



Digital Trust NewsFlash

PwC Digital Services / October 2023 / No. 7

Draft of Implementing Regulation of Law Number 27, 2022 Regarding Personal Data Protection

Draft of Implementing Regulation of Law Number 27, 2022 Regarding Personal Data Protection

Introduction

The Personal Data Protection (PDP) Law, ratified on 17 October 2022, establishes the fundamental principles and framework for data protection, but also acknowledges the need for a more detailed and practical guide for its implementation. To bridge this gap, the draft Implementing Regulation of Law Number 27, 2022 regarding Personal Data Protection (“RPP PDP”) was developed. The RPP PDP provides additional clarity to navigate the intricacies of the PDP Law and offers several more detailed prerequisites regarding Personal Data Protection.

Key Topics Covered in RPP PDP

Privacy Governance

Controllers are required to monitor and govern Personal Data processing activities performed under their control, including those from other parties. To do so, RPP PDP states that Controllers should have a:

1. **Personal Data Protection Policy**, commonly known as a Privacy Policy, is an internal policy Controllers must have. The policy should cover at a minimum a processing policy and audit policy.
2. **Data Protection Agreements**, outlining the obligations and responsibilities of each party relating to Personal Data Protection.
3. **Reporting Channels for Suspected Violations** for the public in case of suspected violations during the processing of Personal Data by Processors.

Data Protection Agreements

In line with prevailing PDP Law, the RPP PDP stipulates that the Controller can appoint Processors to conduct processing activities in accordance with the purpose as determined by the Controller. However, the responsibilities of the Controllers remain under the Controller.

To ensure the adequacy of protection and clear division of roles and responsibilities between parties in Personal Data controlling and processing activities, the RPP PDP stipulates the minimum content of all such agreements – both between Joint Controllers and Controller and Processor.

Agreement between Controller and Processors	Agreement between Joint Controllers
<p>Controllers can appoint Processors to conduct processing activities in accordance with the purpose as determined by the Controller. The responsibilities of the Controllers remain under the Controller.</p>	<p>Joint Controllers are jointly responsible (<i>bertanggung jawab hukum secara tanggung renteng</i>) as Controller for the processing of Personal Data.</p>
<p>The agreement should at the very least contain:</p> <ul style="list-style-type: none"> A. The scope of processing activities performed by the Processor on behalf of the Controller; B. The procedures on how the Personal Data is being processed; C. The type and purpose of processing Personal Data; D. The type of Personal Data processed; E. Categories of Personal Data Subjects; F. Processing time period; G. The rights and obligations of the Controller and Processor; H. The supervision, audit, and inspection mechanism; I. Dispute resolution; J. Involvement of other Processor, if any; and K. Appointment of a jointly appointed contact person with regards to processing activities. 	<p>The agreement should at the very least contain:</p> <ul style="list-style-type: none"> A. Legal basis for processing the Personal Data of each Controller; B. Relationship between the purpose of processing the Personal Data controlled by each Controller; C. Information regarding the agreement on how to process the Personal Data; D. Division of roles and responsibilities for the fulfilment of legal obligations under the applicable laws and regulations; and E. Jointly appointed contact person.

Data Protection Officer (DPO)

The RPP PDP introduces an array of pivotal DPO requirements and expectations for both Controllers and Processors. Controllers and Processors, in general, should provide a DPO with necessary resources, ensure their objectiveness, and seek their advice in matters relating to Personal Data Protection.

Privacy Impact Assessments

Privacy Impact Assessments (PIA) serve as tools to ensure processing is both necessary and accompanied by effective risk mitigation measures. Within the RPP PDP, additional PIA requirements for Controllers are:

1. **Legitimate Interest Assessments (LIA)** for using Legitimate Interest as a Legal Basis.
2. **Transfer Impact Assessment (TIA)** for cross border data transfers. Detailed guidelines for this assessment will be provided in the regulations of the Personal Data Protection Authority (PDP Authority).
3. **Data Protection Impact Assessment (DPIA)** before doing potentially high-risk processing activities. The RPP PDP describes minimum items that should be included in the assessment.

