

UNOFFICIAL ENGLISH TRANSLATION

Law No 27 of 2022

Personal Data Protection

This unofficial English translation is provided for reference. The Indonesian text prevails. This document is not a sworn or certified translation.

Includes the enacted text and its Elucidation. This edition follows the supplied 2022 text and is not a consolidated statement of subsequent amendments or court decisions.

legaltrans.id

Edited and formatted English edition

LAW OF THE REPUBLIC OF INDONESIA NUMBER 27 OF 2022
ON THE PROTECTION OF PERSONAL DATA
BY THE GRACE OF ALMIGHTY GOD, THE PRESIDENT OF THE REPUBLIC OF
INDONESIA,

Whereas

- a. that the protection of personal data is a fundamental human right that forms part of the right to personal security; therefore, a legal basis is necessary to ensure the security of personal data, in accordance with the 1945 Constitution of the Republic of Indonesia;
- b. that the protection of personal data is intended to guarantee citizens' right to personal protection, foster public awareness, and ensure recognition of and respect for the importance of personal data protection;
- c. that regulations concerning personal data are currently scattered across various laws and regulations; therefore, to enhance the effectiveness of implementing personal data protection, it is necessary to establish regulations regarding personal data protection in a single law;
- d. whereas, based on the considerations referred to in subparagraphs (a), (b), and (c), it is necessary to enact a Law on Personal Data Protection;

Having regard to: Article 5(1), Article 20, Article 28G(1), Article 28H(4), and Article 28J of the 1945 Constitution of the Republic of Indonesia;

By Mutual Agreement

THE HOUSE OF REPRESENTATIVES OF THE REPUBLIC OF INDONESIA

and

THE PRESIDENT OF THE REPUBLIC OF INDONESIA
HAVE DECIDED:

To Enact

A LAW ON PERSONAL DATA PROTECTION.

CHAPTER I
GENERAL PROVISIONS

Article 1

For the purposes of this Act, the following terms shall have the following meanings:

1. Personal Data means data regarding an individual who is identified or can be identified, either individually or in combination with other information, either directly or indirectly, through electronic or non-electronic systems.
2. Personal Data Protection means all efforts to protect Personal Data throughout the processing of Personal Data in order to guarantee the constitutional rights of the data subject.
3. Information means details, statements, ideas, and signs that contain value, meaning, and messages - whether data, facts, or their explanations - that can be seen, heard, or read, presented in various

forms and formats in accordance with developments in information and communication technology, whether electronic or non-electronic.

4. A Personal Data Controller is any individual, public body, or international organization that, acting alone or jointly with others, determines the purposes of and exercises control over the processing of Personal Data.
5. A Personal Data Processor is any individual, public body, or international organization that acts individually or jointly in processing Personal Data on behalf of the Personal Data Controller.
6. A Data Subject is an individual to whom Personal Data pertains.
7. "Any Person" means a natural person or a corporation.
8. A corporation is a well-organized group of people and/or assets, whether incorporated or unincorporated.
9. State institutions are executive, legislative, and judicial bodies, and other bodies whose primary functions and duties relate to the administration of the state, and whose funding is derived in part or in full from the State Budget and/or the Regional Budget, or non-governmental organizations provided that their funding is derived in part or in full from the State Budget and/or the Regional Budget, public donations, and/or foreign sources.
10. An international organization is an organization recognized as a subject of international law and possessing the capacity to enter into international agreements.
11. The Central Government, hereinafter referred to as the Government, is the President of the Republic of Indonesia who holds the executive power of the Republic of Indonesia as referred to in the 1945 Constitution of the Republic of Indonesia.

Article 2

- (1) This Law applies to every person, public entity, and international organization that performs legal acts as regulated in this Law:
 - a. within the jurisdiction of the Republic of Indonesia; and
 - b. outside the jurisdiction of the Republic of Indonesia, which have legal consequences:
 1. within the jurisdiction of the Republic of Indonesia; and/or
 2. for Indonesian citizens who are Data Subjects outside the jurisdiction of the Republic of Indonesia.
- (2) This Law does not apply to the processing of Personal Data by individuals in the course of personal or household activities.

CHAPTER II

PRINCIPLES

Article 3

This Law is based on:

- a. protection;
- b. legal certainty;

- c. the public interest;
- d. benefit;
- e. prudence;
- f. balance;
- g. accountability; and
- h. confidentiality.

CHAPTER III

TYPES OF PERSONAL DATA

Article 4

- (1) Personal Data consists of:
- a. Personal data of a specific nature; and
 - b. General personal data.
- (2) Specific Personal Data as referred to in paragraph (1)(a) includes:
- a. health data and information;
 - b. biometric data;
 - c. genetic data;
 - d. criminal records;
 - e. data on children;
 - f. personal financial data; and/or
 - g. other data as provided for by applicable laws and regulations.
- (3) General Personal Data as referred to in paragraph (1)(b) includes:
- a. full name;
 - b. gender;
 - c. nationality;
 - d. religion;
 - e. marital status; and/or
 - f. Personal Data combined to identify an individual.

CHAPTER IV

RIGHTS OF DATA SUBJECTS

Article 5

A Data Subject has the right to obtain information regarding the clarity of identity, the legal basis, the purpose of the request and use of Personal Data, and the accountability of the party requesting the Personal Data.

Article 6

The Data Subject has the right to supplement, update, and/or correct errors and/or inaccuracies in their Personal Data in accordance with the purposes of Personal Data processing.

Article 7

The Data Subject has the right to access and obtain a copy of the Personal Data concerning him or her in accordance with the provisions of laws and regulations.

Article 8

The Data Subject has the right to terminate the processing, delete, and/or destroy Personal Data concerning him or her in accordance with the provisions of laws and regulations.

Article 9

The Data Subject has the right to withdraw consent for the processing of Personal Data concerning him or her that has been given to the Data Controller.

Article 10

- (1) The Data Subject has the right to object to decision-making actions based solely on automated processing, including profiling, that result in legal consequences or have a significant impact on the Data Subject.
- (2) Further provisions regarding the filing of objections to automated processing as referred to in paragraph (1) are set forth in a Government Regulation.

Article 11

The Data Subject has the right to suspend or restrict the processing of Personal Data in a manner proportionate to the purpose of the processing of Personal Data.

