacted and will be in force.

Based on the latest draft PDP Law that is available on the Indonesian Parliament's website (as of 20 September 2022), the PDP Law will contain 16 chapters and 76 articles.

The government is hoping that the PDP Law can provide more certainty and clarity on personal data protection in Indonesia, with the intention to provide better protection to data subjects. But the PDP Law will also affect how businesses can process personal data.

Key takeaways

Status, Applicability and Transitional Period

As mentioned above, the PDP Law has been approved by the Indonesian Parliament but not yet enacted, and so it is not yet effective.

The latest draft PDP Law indicates that it will apply 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 of Indonesia.

The PDP Law will not apply to personal data processing by individuals on private or household matters. Unfortunately, there is no further elaboration on this, and we suspect this is something that can be stretched in practice. We will need to see how the authorities interpret and implement this in practice.

In addition, the PDP Law will have a transitional period of two years (after it is enacted), 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 latest draft. But Article 16.1 of the latest draft PDP Law states that personal data processing includes collecting, managing, analyzing, storing, revising, updating, displaying, announcing, transferring, disseminating, disclosing, deleting and destroying personal data, which effectively means any use of personal data.

As such, it can be assumed that the two-year transitional period applies to almost all of the provisions of the PDP Law. We will need to wait and see after the law is enacted whether any part or provision of the PDP Law is immediately enforced by the government despite the transitional period.

Adjustment to practices

Subject to the enacted PDP Law to be officially issued, some initial observations:

- *Controller vs processor*: The latest draft PDP Law introduces the concept of data controllers (i.e., the party that determines the purpose of personal data processing) and data processors (i.e., the party that processes personal data on behalf of a data controller). With the introduction of this concept, companies will need to be aware of their status in data processing activities, as this will impact the compliance requirements and liabilities.

  Under the latest draft PDP Law, a data controller is responsible for the processing of personal data by a data processor. While this is because the processing of personal data by a data processor is done based on instructions from a data controller, the flip side is companies that act as data controllers will need to be very careful in drafting a data processing agreement or a cooperation agreement that involves personal data processing with a data processor.

- *General vs Specific Personal Data:* In the latest draft PDP Law, personal data is categorized into general personal data and specific personal data. General personal data includes generic information, such as name, gender, nationality, religion and marital status. Specific personal data includes particular information such as health data, biometric data, genetic data, criminal records, and personal financial data.

  Despite the categorization of general and specific personal data, we have not yet seen any specific treatment that will be required for handling specific personal data. But if certain personal data is categorized as specific personal data, it could indicate that the processing of that personal data carries a high potential risk, which would require the data controller to prepare a data protection impact assessment. It could also indicate that the data controller and data processor are required to appoint a data protection officer.

- *Lawful Bases for Processing Personal Data*: The latest draft PDP Law recognizes lawful bases to process personal data other than explicit consent from the data subject, such as fulfillment of a contractual obligation, fulfillment of the data controller's legal obligation, protection of a data subject's vital interest, or fulfillment of a duty related to public interest or services.

  This is actually in line with the treatment in some other jurisdictions, where personal data processing is not solely based on consent, but there is room for flexibility in a contained environment, e.g., for implementing an obligation under an agreement or for decision making in urgent circumstances involving the life of a data subject.

- *Data protection impact assessment:* Data controllers that perform personal data processing with high potential risks must prepare a data protection impact assessment ("**DPIA**"). Personal data processing can be considered to possess high potential risks if it meets certain conditions. Those include automated decision making that could have a significant impact on the data subject, processing of specific personal data, large-scale personal data processing, or use of new technology for personal data processing.

  There is no elaboration on these conditions, and it may be unclear whether a condition is met, e.g., what would constitute large-scale personal data processing. The draft PDP Law also does not stipulate the minimum standard and format of the DPIA. We suspect these matters will be regulated in an implementing government regulation.

- *Data Protection Officer*: Certain data controllers and data processors are required to appoint a data protection officer who is responsible for ensuring data privacy compliance and mitigating the risk of data privacy breaches. This applies to data controllers and data processors that process personal data for the purpose of public service, those that have core activities that require systematic and orderly monitoring of large-scale personal data processing, and those that process specific personal data or criminal records.

  Data protection officers have the duty to advise on data privacy requirements and compliance, ensure the fulfillment of that compliance, advise on personal data protection impact assessment, and act as the data privacy liaison officer of the data controller or data processor.

