Data. Protection. Adding Value.

Personal Data Protection Law - Indonesia

Legislation

Law No. 27 of 2022 on Personal Data Protection ("**PDP Law**") has been enacted by the Indonesian government on 17 October 2022. Following the effective enforcement of the PDP Law, personal data controllers, personal data processors, and other parties that conduct personal data processing were granted a two-year transition period to ensure compliance with the provisions of the PDP Law. The transition period ended on 17 October 2024.

Scope: PDP Law applies to every person, public agency and international organization that performs legal acts as regulated in the PDP Law:

- **located within the Indonesian territory; and**
- **located outside the Indonesian territory,** which has a legal consequences within the jurisdiction of Indonesia and/or personal data subject which are Indonesian citizens outside the jurisdiction of Indonesia.

Exemptions: PDP Law does not apply to the processing of personal data by individuals in personal or household.

Risk Level: High

Enforcement

Enforcement: The enforcement of PDP Law encompasses administrative and criminal sanctions. Administrative sanction which shall be in the form of a written reprimand, temporary suspension of personal data processing activities, erasure or removal of personal data, and/or administrative fines up to a maximum of 2% of annual revenue. Regarding criminal sanctions, the PDP Law stipulates a maximum imprisonment of 6 years and/or a maximum fine of IDR 6 billion, depending on the prohibited actions.

Criminal sanctions also may be imposed towards corporations which may include but is not limited to suspension of all or part of corporation's business and permanent prohibition on certain activities.

Personal Data Protection Principles

PDP Law emphasizes the **principles of personal data protection** that needs to be upheld during personal data processing, which are:

- personal data collection shall be conducted in a limited and specific manner, and be legally valid and transparent;
- personal data processing shall be conducted in accordance with its purpose;
- personal data processing shall be carried out by ensuring the rights of personal data subject;
- personal data processing shall be conducted accurately, completely, not misleading, up to date, and accountable manner;
- personal data processing shall be conducted by protecting the security of personal data from unauthorized access, unauthorized disclosure, unauthorized alteration, misuse, destruction, and/or loss of personal data;
- personal data processing shall be carried out by notifying the purpose and processing activities, as well as failure of personal data protection;
- personal data shall be destroyed and/or deleted after the retention period ends or based on the request of the personal data subject, unless otherwise specified by laws and regulations; and
- personal data processing shall be carried out responsibly and be clearly proven.

Supervisory Authority

Supervisory Authority: As of July 2025, Indonesia has yet to establish a data protection supervisory authority as mandated by the PDP Law. The supervisory authority role is currently held by the Ministry of Digital Communication to facilitate the transition to a designated data protection authority that will be established. Furthermore, relevant authorities, including the Indonesian Financial Services Authority (*Otoritas Jasa Keuangan* or OJK), have played a significant role in supervising the implementation of data protection through a sectoral approach. One of the key measures undertaken by the OJK is the enactment of OJK Regulation (POJK) No. 22 of 2023 concerning Consumer and Community Protection in the Financial Services Sector, which requires Financial Services Business Actor (*Pelaku Usaha Jasa Keuangan or PUJK*) to ensure the implementation of personal data protection in the financial services sector.

Registration/Approval Requirements: The PDP Law does not stipulate any requirements to register or to obtain approval from the supervisory authority in terms of processing personal data.

Personal Data Processing

Legal Basis for Processing: The processing of personal data shall be conducted with a basis for processing data, which are:

- an explicit valid consent from personal data subjects;
- fulfillment of contractual obligations in the event the personal data subject is a party or to fulfil the request of the personal data subject;
- fulfillment of legal obligation;
- fulfillment of the protection of vital interests of the personal data subject;
- carrying out duties in the context of public interest, public services, or exercising the authority of the personal data controller based on laws and regulation; and/or
- fulfillment of other legitimate interests by considering the purposes, needs, and balance of interests of the personal data controller and the rights of the personal data subject.

Types of Personal Data: PDP Law categorizes personal data into two types which are general and specific personal data. Specific personal data are personal data in which the processing can result in a greater impact towards personal data subject. Examples of general personal data are full name, gender, religion, whereas examples of specific personal data are biometric data and personal financial data.

Exemptions: There are several exemptions to a personal data subject's rights and personal data controller's obligations, which include but is not limited to personal data processing for the interests of national defence and security.

pwc

Personal Data Subject Rights

The PDP Law outlines the **rights of personal data subjects**, emphasizing the importance of safeguarding individuals' rights and ensuring their control over their own personal data which includes:

- right to obtain information regarding identity clarity, basis of legal interest, purpose of requesting and using personal data, and accountability of parties that request personal data;
- right to complete, update and/or correct errors and/or inaccuracies;
- right to access and obtain a copy of their personal data;
- right to end processing, delete, and/or destroy their personal data;
- right to withdraw consent to the processing of their personal data;
- right to object a decision-making action that is based solely on automated processing which has legal consequences or have a significant impact;
- right to delay or limit the personal data;
- right to sue and receive compensation for violations of the processing;
- right to obtain and/or use their personal data in a form that is in accordance with the structure and/or format commonly used or readable by an electronic system; and
- right to use and send their personal data, as long as the system used can communicate with each other securely.

Security & Data Breaches

Personal data breach included under the concept of personal data protection failure under the PDP Law which is defined as a failure to protect person's personal data in terms of confidentiality, integrity, and availability of personal data including security breaches. In the event of such a personal data protection failure, the personal data controller must provide a written notification within 3 x 24 hours to the personal data subject and data protection supervisory authority.

Other Business Obligations

Data Protection Officer: The PDP Law requires personal data controllers and personal data processors to appoint a data protection officer(s) if:

- the personal data processing is for public service purposes;
- 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/or
- the core activities of the personal data controller consist of the personal data processing on a large scale for specific personal data and/or personal data related to crimes.

Record of Processing Activities: The PDP Law mandates that personal data controllers shall record all personal data processing activities.

Data Protection Impact Assessment: Personal data controllers must assess the impact of personal data protection if the personal data processing has a high-risk potential to the personal data subject. High-risk processing includes processing activities that may include but is not limited to those which include automatic decision-making and/or processing for systemic evaluation, scoring or monitoring of personal data subject.

Cross-Border Transfers

Transfer of personal data outside the jurisdiction of the Republic of Indonesia: The PDP Law requires the transferring personal data controller to ensure that the country of domicile of the party receiving the personal data has personal data protection level that is equal or higher than the standard as regulated in the PDP Law. In absence of the protection, the personal data controller is required to ensure that there is an adequate and binding personal data protection. If neither condition is met, prior consent shall be obtained from the personal data subject to conduct the transfer.

Localization Requirements: There are no localization requirements under the PDP Law.

To Watch

Currently, Indonesia does not have implementing regulations for the PDP Law. Furthermore, we expect the implementing regulations and the personal data protection supervisory authority to be established in 2025.

Let's connect to discuss how we can help:

Indra Allen
Legal Partner,
PwC Legal Indonesia
indra.allen@pwc.com

Roro Astuti
Legal Senior Manager,
PwC Legal Indonesia
roro.astuti@pwc.com

Sultan Buruni
Legal Senior Manager,
PwC Legal Indonesia
sultan.buruni@pwc.com

Gery Fathurrachman
Legal Senior Manager,
PwC Legal Indonesia
gery.fathurrachman@pwc.com

Putu Putra
Legal Manager,
PwC Legal Indonesia
putu.putra@pwc.com

RITM8650648