Article 12

- (1) A Data Subject has the right to file a lawsuit and receive compensation for violations of the processing of Personal Data concerning him or her in accordance with the provisions of laws and regulations.
- (2) Further provisions regarding violations of Personal Data processing and the procedures for awarding compensation as referred to in paragraph (1) are regulated in a Government Regulation.

Article 13

- (1) A Data Subject has the right to obtain and/or use Personal Data concerning him or her from the Personal Data Controller in a form consistent with commonly used structures and/or formats or in a format readable by an electronic system.
- (2) The Data Subject has the right to use and transmit Personal Data concerning him or her to another Personal Data Controller, provided that the systems used can communicate securely with one another in accordance with the principles of Personal Data Protection under this Act.
- (3) Further provisions regarding the rights of Data Subjects to use and transmit Personal Data as referred to in paragraph (2) are regulated in a Government Regulation.

Article 14

The exercise of the rights of the Data Subject as referred to in Articles 6 through 11 shall be submitted through a recorded request delivered electronically or non-electronically to the Data Controller.

Article 15

- (1) The rights of Data Subjects as referred to in Article 8, Article 9, Article 10(1), Article 11, and Article 13(1) and (2) are exempted for:
 - a. matters of national defense and security;
 - b. the interests of law enforcement;
 - c. the public interest in the context of state administration;
 - d. the interests of oversight of the financial services sector, monetary policy, payment systems, and financial system stability carried out in the context of state administration; or
 - e. statistical and scientific research purposes.
- (2) The exceptions referred to in paragraph (1) shall be implemented solely for the purpose of enforcing the provisions of this Act.

CHAPTER V

PROCESSING OF PERSONAL DATA

Article 16

- (1) The processing of personal data includes:
 - a. acquisition and collection;
 - b. processing and analysis;
 - c. storage;
 - d. correction and updating;
 - e. display, publication, transfer, dissemination, or disclosure; and/or
 - f. deletion or destruction.
- (2) The processing of Personal Data as referred to in paragraph (1) shall be conducted in accordance with the principles of Personal Data Protection, including:
 - a. the collection of Personal Data is limited and specific, legally valid, and transparent;
 - b. the processing of Personal Data is carried out in accordance with its purpose;
 - c. the processing of Personal Data is carried out in a manner that guarantees the rights of the Data Subject;
 - d. the processing of Personal Data is carried out accurately, completely, without being misleading, up-to-date, and in a manner that can be accounted for;
 - e. the processing of Personal Data is carried out by protecting its security from unauthorized access, unauthorized disclosure, unauthorized alteration, misuse, destruction, and/or loss;
 - f. the processing of Personal Data is carried out by notifying the Data Subject of its purposes and activities, as well as any Failure of Personal Data Protection;

- g. Personal Data is destroyed and/or deleted after the retention period expires or upon request by the Data Subject, unless otherwise specified by law; and
 - h. the processing of Personal Data is carried out responsibly and can be clearly substantiated.
- (3) Further provisions regarding the implementation of the processing of Personal Data as referred to in paragraph (1) are regulated in a Government Regulation.

Article 17

- (1) The installation of visual data processing or analysis devices in public places and/or at public service facilities shall be subject to the following conditions:
- a. for the purposes of security, disaster prevention, and/or traffic management or the collection, analysis, and regulation of traffic information;
 - b. the information must be displayed in the area where the visual data processing or analysis devices have been installed; and
 - c. they must not be used to identify individuals.
- (2) The provisions referred to in paragraph (1)(b) and (c) are exempted for the prevention of criminal acts and law enforcement processes in accordance with the provisions of laws and regulations.

Article 18

- (1) The processing of Personal Data may be carried out by 2 (two) or more Personal Data Controllers.
- (2) In the event that the processing of Personal Data is carried out by 2 (two) or more Personal Data Controllers, the following minimum requirements must be met:
- a. there is an agreement among the Data Controllers that sets forth the roles, responsibilities, and relationships among the Data Controllers;
 - b. there must be mutually related purposes and jointly determined methods for the processing of Personal Data; and
 - c. there is a jointly designated point of contact.

CHAPTER VI

OBLIGATIONS OF PERSONAL DATA CONTROLLERS AND PERSONAL DATA PROCESSORS IN THE PROCESSING OF PERSONAL DATA

Section One: General Provisions

Article 19

Personal Data Controllers and Personal Data Processors include:

- a. Any Person;
- b. Public Entities; and
- c. International Organizations.

Part Two: Obligations of Personal Data Controllers

Article 20

- (1) A Personal Data Controller must have a legal basis for processing Personal Data.
- (2) The legal basis for the processing of Personal Data as referred to in paragraph (1) includes:
 - a. explicit and valid consent from the Data Subject for one (1) or more specific purposes that have been communicated by the Data Controller to the Data Subject;
 - b. fulfillment of contractual obligations where the Data Subject is a party to the agreement or to fulfill the Data Subject's request at the time of entering into the agreement;
 - c. compliance with the legal obligations of the Personal Data Controller in accordance with the provisions of laws and regulations;
 - d. protection of the vital interests of the Data Subject;
 - e. the performance of duties in the public interest, the provision of public services, or the exercise of the Personal Data Controller's authority as provided by law; and/or
 - f. fulfilling other legitimate interests while taking into account the purposes, needs, and balance of interests between the Personal Data Controller and the rights of the Data Subject.

Article 21

- (1) When processing Personal Data based on consent as referred to in Article 20(2)(a), the Personal Data Controller must provide information regarding:
 - a. the legality of the processing of Personal Data;
 - b. the purpose of processing Personal Data;
 - c. the types and relevance of the Personal Data to be processed;
 - d. the retention period for documents containing Personal Data;
 - e. Details regarding the information collected;
 - f. the duration of Personal Data processing; and
 - g. the rights of the Data Subject.
- (2) In the event of a change in the information referred to in paragraph (1), the Personal Data Controller is required to notify the Data Subject prior to the change in the information.

Article 22

- (1) Consent to the processing of Personal Data is given through written or recorded consent.
- (2) The consent referred to in paragraph (1) may be provided electronically or non-electronically.
- (3) The consent referred to in paragraph (1) has the same legal effect.
- (4) In the event that the consent referred to in paragraph (1) includes other purposes, the request for consent must meet the following requirement:
 - a. be clearly distinguishable from other matters;
 - b. be presented in a format that is understandable and easily accessible; and
 - c. use simple and clear language.