All of these assessments must be documented. Additionally, Data Protection Officer (DPO) should be consulted for impact assessments.

Privacy by Design

In the development of systems, services, products, as well as during Personal Data processing, Controllers must:

1. **Implement Privacy by Design** by performing risk assessment and implementing organisational and technical measures (e.g. encryption and pseudonymisation, regular testing) in the development and during processing, use of system, or providing products/services to fulfil Personal Data Protection principles.
2. **Data minimisation by default**, implement measures to ensure personal data is processed to what is specifically needed to achieve the purpose.

Data Accuracy and Retention

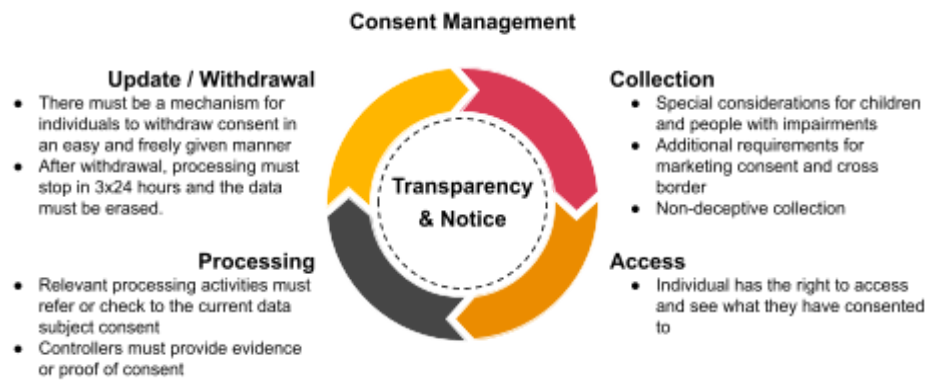
Controllers should ensure data accuracy and completeness by establishing quality standards and mechanisms. Controllers should take proportionate measures to ensure accuracy, determine retention period and policies, and define mechanisms to securely erase and destroy data.

Privacy Incident Management

Controllers need to mitigate personal data breaches by creating a privacy incident management process. This should cover planning, where Controllers must create policies and plans, and implement measures to mitigate or minimise the risk of personal data breaches. In handling and post-incident, Controllers must ensure the notification mechanism is defined, perform post-incident analysis, and create lessons learned for improvements.

Consent Collection and Management

Amongst the six legal basis specified in PDP Law, consent needs to be managed as Data Subjects have the right to change and withdraw their consent, even more so in marketing consent as these have new requirements under RPP PDP.



Claim Over Compensation

Data Subjects have the right to submit a claim and receive compensation for damages due to violations, either based on fault or negligence of a Controller in processing the Personal Data of Data Subjects. The request for compensation for the violation may be submitted by providing evidence of the violation, information regarding damage suffered, proof of processing, and information and evidence of failure to protect Personal Data.

There are two types of compensation based on the RPP PDP, namely material and immaterial compensation. Material compensation occurs by giving a certain amount of money with a value equivalent to the loss suffered due to processing activities, and immaterial compensation occurs in the form of recovery measures to restore conditions prior to the violation.





Cross-Border Data Transfer

Controllers are permitted to transfer Personal Data to other Controllers and/or Processors outside the territory of the Republic of Indonesia. It is to be noted that the Controller transferring the Personal Data has the obligation to ensure that the country of the receiving entity has Personal Data Protection at a level that is equal or higher than that of the PDP Law (which will be further regulated in the implementing regulation of the PDP Law that is still being prepared by the Government of Indonesia). Where the level of Personal Data Protection is lower than the level of the PDP Law, then the Controller must ensure there is adequate and binding Personal Data Protection, or must obtain explicit and express consent from the Data Subject (owner).