  The latest draft PDP Law does not include a requirement for a data protection officer to be specifically certified. The draft law only mentions that a data protection officer is appointed based on, among other things, their professionalism, legal knowledge and capability in the area of data privacy practice. But it does state that further provisions on data protection officers, possibly including a certification requirement, will be set out in a government regulation. The latest draft PDP Law also allows the data protection officer position to be outsourced.

- *Offshore Transfer of Personal Data*: The requirements for transferring personal data outside of Indonesia have been surprisingly simplified compared to the 2020 version of the draft PDP Law.

  The latest draft PDP Law 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. 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.

  While it seems that the requirement to transfer personal data offshore has been simplified to a mere consent requirement, interestingly the latest draft PDP Law only uses the term "data controller", which might suggest that only data controllers are allowed to transfer personal data offshore.

- *Data breach notification:* Under the latest draft PDP Law, data controllers are now required to notify data breach incidents to the relevant data subject within three days, by informing about (i) the affected personal data that is disclosed; (ii) when and how the data is disclosed; and (iii) the data controllers' efforts to handle the incident. Apart from the data subject, the data controller must also notify the data protection authority - which will be established in the future as mandated by the draft PDP Law.

- *Announcement on a Corporate Action*: Data controllers that intend to do a merger, consolidation, acquisition, spin-off, or dissolution must notify data subjects on the transfer of their personal data twice, i.e., before and after the corporate action. The notification can be given either personally to each 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. As such, this notification can be given together with other required notifications (e.g., a newspaper announcement for an acquisition under the Indonesian Company Law).

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

Data Protection Authority

The Ministry of Communication and Informatics (*Kementerian Komunikasi dan Informatika*) is currently the supervisory authority on the operation of electronic system operators, including matters related to personal data protection compliance. But the latest draft PDP Law introduces a specific data protection authority, though it does not provide the name of the authority.

That data protection authority will be an institution established by the President by virtue of a Presidential regulation, and will report directly to the President.

The authority will have very broad duties and authorities, from drafting and stipulating policies and guidelines to imposing administrative sanctions. It is also possible that this authority will provide technical guidance on the implementation of the PDP Law, along with other data protection issues, in the future.

It is expected that the data protection authority will be established and stipulated by the President within the two-year transitional period. With the presidential election coming in early 2024, the stipulation of the data protection authority may be one of the last stipulations of President Joko Widodo or one of the first stipulations of the next President.

Sanctions

There are two types of sanctions under the latest draft PDP Law, i.e., administrative sanctions and criminal sanctions.

Administrative 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 data protection officer 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

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

- Prohibition to unlawfully collect personal data of others with an intention to benefit/enrich oneself or other parties that causes losses to the data subject
- Prohibition to unlawfully disclose personal data of others
- Prohibition to unlawfully use personal data of others

The criminal sanctions are in the form of a monetary penalty of IDR 4-6 billion and/or imprisonment of 4-6 years, depending on the crime.

In addition, there are extra provisions if the crime is conducted by an entity, i.e.,:

- Criminal sanctions can be imposed on the management, the controller, the instructor or the beneficial owner of the entity, and/or on the entity itself - note that the entity can only be imposed with a monetary penalty.
- The monetary penalty will be 10 times the amount stated above.
- In addition to the monetary penalty, additional criminal sanctions can be imposed such as seizure of profits/gains, freezing of business, permanent prohibition of certain acts, closure of business, revocation of license and/or dissolution of the entity.

Actions to Consider

Considering the PDP Law only provides an umbrella regulatory framework that contains general rules on data protection, we expect further implementing regulations will be issued to provide more clarity on some provisions in the PDP Law, particularly on how to determine the amount of administative penalties for violation of the data protection provisions in the PDP Law (as no formula is provided in the latest draft PDP Law).

For the time being, businesses should monitor the enactment of the PDP Law and conduct internal assessments to understand what adjustments may be necessary to comply with the PDP Law. But businesses can take comfort from the two-year transitional period provided for all parties to comply with the data processing activity provisions in the PDP Law.

Contact Us

Daniel Pardede
Senior Partner
Daniel.pardede@bakermckenzie.com

Adhika Wiyoso
Associate Partner
Adhika.wiyoso@bakermckenzie.com

Wiku Anindito
Associate Partner
Wiku.anindito@bakermckenzie.com

Bimo Harimahesa
Senior Associate
Bimo.harimahesa@bakermckenzie.com

Bratara Damanik
Associate
Bratara.damanik@bakermckenzie.com

Devinka Adira
Associate
Devinka.adira@bakermckenzie.com