- (5) Any consent that does not meet the requirements referred to in paragraphs (1) and (4) shall be null and void.

Article 23

Any agreement containing a request for the processing of Personal Data that does not include the explicit and valid consent of the Data Subject shall be null and void.

Article 24

When processing Personal Data, the Personal Data Controller must provide evidence of the consent given by the Data Subject.

Article 25

- (1) The processing of children's Personal Data shall be conducted in a special manner.
- (2) The processing of a child's Personal Data as referred to in paragraph (1) must obtain consent from the child's parents and/or legal guardian in accordance with the provisions of applicable laws and regulations.

Article 26

- (1) The processing of Personal Data of persons with disabilities shall be conducted in a special manner.
- (2) The processing of Personal Data of persons with disabilities as referred to in paragraph (1) shall be carried out through communication using specific methods in accordance with the provisions of laws and regulations.
- (3) The processing of Personal Data of persons with disabilities as referred to in paragraph (2) must obtain consent from the person with a disability and/or the person's guardian in accordance with the provisions of applicable laws and regulations.

Article 27

The Personal Data Controller is required to process Personal Data in a limited and specific manner that is legally valid and transparent.

Article 28

A Personal Data Controller must process Personal Data in accordance with the purpose of such processing.

Article 29

- (1) The Personal Data Controller must ensure the accuracy, completeness, and consistency of Personal Data in accordance with the provisions of laws and regulations.
- (2) In ensuring the accuracy, completeness, and consistency of Personal Data as referred to in paragraph (1), the Personal Data Controller is required to conduct verification.

Article 30

- (1) The Personal Data Controller shall update and/or correct errors and/or inaccuracies in Personal Data no later than 3 x 24 (three times twenty-four) hours from the time the Personal Data Controller receives a request for the update and/or correction of Personal Data.

- (2) The Personal Data Controller must notify the Data Subject of any updates and/or corrections to the Personal Data.

Article 31

The Personal Data Controller is required to keep records of all Personal Data processing activities.

Article 32

- (1) The Personal Data Controller is required to provide the Data Subject with access to the processed Personal Data along with the audit trail of the Personal Data processing in accordance with the retention period for Personal Data.
- (2) The access referred to in paragraph (1) shall be granted no later than 3 x 24 (three times twenty-four) hours from the time the Personal Data Controller receives the access request.

Article 33

The Personal Data Controller is obligated to refuse to grant access to or allow changes to Personal Data to the Data Subject in the following cases:

- a. it endangers the safety, physical health, or mental health of the Data Subject and/or others;
- b. it would result in the disclosure of another person's Personal Data; and/or
- c. contradict national defense and security interests.

Article 34

- (1) The Personal Data Controller is required to conduct a Personal Data Protection Impact Assessment if the processing of Personal Data poses a high potential risk to the Data Subject.
- (2) The processing of Personal Data that poses a high potential risk as referred to in paragraph (1) includes:
 - a. automated decision-making that has legal consequences or a significant impact on Data Subjects;
 - b. the processing of specific types of Personal Data;
 - c. large-scale processing of Personal Data;
 - d. the processing of Personal Data for systematic evaluation, scoring, or monitoring of Data Subjects;
 - e. processing of Personal Data for activities matching or merging a group of data;
 - f. the use of new technologies in the processing of Personal Data; and/or
 - g. the processing of Personal Data that restricts the exercise of the rights of the Data Subject.
- (3) Further provisions regarding Personal Data Protection impact assessments are set forth in a Government Regulation.

Article 35

A Personal Data Controller is required to protect and ensure the security of the Personal Data it processes by:

- a. the development and implementation of technical and operational measures to protect Personal Data from any processing of Personal Data that violates applicable laws and regulations; and

- b. determining the level of security for Personal Data by taking into account the nature and risks of the Personal Data that must be protected during the processing of Personal Data.

Article 36

In processing Personal Data, the Personal Data Controller is obligated to maintain the confidentiality of Personal Data.

Article 37

The Personal Data Controller is required to supervise every party involved in the processing of Personal Data under the control of the Personal Data Controller.

Article 38

The Personal Data Controller is required to protect Personal Data from unlawful processing.

Article 39

- (1) The Personal Data Controller shall prevent unauthorized access to Personal Data.
- (2) The prevention referred to in paragraph (1) shall be carried out by using a security system for the Personal Data being processed and/or by processing Personal Data using an electronic system in a reliable, secure, and responsible manner.
- (3) The prevention referred to in paragraph (2) shall be carried out in accordance with the provisions of laws and regulations.

Article 40

- (1) The Personal Data Controller is required to cease the processing of Personal Data in the event that the Data Subject withdraws consent for the processing of Personal Data.
- (2) The cessation of the processing of Personal Data as referred to in paragraph (1) shall be carried out no later than 3 x 24 (three times twenty-four) hours from the time the Personal Data Controller receives the request to withdraw consent for the processing of Personal Data.

Article 41

- (1) The Personal Data Controller is required to suspend and restrict the processing of Personal Data, either in part or in full, no later than 3 x 24 (three times twenty-four) hours from the time the Personal Data Controller receives a request to suspend and restrict the processing of Personal Data.
- (2) The suspension and restriction of the processing of Personal Data as referred to in paragraph (1) shall not apply in the following cases:
 - a. there are provisions in laws and regulations that do not permit the suspension and restriction of the processing of Personal Data;
 - b. it may endanger the safety of others; and/or
 - c. the Data Subject is bound by a written agreement with the Personal Data Controller that does not permit the suspension or restriction of the processing of Personal Data.
- (3) The Personal Data Controller is required to notify the Data Subject that the suspension and restriction of the processing of Personal Data have been implemented.

Article 42

- (1) The Personal Data Controller is required to cease processing Personal Data in the following cases:
- a. the retention period has expired;
 - b. the purpose of processing the Personal Data has been achieved; or
 - c. there is a request from the Data Subject.
- (2) The termination of the processing of Personal Data as referred to in paragraph (1) shall be carried out in accordance with the provisions of laws and regulations.

Article 43

- (1) The Personal Data Controller is required to delete Personal Data in the following cases:
- a. the Personal Data is no longer necessary to achieve the purposes of processing Personal Data;
 - b. The Data Subject has withdrawn consent for the processing of Personal Data;
 - c. there is a request from the Data Subject; or
 - d. the Personal Data was obtained and/or processed in violation of the law.
- (2) The erasure of Personal Data as referred to in paragraph (1) shall be carried out in accordance with the provisions of laws and regulations.