Personal Data Protection Authority (PDP Authority)

The RPP PDP stipulates further regarding the Personal Data Protection Authority which is responsible for implementing Personal Data protection in the Republic of Indonesia. In doing so, under the RPP PDP, the Personal Data Protection Authority has the following authorities and responsibilities:

PDP Authority Responsibilities and Authorities

 Policy Maker <ul style="list-style-type: none">• Formulate and establish PDP policies	 Dispute Resolution Facilitator <ul style="list-style-type: none">• Facilitate dispute resolution to PDP matters outside of court• Request legal assistance from the prosecutors' office for dispute resolution
 Supervisory <ul style="list-style-type: none">• Monitor PDP compliance• Conduct compliance assessment for transfer outside Indonesia• Give orders to controllers/processors in regards to supervision• Publish result of supervision• Receive complains and/or reports regarding violation allegations• Conduct inspection and search against violation allegations	 Enforcement <ul style="list-style-type: none">• Impose administrative sanctions• Assist law enforcement in handling PDP offense• Cooperate with international PDP agencies to resolve violation allegations• Summon and present parties related to violation allegations• Request information, data, and documents in regards to violation allegations• Summon and present necessary experts in examination and investigations

Dispute Resolution and Administrative Sanctions

The Data Subject, Controller, and/or Processor may submit a report regarding a dispute either electronically or non-electronically to the PDP Authority. Upon verifying the information provided, the PDP Authority will attempt to resolve the dispute by prioritising mediation. The PDP Authority is authorised to impose administrative sanctions in various forms. The sanctions imposed vary based on several factors, including but not limited to transparency and cooperativeness during the investigation. Entities that cooperate, share information transparently, and engage constructively during investigations may face milder sanctions.

Key Takeaway & What You Need To Do

RPP PDP sets forth a lot of detailed prerequisites regarding Personal Data Protection provisioned in the PDP Law. Though there may be a lot of things to go through, to prepare your organisation in Personal Data Protection implementation and compliance, **you must have the team to perform your privacy programme**. Based on the DPO requirements, determine if you need to appoint a DPO and while developing the DPO function, you may prepare a task force team (consisting of Risk, Legal, Compliance, and IT Security) to understand your organisation's end-to-end business process and how personal data processing activities are conducted in your organisation to identify gaps (gap assessment). Moreover, you must be aware of what personal data is processed and its data flow within and outside your organisation. **You may leverage the identified gap results in your business process and your understanding of data as your current state identification to further prepare the implementation areas** such as, identified high-risk processing to prepare DPIA, identified cross-border transfer to prepare TIA, identified consent as legal basis to prepare consent management, among others.

This publication is only intended to give an overview of several provisions in the RPP PDP dated on 31 August 2023. It does not cover all requirements and provisions. Please do not hesitate to contact us if you need more detailed advice or have specific questions.

Your PwC Indonesia Contacts:

Subianto

Broader Assurance Leader,
Chief Digital and Technology Officer
subianto.subianto@pwc.com

Indra Allen

Legal Partner
indra.allen@pwc.com

Richard Ticoalu

Risk Assurance Partner
richard.ticoalu@pwc.com

Beatrix Ariane

Cybersecurity and Privacy Director
beatrix.b.ariane@pwc.com

Andrew Tirtadjaja

Cybersecurity and Privacy Director
andrew.tirtadjaja@pwc.com

Hengky Antony

Data and Analytics Director
hengky.antony@pwc.com

Jeffry Kusnadi

Cybersecurity and Technology Director
jeffry.kusnadi@pwc.com

Roro Astuti

Legal Senior Managing Associate
roro.astuti@pwc.com

www.pwc.com/id



PwC Indonesia



@PwC_Indonesia

This publication has been prepared for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, PwC, its members, employees and agents do not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.

The documents, or information obtained from PwC, must not be made available or copied, in whole or in part, to any other persons/parties without our prior written permission which we may, at our discretion, grant, withhold or grant subject to conditions (including conditions as to legal responsibility or absence thereof).

PwC Indonesia is comprised of KAP Tanudiredja, Wibisana, Rintis & Rekan, PT PricewaterhouseCoopers Indonesia Advisory, PT Prima Wahana Caraka, PT PricewaterhouseCoopers Consulting Indonesia, and PwC Legal Indonesia, each of which is a separate legal entity and all of which together constitute the Indonesian member firm of the PwC global network, which is collectively referred to as PwC Indonesia.

© 2023 PwC. All rights reserved.

PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see <http://www.pwc.com/structure> for further details.