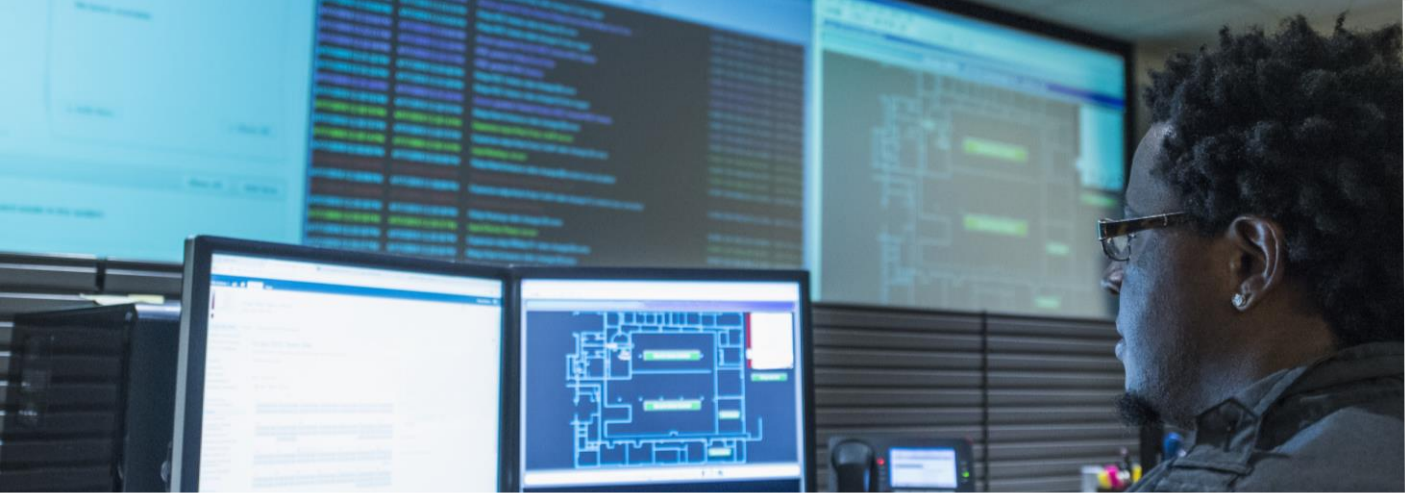

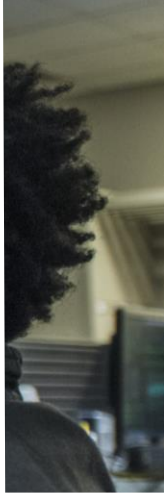

Digital Trust NewsFlash

PwC Digital Services / October 2022 / No. 05

Indonesian Personal Data Protection Law [P1]

Indonesian Personal Data Protection Law

The Indonesian Personal Data Protection (PDP) Law has been ratified by President Joko Widodo on 17 October 2022 and listed as *UU No. 27 tahun 2022* regarding Personal Data Protection, referred to herein as the "UU PDP".

The UU PDP aims to provide guidelines on personal data processing and obligations of data controller and processors in protecting personal data in order to uphold the data subject rights. In addition, the presence of data protection authority (*kelembagaan*) is now stipulated, which was previously undefined in the 2019 bill.

What's in the UU PDP?

New Provisions and Adjustments

The House of Representatives (DPR) published the PDP bill on 6 December 2019, which was then adjusted and republished on 5 September 2022 and 20 September 2022. Some key differences/additions of provisions in the UU PDP ratified on 17 October 2022 compared to the initial draft, are:

a. **Consent** includes provisions for **children** and **people with disabilities**. *(Ref: Articles 25-26)*
b. **Data protection impact analysis (DPIA)** must be performed for personal data with **high-risk criteria**. *(Ref: Article 34)*
c. **Administrative fine** is a **maximum of 2% of the annual revenue** for the violation variable. *(Ref: Article 57)*

Personal Data Protection

The UU PDP applies to every person, public body, and international organisations that carry out legal actions in the jurisdiction of the Republic of Indonesia or outside the jurisdiction of the Republic of Indonesia which has legal consequences in Indonesia or for Indonesian citizen data subjects. *(Ref: Article 2)*

Several general terms in the UU PDP were introduced as follows:

a. **Personal data** is information that relates to an **identified or identifiable** individual (natural person/data subject), who can be identified, directly or indirectly, combined or stand alone, electronic or non-electronic. The UU PDP classified personal data as 2 types which are:
    1. **General data:** name, nationality, marriage, gender, religion, etc.