Article 44

- (1) The Personal Data Controller is required to destroy Personal Data in the following cases:
- a. the retention period has expired and it is specified that the data shall be destroyed based on the records retention schedule;
 - b. there is a request from the Data Subject;
 - c. is not related to the resolution of a legal proceeding; and/or
 - d. the Personal Data was obtained and/or processed unlawfully.
- (2) The destruction of Personal Data as referred to in paragraph (1) shall be carried out in accordance with the provisions of laws and regulations.

Article 45

The Personal Data Controller is required to notify the Data Subject of the deletion and/or destruction of Personal Data.

Article 46

- (1) In the event of a Personal Data breach, the Personal Data Controller is required to provide written notification no later than 3 x 24 (three times twenty-four) hours to:
- a. the Data Subject; and
 - b. the relevant authority.
- (2) The written notification referred to in paragraph (1) must at a minimum include:
- a. the Personal Data that was disclosed;
 - b. when and how the Personal Data was disclosed; and

- c. measures taken by the Personal Data Controller to address and remedy the disclosure of Personal Data.
- (3) In certain cases, the Personal Data Controller is required to notify the public of a Personal Data Protection breach.

Article 47

The Personal Data Controller shall be responsible for the processing of Personal Data and shall demonstrate accountability in fulfilling the obligations to implement the principles of Personal Data Protection.

Article 48

- (1) A Personal Data Controller in the form of a legal entity that undergoes a merger, demerger, acquisition, consolidation, or dissolution must notify the Data Subject of the transfer of Personal Data.
- (2) The notification of the transfer of Personal Data as referred to in paragraph (1) shall be provided before and after a merger, demerger, acquisition, consolidation, or dissolution of a legal entity.
- (3) In the event that a Personal Data Controller in the form of a legal entity dissolves or is dissolved, the storage, transfer, deletion, or destruction of Personal Data shall be carried out in accordance with the provisions of applicable laws and regulations.
- (4) The storage, transfer, deletion, or destruction of Personal Data as referred to in paragraph (3) shall be notified to the Data Subject.
- (5) Further provisions regarding the procedures for notification as referred to in paragraphs (1), (2), and (4) are regulated in a Government Regulation.

Article 49

The Personal Data Controller and/or Personal Data Processor shall comply with the directives of the relevant agency in the implementation of Personal Data Protection in accordance with this Act.

Article 50

- (1) The obligations of the Personal Data Controller as referred to in Article 30, Article 32, Article 36, Article 42, Article 43 paragraph (1) letters a through c, Article 44 paragraph (1) letter b, Article 45, and Article 46 paragraph (1) letter a, are exempted for:
 - a. matters of national defense and security;
 - b. the interests of law enforcement;
 - c. the public interest in the context of state administration; or
 - d. the interests of supervision of the financial services, monetary, and payment systems sectors, and financial system stability, carried out in the context of the administration of the state.
- (2) The exceptions referred to in paragraph (1) shall be implemented solely for the purpose of enforcing the provisions of the Act.

Part Three: Obligations of Personal Data Processors

Article 51

- (1) In the event that a Personal Data Controller appoints a Personal Data Processor, the Personal Data Processor shall process Personal Data in accordance with the instructions of the Personal Data Controller.
- (2) The processing of Personal Data as referred to in paragraph (1) shall be carried out in accordance with the provisions set forth in this Act.
- (3) The processing of Personal Data as referred to in paragraph (1) falls under the responsibility of the Personal Data Controller.
- (4) A Personal Data Processor may engage another Personal Data Processor to process Personal Data.
- (5) A Personal Data Processor must obtain written consent from the Personal Data Controller before engaging another Personal Data Processor as referred to in paragraph (4).
- (6) In the event that a Personal Data Processor processes Personal Data beyond the instructions and purposes established by the Personal Data Controller, the processing of Personal Data becomes the responsibility of the Personal Data Processor.

Article 52

The provisions regarding the obligations of the Personal Data Controller as referred to in Articles 29, 31, 35, 36, 37, 38, and 39 also apply to the Personal Data Processor.

Part Four

Officials or Officers Performing Personal Data Protection Functions

Article 53

- (1) Personal Data Controllers and Personal Data Processors are required to appoint officials or staff members to perform personal data protection functions in the following matters:
 - a. the processing of Personal Data for the purposes of public service;
 - b. the core activities of the Personal Data Controller have a nature, scope, and/or purpose that require regular and systematic monitoring of Personal Data on a large scale; and
 - c. the core activities of the Personal Data Controller consist of the processing of Personal Data on a large scale involving specific types of Personal Data and/or Personal Data related to criminal offenses.
- (2) Officials or staff members who perform the Personal Data Protection functions referred to in paragraph (1) shall be appointed based on their professionalism, knowledge of the law and Personal Data Protection practices, and ability to fulfill their duties.
- (3) Officials or staff who carry out the Personal Data Protection functions referred to in paragraph (2) may come from within and/or outside the Personal Data Controller or Personal Data Processor.

Article 54

- (1) Officials or staff members who perform personal data protection functions shall have the following minimum duties:

- a. inform and advise the Personal Data Controller or Personal Data Processor to comply with the provisions of this Act;
 - b. monitor and ensure compliance with this Act and the policies of the Personal Data Controller or Personal Data Processor;
 - c. provide advice on Personal Data Protection impact assessments and monitor the performance of the Personal Data Controller and the Personal Data Processor; and
 - d. coordinate and act as a point of contact for issues related to the processing of Personal Data.
- (2) In carrying out the duties referred to in paragraph (1), officials or officers performing Personal Data Protection functions shall take into account the risks associated with the processing of Personal Data, considering the nature, scope, context, and purpose of the processing.
- (3) Further provisions regarding officials or staff members who perform Personal Data Protection functions are set forth in a Government Regulation.

CHAPTER VII

TRANSFER OF PERSONAL DATA

Section One

Transfer of Personal Data Within the Jurisdiction of the Republic of Indonesia

Article 55

- (1) A Personal Data Controller may transfer Personal Data to another Personal Data Controller within the jurisdiction of the Republic of Indonesia.
- (2) A Personal Data Controller that transfers Personal Data and the recipient of such a transfer are required to ensure the protection of Personal Data as provided for in this Act.

Part Two

Transfer of Personal Data Outside the Jurisdiction of the Republic of Indonesia

Article 56

- (1) A Personal Data Controller may transfer Personal Data to a Personal Data Controller and/or a Personal Data Processor outside the jurisdiction of the Republic of Indonesia in accordance with the provisions set forth in this Act.
- (2) When transferring Personal Data as referred to in paragraph (1), the Personal Data Controller must ensure that the country where the Personal Data Controller and/or Personal Data Processor receiving the transfer of Personal Data is located has a level of Personal Data Protection that is equivalent to or higher than that stipulated in this Act.
- (3) If the requirement referred to in paragraph (2) is not met, the Personal Data Controller must ensure that there is adequate and binding Personal Data Protection.
- (4) If the requirements referred to in paragraphs (2) and (3) are not met, the Personal Data Controller must obtain the consent of the Data Subject.
- (5) Further provisions regarding the transfer of Personal Data are set forth in a Government Regulation.

CHAPTER VIII

ADMINISTRATIVE SANCTIONS

Article 57

- (1) Violations of Article 20(1), Article 21, Article 24, Article 25(2), Article 26(3), Article 27, Article 28, Article 29, Article 30, Article 31, Article 32(1), Article 33, Article 34(1), Article 35, Article 36, Article 37, Article 38, Article 39(1), Article 40(1), Article 41(1) and (3), Article 42(1), Article 43(1), Article 44(1), Article 45, Article 46(1) and (3), Article 47, Article 48(1), Article 49, Article 51(1) and (5), Article 52, Article 53(1), Article 55(2), and Article 56(2) through (4) shall be subject to administrative sanctions.
- (2) The administrative sanctions referred to in paragraph (1) consist of:
 - a. a written warning;
 - b. temporary suspension of Personal Data processing activities;
 - c. deletion or destruction of Personal Data; and/or
 - d. an administrative fine.
- (3) Administrative sanctions in the form of administrative fines as referred to in paragraph (2)(d) shall not exceed 2 (two) percent of annual revenue or annual receipts related to the specific violation.
- (4) The imposition of administrative sanctions as referred to in paragraph (2) shall be carried out by the agency.
- (5) Further provisions regarding the procedures for imposing administrative sanctions as referred to in paragraph (3) are regulated in a Government Regulation.

CHAPTER IX

INSTITUTIONAL STRUCTURE

Article 58

- (1) The Government shall play a role in ensuring the implementation of Personal Data Protection in accordance with the provisions of this Act.
- (2) The administration of Personal Data Protection as referred to in paragraph (1) shall be carried out by an agency.
- (3) The agency referred to in paragraph (2) shall be designated by the President.
- (4) The agency referred to in paragraph (2) is accountable to the President.
- (5) Further provisions regarding the agency referred to in paragraph (2) shall be regulated by a Presidential Regulation.

Article 59

The agency referred to in Article 58 paragraph (2) shall carry out the following:

- a. the formulation and establishment of Personal Data Protection policies and strategies that serve as guidelines for Data Subjects, Personal Data Controllers, and Personal Data Processors;
- b. oversight of the implementation of Personal Data Protection;

- c. enforcement of administrative law regarding violations of this Act; and
- d. facilitation of out-of-court dispute resolution.

Article 60

The agency referred to in Article 58(2) shall have the authority to:

- a. formulate and establish policies in the field of Personal Data Protection;
- b. to supervise the compliance of Personal Data Controllers;
- c. impose administrative sanctions for violations of Personal Data Protection committed by Personal Data Controllers and/or Personal Data Processors;
- d. assist law enforcement authorities in handling alleged criminal offenses related to Personal Data as referred to in this Act;
- e. cooperating with personal data protection agencies of other countries in resolving alleged cross-border personal data protection violations;
- f. assess compliance with the requirements for the transfer of Personal Data outside the jurisdiction of the Republic of Indonesia;
- g. issuing orders to Personal Data Controllers and/or Personal Data Processors in connection with follow-up actions based on the results of supervision;
- h. publish the results of Personal Data Protection oversight in accordance with the provisions of laws and regulations;
- i. receive complaints and/or reports regarding alleged violations of Personal Data Protection;
- j. to investigate and examine complaints, reports, and/or the results of oversight regarding alleged violations of Personal Data Protection;
- k. summon and require the appearance of any individual and/or public entity related to alleged violations of Personal Data Protection;
- l. requesting statements, data, information, and documents from any person and/or public agency regarding alleged violations of Personal Data Protection;
- m. summon and have experts appear as necessary in the investigation and inquiry regarding alleged violations of Personal Data Protection;
- n. conduct investigations and inquiries into electronic systems, facilities, rooms, and/or premises used by the Personal Data Controller and/or Personal Data Processor, including obtaining access to data and/or appointing a third party; and
- o. request legal assistance from the public prosecutor's office in the resolution of Personal Data Protection disputes.

Article 61

Provisions regarding the procedures for the exercise of the authority of the agency as referred to in Article 60 are regulated in a Government Regulation.

CHAPTER X

INTERNATIONAL COOPERATION

Article 62

- (1) International cooperation shall be carried out by the Government with the governments of other countries or international organizations regarding the protection of personal data.
- (2) International cooperation in the implementation of this Act shall be carried out in accordance with the provisions of laws and regulations and the principles of international law.

CHAPTER XI

PUBLIC PARTICIPATION

Article 63

- (1) The public may play a role, either directly or indirectly, in supporting the implementation of Personal Data Protection.
- (2) The fulfillment of the role referred to in paragraph (1) may be carried out through education, training, advocacy, public awareness campaigns, and/or oversight in accordance with the provisions of applicable laws and regulations.

CHAPTER XII

DISPUTE RESOLUTION AND PROCEDURAL LAW

Article 64

- (1) Disputes regarding Personal Data Protection shall be resolved through arbitration, court proceedings, or other alternative dispute resolution mechanisms in accordance with the provisions of laws and regulations.
- (2) The procedural law applicable to dispute resolution and/or judicial proceedings regarding Personal Data Protection as referred to in paragraph (1) shall be implemented in accordance with the applicable procedural law as stipulated by laws and regulations.
- (3) Admissible evidence under this Act includes:
 - a. evidence as referred to in procedural law; and
 - b. other evidence in the form of electronic information and/or electronic documents in accordance with the provisions of laws and regulations.
- (4) Where necessary to protect Personal Data, court proceedings shall be held in camera.