2. **Specific data:** health records, biometric data, genetic data, criminal records, children data, financial data, etc.

b. **Data Protection Authority or Authority/*Lembaga*** is the national body established to be responsible for upholding the rights of individuals to the protection of their personal data through the enforcement and monitoring of compliance with local data privacy laws.

c. **Data Controller** is defined as any person, public body, or international organisation that acts individually or jointly in determining the purpose of data processing and performing control over data processing activities.
A data controller must **perform** the following:
   1. Lawfulness, fairness and transparency of data processing. *(Ref: Article 27)*
   2. Data processing according to purpose. *(Ref: Article 28)*
   3. Accuracy, completeness, and consistency of data through verification. *(Ref: Article 29)*

d. **Data Processor** is defined as any person, public body, and international organisation acting individually or jointly in processing personal data on behalf of the Data Controller.

e. **Data Protection Officer (DPO)** is mandatory for organisations that fulfil one of the following criteria *(Ref: Article 53)*:
   1. Processing personal data for public interests.
   2. Data controller's main activities involve the continuous and systematic monitoring of personal data on a large scale.
   3. Data controller's main activities involve processing specific personal data or personal data related to criminal data.

   DPO must be appointed based on professionalism, knowledge of the law, personal data protection practices, and ability to fulfill their duties.
   DPO can be appointed from internal data controller/data processor or external parties. At the minimum, obligations of DPO are to *(Ref: Article 54)*:
   1. Inform and advise data controller/data processor for the compliance with the UU PDP.
   2. Monitor and ensure the compliance of UU PDP and data controller/data processor policies.
   3. Provide advice to the DPIA and monitor the performance of the data controller/data processor.
   4. Coordinate and act as a liaison for issues related to data processing.

f. **Data Subject or Individual** is defined as the person to whom the personal data relates. The rights of data subject as defined in the UU PDP articles 5-13 are:
   1. The right to be informed;
   2. The right to rectification;
   3. The right of access;
   4. The right to erasure;
   5. The right to restrict of processing;
   6. Rights in relation to automated decision making and profiling;
   7. The right to object;
   8. The right to claim compensation; and
   9. The right to data portability.

Personal Data Processing

Personal data processing includes the activity of collecting, storing, processing, transferring, updating, and destroying personal data. According to article 20, processing personal data must have a **legal basis,** which are:

a. Explicit consent from data subject in a form of electronic or non-electronic documentation is required, including agreement clause that consists of personal data processing request, such as:
   1. Processing **children's data** requires **consent from the holder of parental responsibility over the child** or **guardian**. *(Ref: Article 25)*
   2. Processing **people with disabilities' data** requires consent from the **data subject** or **guardian**. *(Ref: Article 26)*

b. Fulfillment of a contract
c. Legitimate Interest
d. Vital Interest
e. Legal Requirement
f. Public Interest

In addition, personal data protection principles must be upheld in processing personal data. The principles are: *(Ref: Article 16)*

a. Lawfulness, fairness and transparency
b. Purpose limitation
c. Data minimisation
d. Accuracy
e. Storage limitation
f. Integrity and confidentiality
g. Accountability

While processing personal data, the **data controller is obliged to maintain records of all personal data processing activities (ROPA).** *(Ref: Article 31)*

Data Breach (Failure to Protect)

When a breach occurs, it needs to be reported within 3 x 24 hours in the form of written notice, notifying the related data subjects and authority. However, in some cases, the data controller is also obliged to notify the public regarding the data breach. The written notice must at least include the following details:

a. What personal data that has been breached
b. When the breach occurred
c. How the breach occurred
d. What remedial actions are taken.

(Ref: Article 46)

Obligations of Data Controller

The UU PDP article 21 states that in gaining consent from a data subject, the data controller must inform the privacy notice of legality of data processing, purpose of data processing, type and relevancy of personal data to be processed, retention period, information collected, period of data processing, and data subject rights. Should there be any changes to the privacy notice, the data controller must notify the data subject in advance.

a. The data controller must **complete** the following activities within **3 x 24 hours** from when the data controller receives the request from data subject:
    1. To rectify personal data according to the data subject's request. *(Ref: Article 30)*
    2. To grant access to personal data processed and its historical records. *(Ref: Article 32)*
    3. To stop data processing activities. *(Ref: Article 40)*
    4. To postpone and restrict data processing activities. *(Ref: Article 41)*
b. The data controller must **stop** data processing activities when:
    1. The retention period has been reached;
    2. The purpose of data processing has been fulfilled; or
    3. The data subject objects to the processing. *(Ref: Article 42)*
c. The data controller must **erase** personal data when:
    1. Personal Data is no longer needed to fulfil the processing purpose;
    2. The data subject withdraws consent;
    3. The data subject objects to the processing pursuant; or
    4. Personal data have been unlawfully collected/processed. *(Ref: Article 43)*
d. The data controller must **destroy** personal data when:
    1. The retention period has been reached and required to be disposed;
    2. The data subject objects to the processing pursuant;
    3. Personal data is not involved in any legal case settlement process; or
    4. Personal data is collected against the law. *(Ref: Article 44)*

Derogations of data controllers' obligations apply to national defence and security, law enforcement, public interest and financial services authority interest for the purpose of state administration. *(Ref: Article 50)*

Personal Data Transfer (Cross-Border)

The transfer of personal data is allowed with the following conditions:

a. **Within** the Legal Territory of the Republic of Indonesia, as regulated in the UU PDP. *(Ref: Article 55)*
b. **Outside** the Legal Territory of the Republic of Indonesia, with the following provisions *(Ref: Article 56)*:
    1. Ensure that the country of domicile of the data controller or data processor receiving the data has a personal data protection level that is equal to or higher than UU PDP; or
    2. Ensure that there is adequate personal data protection and such protection is binding in nature; or
    3. Personal data subject's consent regarding the data transfer has been obtained.