CHAPTER XIII

PROHIBITIONS ON THE USE OF PERSONAL DATA

Article 65

- (1) No person shall unlawfully obtain or collect Personal Data that does not belong to them with the intent to benefit themselves or others, which may result in harm to the Data Subject.

- (2) No person shall unlawfully disclose Personal Data that does not belong to them.
- (3) No person shall unlawfully use Personal Data that does not belong to them.

Article 66

No person shall create false Personal Data or falsify Personal Data with the intent to benefit themselves or others, which may result in harm to others.

CHAPTER XIV CRIMINAL PROVISIONS

Article 67

- (1) Any person who intentionally and unlawfully obtains or collects Personal Data that does not belong to them, with the intent to benefit themselves or another person, which may result in harm to the Data Subject as referred to in Article 65(1), shall be punished by imprisonment for a maximum of 5 (five) years and/or a fine of up to Rp5,000,000,000.00 (five billion rupiah).
- (2) Any person who intentionally and unlawfully discloses Personal Data that does not belong to them, as referred to in Article 65(2), shall be punished by imprisonment for a maximum of 4 (four) years and/or a fine of up to Rp4,000,000,000.00 (four billion rupiah).
- (3) Any person who intentionally and unlawfully uses Personal Data that does not belong to them, as referred to in Article 65(3), shall be punished by imprisonment for a maximum of 5 (five) years and/or a fine of up to Rp5,000,000,000.00 (five billion rupiah).

Article 68

Any person who intentionally creates false Personal Data or falsifies Personal Data with the intent to benefit themselves or another person, which may result in harm to another person as referred to in Article 66, shall be punished by imprisonment for a maximum of 6 (six) years and/or a fine of up to Rp6,000,000,000.00 (six billion rupiah).

Article 69

In addition to the penalties referred to in Articles 67 and 68, an additional penalty may also be imposed in the form of forfeiture of profits and/or assets obtained or derived from the criminal act, as well as payment of damages.

Article 70

- (1) In the event that a criminal offense as referred to in Articles 67 and 68 is committed by a corporation, penalties may be imposed on the directors, controlling officers, those who gave the orders, beneficial owners, and/or the corporation itself.
- (2) The only penalty that may be imposed on a corporation is a fine.
- (3) The fine imposed on a corporation shall not exceed 10 (ten) times the maximum fine prescribed for the offense.
- (4) In addition to the fine referred to in paragraph (2), a corporation may be subject to the following additional penalties:
 - a. forfeiture of profits and/or assets obtained or derived from the criminal act;

- b. freezing of all or part of the Corporation's business activities;
- c. a permanent prohibition on carrying out certain activities;
- d. the closure of all or part of the Corporation's business premises and/or activities;
- e. fulfilling obligations that have been neglected;
- f. payment of damages;
- g. revocation of a license; and/or
- h. dissolution of the Corporation.

Article 71

- (1) In the event that a court imposes a criminal fine, the convicted person shall be given a period of 1 (one) month from the date the judgment becomes final and binding to pay the fine.
- (2) If there are compelling reasons, the period referred to in paragraph (1) may be extended for a maximum of 1 (one) month.
- (3) If the convicted person fails to pay the criminal fine within the time period referred to in paragraph (1) or paragraph (2), the convicted person's assets or income may be seized and auctioned by the prosecutor to settle the unpaid criminal fine.
- (4) If the seizure and auction of assets or income as referred to in paragraph (3) are insufficient or cannot be carried out, the unpaid fine shall be replaced with a prison sentence of the maximum duration prescribed for the relevant criminal offense.
- (5) The duration of the prison sentence referred to in paragraph (4), as determined by the judge, shall be stated in the court's judgment.

Article 72

- (1) In the event that the seizure and auction of assets or income as referred to in Article 71 paragraph (4) are carried out against a corporate defendant and are insufficient to pay the fine, the corporation shall be subject to a substitute penalty in the form of the freezing of some or all of the corporation's business activities for a period not exceeding 5 (five) years.
- (2) The duration of the suspension of part or all of the Corporation's business activities as referred to in paragraph (1), as determined by the judge, shall be stated in the court's decision.

Article 73

The provisions referred to in Articles 71 and 72 also apply in the case of the imposition of an additional penalty in the form of payment of damages.

CHAPTER XV

TRANSITIONAL PROVISIONS

Article 74

Upon the effective date of this Act, Personal Data Controllers, Personal Data Processors, and other parties involved in the processing of Personal Data shall comply with the provisions on the processing of Personal Data under this Act no later than 2 (two) years from the date this Act is promulgated.

Article 75

Upon the effective date of this Act, all provisions of laws and regulations governing the Protection of Personal Data shall remain in force to the extent they do not conflict with the provisions of this Act.

CHAPTER XVI**FINAL PROVISIONS****Article 76**

This Act shall take effect on the date of its promulgation.

So that everyone may be aware of it, the promulgation of this Law is hereby ordered by its publication in the State Gazette of the Republic of Indonesia.

Enacted in Jakarta

on October 17, 2022

THE PRESIDENT OF THE REPUBLIC OF INDONESIA

signed,

JOKO WIDODO

Promulgated in Jakarta

on October 17, 2022

MINISTER OF STATE SECRETARY OF THE REPUBLIC OF INDONESIA

Signed

PRATIKNO

OFFICIAL GAZETTE OF THE REPUBLIC OF INDONESIA YEAR 2022 NUMBER 196

[Certification appearing in the Indonesian source copy]

Certified true copy

MINISTRY OF THE STATE SECRETARIAT OF THE REPUBLIC OF INDONESIA

Deputy for Legislation and Legal Administration

Anna Djaman

ELUCIDATION
OF LAW OF THE REPUBLIC OF INDONESIA NUMBER 27 OF 2022
ON PERSONAL DATA PROTECTION

I. GENERAL

The rapid development of information and communication technology has created various opportunities and challenges. Information technology enables people to connect with one another without regard to national borders, making it one of the driving forces behind globalization. Various sectors of life have utilized information technology systems, such as the implementation of electronic commerce (e-commerce) in the trade/business sector, electronic education (e-education) in the field of education, electronic health (e-health) in the field of healthcare, electronic government (e-government) in the field of governance, as well as information technology utilized in other fields. The use of this information technology has made it very easy to collect and transfer an individual's Personal Data from one party to another without the knowledge of the Data Subject, thereby threatening the constitutional rights of the Data Subject.

Personal data protection falls under the protection of human rights. Thus, regulations concerning personal data are a manifestation of the recognition and protection of fundamental human rights. The existence of a Personal Data Protection Act is an absolute necessity that can no longer be postponed, as it is urgently needed for various national interests. Indonesia's participation in the international community also necessitates the protection of personal data. Such protection can facilitate transnational trade, industry, and investment.

The Law on Personal Data Protection is mandated by Article 28G, paragraph (1) of the 1945 Constitution of the Republic of Indonesia, which states that, "Every person has the right to protection of their personal self, family, honor, dignity, and property under their control, as well as the right to feel secure and to be protected from the threat of fear of doing or not doing something that constitutes a fundamental right." The issue of Personal Data Protection arises from concerns regarding violations of Personal Data that may be experienced by individuals and/or legal entities. Such violations can result in material and non-material losses.

The formulation of regulations on Personal Data Protection is justified by the need to protect individual rights within society in connection with the processing of Personal Data, whether conducted electronically or non-electronically using data processing devices. Adequate protection of Personal Data will foster public trust, enabling individuals to provide Personal Data for the greater public good without it being misused or their personal rights violated. Thus, these regulations will strike a balance between the rights of individuals and those of society, the interests of which are represented by the state. These regulations on Personal Data Protection will make a significant contribution to the creation of order and progress in the information society.

To minimize overlapping provisions regarding Personal Data Protection, the provisions in this Act essentially serve as general standards for Personal Data Protection - whether processed in part or in full, electronically or non-electronically - allowing each sector to implement Personal Data Protection measures in accordance with its specific characteristics. The regulations on Personal Data Protection aim, among other things, to protect and guarantee the fundamental rights of citizens regarding personal privacy; to ensure that the public can access services from corporations, public agencies, international organizations, and the government; to promote the growth of the digital economy and the information

and communications technology industry; and to support the enhancement of the competitiveness of domestic industries.

ARTICLE BY ARTICLE

Article 1

Self-explanatory.

Article 2

Self-explanatory.

Article 3

Letter a

The term "principle of protection" means that any processing of Personal Data must be conducted in a manner that protects the Data Subject regarding their Personal Data and ensures that such Personal Data is not misused.

Letter b

The term "principle of legal certainty" means that all processing of Personal Data is conducted based on a legal foundation to ensure the protection of Personal Data, as well as all measures supporting its implementation, so that it receives legal recognition both in and out of court.

Letter c

The term "principle of public interest" means that in enforcing Personal Data Protection, the broader public interest or the interests of society must be taken into account. Such public interests include, among others, the interests of state administration and national defense and security.

Letter d

The "principle of utility" means that regulations on the protection of personal data must serve the national interest, particularly in realizing the goal of public welfare.

Letter e

The "principle of prudence" means that parties involved in the processing and supervision of Personal Data must take into account all aspects that could potentially cause harm.

Letter f

The "principle of balance" refers to efforts in Personal Data Protection to balance the right to Personal Data, on the one hand, with the legitimate rights of the state based on the public interest.

Letter g

The term "principle of accountability" means that all parties involved in the processing and supervision of Personal Data must act responsibly so as to ensure a balance between the rights and obligations of the relevant parties, including the Data Subjects.

Letter h

The term "principle of confidentiality" means that Personal Data is protected from unauthorized parties and/or from unlawful processing of Personal Data.

Article 4

Paragraph (1)

Letter a

Specific Personal Data means Personal Data whose processing may have a greater impact on the Data Subject, including discrimination and greater harm to the Data Subject.

Letter b

Self-explanatory.

Paragraph (2)

Letter a

"Health data and information" refers to individual records or information related to physical health, mental health, and/or health care services.

Letter b

"Biometric data" refers to data related to an individual's physical, physiological, or behavioral characteristics that enable the unique identification of that individual, such as facial images or dactyloscopic data. Biometric data also pertains to the unique nature and/or characteristics of a person that must be safeguarded and protected, including but not limited to fingerprint records, retinal scans, and DNA samples.

Letter c

"Genetic data" refers to all data of any kind regarding an individual's characteristics that are inherited or acquired during early prenatal development.

Letter d

The term "criminal record" refers to a written record of a person who has committed an unlawful act or is currently undergoing legal proceedings for an act committed, including, among others, police records and inclusion on a watchlist or blacklist.

Letter e

Self-explanatory.

Letter f

The term "personal financial data" includes, but is not limited to, data on the amount of funds held in banks, including savings accounts, time deposits, and credit card data.

Letter g

Self-explanatory.

Paragraph (3)

Letter a

Self-explanatory.

Letter b

Self-explanatory.

Letter c

Self-explanatory.

Letter d

Self-explanatory.

Letter e

Self-explanatory.

Letter f

"Personal Data combined to identify a person" includes, among other things, mobile telephone numbers and IP addresses.

Article 5

Self-explanatory.

Article 6

Self-explanatory.

Article 7

The right to obtain a copy of Personal Data is provided free of charge, except under certain conditions that do require a fee.

Article 8

Self-explanatory.

Article 9

Self-explanatory.

Article 10**Paragraph (1)**

"Profiling" refers to the activity of identifying an individual, including but not limited to their employment history, economic status, health, personal preferences, interests, reliability, behavior, location, or movements of the Subject of Personal Data, conducted electronically.

Paragraph (2)

Self-explanatory.

Article 11

Self-explanatory.

Article 12

Self-explanatory.

Article 13

Self-explanatory.

Article 14

Self-explanatory.

Article 15

Paragraph (1)

Letter a

Self-explanatory.

Letter b

What is meant by "the interests of the law enforcement process" are interests related to efforts or steps taken to implement or enforce legal rules based on statutory provisions, including, among others, the processes of investigation, inquiry, and prosecution.

Letter c

"The public interest in the context of state administration" refers, among other things, to the administration of civil registration, social security, taxation, customs, and electronically integrated business licensing services.

Letter d

The term "financial services sector" refers to banking, capital markets, insurance, financing institutions, pension funds, technology-based regulation, financial technology, and other technology-based sectors under the supervision of Bank Indonesia, the Financial Services Authority, and the Deposit Insurance Corporation.

Letter e

Self-explanatory.

Paragraph (2)

Self-explanatory.