Data Protection Impact Assessment (DPIA)

Data controllers shall uphold personal data protection principles in personal data processing activities and should any condition potentially **raise the risk towards a data subject, data controllers are required to perform a DPIA**. The high risk criteria are described as follows *(Ref: Article 34)*:

a. Automated decision-making
b. Specific data processing
c. Large scale data processing
d. Systematic monitoring
e. Data matching
f. Innovative technology
g. Denial of service

For Considerations

At the minimum, the following activities need to be performed in order to comply with the UU PDP:

No	Area	Definition	High Level Regulatory Reference
1	**Privacy Governance**	• Formalise privacy strategy • Formalise privacy governance structure, e.g. DPO office • Appoint Data Protection Officer (DPO)	• UU PDP chapter VI on Data Controller's and Data Processor's Obligations • UU PDP articles 53-54 on DPO
2	**Policy Management**	• Formalise Privacy Policy • Data Protection Impact Analysis (DPIA)	• UU PDP chapter IV on Data Subject's rights • UU PDP chapter V on Personal Data Processing • UU PDP article 34 on DPIA
3	**Cross border data strategy**	• Establish cross border data privacy processes	• UU PDP chapter VII on Cross Border Data Transfer
4	**Data Lifecycle Management**	• Establish Data Lifecycle documentation / • Records of Processing Activities (ROPA) • Update data retention policy	• UU PDP chapter V on Personal Data Processing • UU PDP chapter VI part 2 on Data Controller's Obligations • UU PDP article 31 on ROPA • UU PDP articles 42 - 45 on data retention and erasure

No	Area	Definition	High Level Regulatory Reference
5	**Data Subject Rights**	• Establish data subject rights processes • Establish consent management processes • Implement consent management tool (when applicable)	• UU PDP chapter IV on Data Subject's rights
6	**Information Security**	• Formalise data protection program • Enhance third party risk assessments • Update information security policies • Implement data protection tools	• UU PDP articles 35-37, 39 on information security
7	**Incident Management**	• Strengthen incident management response and breach management capabilities	• UU PDP article 46 on reporting on data breach
8	**Data Processor Accountability**	• Improve third party management • Update third party contracts	• UU PDP chapter VI part 3 on Data Processor's Obligations
9	**Training and Awareness**	• Establish data privacy training and awareness	• UU PDP article 63 on awareness and socialisation

Understanding the purpose of collecting and processing personal data is the most important aspect for organisations to accomplish. Compliance with privacy laws cannot be left solely to the legal and compliance departments. To comply with the UU PDP, everyone in the organisation must understand their responsibility to protect personal data. Every company and foreign organisation that process (which includes collecting, storing, and transferring) personal data of Indonesian citizens will be impacted and required to comply with the UU PDP.

Transition Period

Data controller, data processor, and other parties related to personal data processing activities must comply with the UU PDP **since the ratification of the law (17 October 2022) with a maximum of 2 years given as transition period**, all provisions of laws and regulations governing the protection of personal data, are declared valid as long as they do not conflict with the provisions of the UU PDP.

Sanctions

Non-compliance with the requirements of this regulation may result in written warnings, financial sanctions such as **criminal fines to individuals up to Rp 6 billion and corporations up to Rp 60 billion, administrative fine for corporations is a maximum of 2% of the annual annual revenue for the violation variable, imprisonment up to 6 years**, temporary suspension of activities, and dissolution of the corporation.

Your PwC Indonesia Contacts:

Subianto
Broader Assurance Services Leader
Chief Digital & Technology Officer
subianto.subianto@pwc.com

Indra Allen
Legal Partner
indra.allen@pwc.com

Richard Ticoalu
Risk Assurance Partner
Richard.ticoalu@pwc.com

Jeffry Kusnadi
Cybersecurity & Technology Director
jeffry.kusnadi@pwc.com

Andrew Tirtadjaja
Cybersecurity & Privacy Director
andrew.tirtadjaja@pwc.com

Roro Astuti
Legal Senior Manager
roro.astuti@pwc.com

Beatrix Ariane
Cybersecurity & Privacy Director
beatrix.b.ariane@pwc.com

Yusri Amsal
Cybersecurity & Technology Senior Manager
yusri.amsal@pwc.com

Ricky Riswanto
Cybersecurity & Technology Senior Manager
ricky.riswanto@pwc.com

www.pwc.com/id

PwC Indonesia

@PwC_Indonesia

pwc