Article 16

Paragraph (1)

Letter a

Self-explanatory.

Letter b

Self-explanatory.

Letter c

Self-explanatory.

Letter d

Self-explanatory.

Letter e

"Display" means showing Personal Data for certain purposes and to certain parties.

"Publication" means the dissemination of information intended for the general public.

"Transfer" refers to the movement, transmission, and/or duplication of Personal Data, whether electronically or non-electronically, from the Personal Data Controller to another party.

Letter f

Self-explanatory.

Paragraph (2)

Self-explanatory.

Paragraph (3)

Self-explanatory.

Article 17

Self-explanatory.

Article 18

Self-explanatory.

Article 19

Self-explanatory.

Article 20

Paragraph (1)

Self-explanatory.

Paragraph (2)

Letter a

Self-explanatory.

Letter b

Self-explanatory.

Letter c

Self-explanatory.

Letter d

"Vital interests of the Data Subject" refers to matters related to the Data Subject's survival, such as when the processing of Personal Data is necessary for serious medical treatment.

Letter e

Self-explanatory.

Letter f

Self-explanatory.

Article 21

Paragraph (1)

Letter a

Self-explanatory.

Letter b

Self-explanatory.

Letter c

Self-explanatory.

Letter d

Self-explanatory.

Letter e

The term "details regarding the Information collected" refers to a list of Information regarding the Personal Data of Data Subjects - whether general Personal Data or specific Personal Data - collected by the Data Controller for the purpose of processing Personal Data.

Letter f

"The duration of Personal Data processing" refers to the time period from the start to the completion of a series of Personal Data processing activities in accordance with the purposes of such processing.

Letter g

Self-explanatory.

Paragraph (2)

Self-explanatory.

Article 22

Paragraph (1)

Self-explanatory.

Paragraph (2)

Self-explanatory.

Paragraph (3)

Self-explanatory.

Paragraph (4)

Letter a

Self-explanatory.

Letter b

Self-explanatory.

Letter c

The term "language" refers to the Indonesian language.

Paragraph (5)

Self-explanatory.

Article 23

Self-explanatory.

Article 24

Self-explanatory.

Article 25

Self-explanatory.

Article 26

Self-explanatory.

Article 27

The term "limited and specific" means that the collection of Personal Data must be limited to the purposes of its processing, and the purposes of processing Personal Data must be explicit, lawful, and determined at the time of collection.

The term "legally valid" means that the processing of Personal Data is carried out in accordance with the provisions of applicable laws and regulations.

"Transparent" means that the processing of Personal Data is carried out in a manner that ensures the Data Subject is aware of the Personal Data being processed and how it is processed, and that all information and communications related to such processing are easily accessible and understandable, using clear language.

Article 28

Self-explanatory.

Article 29

Self-explanatory.

Article 30

Self-explanatory.

Article 31

Self-explanatory.

Article 32

Self-explanatory.

Article 33

Letter a

The term "endangering the safety, physical health, or mental health of the Data Subject and/or others" refers, among other things, to changes in medical history data that have the potential to endanger the safety of oneself and/or others.

Letter b

The term "affecting the disclosure of another person's Personal Data" refers, among other things, to changes in a customer's Personal Data that result in the disclosure of another person's Personal Data

Letter c

Self-explanatory.

Article 34

Paragraph (1)

A Personal Data Protection impact assessment is conducted to evaluate the potential risks arising from the processing of Personal Data, as well as the efforts or measures that must be taken to mitigate those risks, including with respect to the rights of Data Subjects and compliance with this Act.

Paragraph (2)

Self-explanatory.

Paragraph (3)

Self-explanatory.

Article 35

Self-explanatory.

Article 36

Self-explanatory.

Article 37

Self-explanatory.

Article 38

Self-explanatory.

Article 39

Self-explanatory.

Article 40

Self-explanatory.

Article 41

Self-explanatory.

Article 42

Self-explanatory.

Article 43

Self-explanatory.

Article 44**Paragraph (1)**

The term "destroy" refers to the act of removing, eliminating, or destroying Personal Data so that it can no longer be used to identify the Data Subject.

Paragraph (2)

Self-explanatory.

Article 45

Self-explanatory.

Article 46**Paragraph (1)**

"Personal Data Protection Breach" means a failure to protect an individual's Personal Data with regard to its confidentiality, integrity, and availability, including security breaches - whether intentional or unintentional - that result in the destruction, loss, alteration, disclosure, or unauthorized access to Personal Data that is transmitted, stored, or processed.

Paragraph (2)

Self-explanatory.

Paragraph (3)

The term "under certain circumstances" refers, among other things, to situations where a failure to protect Personal Data disrupts public services and/or has a serious impact on the public interest.

Article 47

Self-explanatory.

Article 48**Paragraph (1)**

The term "notification" refers to a notification to the Data Subject or a general notification through the mass media, whether electronic or non-electronic.

Paragraph (2)

Self-explanatory.

Paragraph (3)

Self-explanatory.

Paragraph (4)

Self-explanatory.

Paragraph (5)

Self-explanatory.

Article 49

Self-explanatory.

Article 50

Self-explanatory.

Article 51

Self-explanatory.

Article 52

Self-explanatory.

Article 53**Paragraph (1)**

The term "official or employee performing Personal Data Protection functions" refers to an official or employee responsible for ensuring compliance with the principles of Personal Data Protection and mitigating the risk of Personal Data Protection violations.

Paragraph (2)

Self-explanatory.

Paragraph (3)

Self-explanatory.

Article 54

Self-explanatory.

Article 55

Self-explanatory.

Article 56

Self-explanatory.

Article 57**Paragraph (1)**

Self-explanatory.

Paragraph (2)

Self-explanatory.

Paragraph (3)

"Revenue" refers to the gross inflow of economic benefits arising from the entity's normal activities during the period, provided that such inflow results in an increase in equity that does not stem from contributions by investors.

Paragraph (4)

Self-explanatory.

Paragraph (5)

Self-explanatory.

Article 58

Self-explanatory.

Article 59**Letter a**

Self-explanatory.

Letter b

Self-explanatory.

Letter c

Self-explanatory.

Letter d

"Facilitation of dispute resolution outside of litigation" refers to the provision of means for dispute resolution through procedures agreed upon by the parties, namely out-of-court settlement by way of consultation, arbitration, negotiation, mediation, conciliation, or expert assessment in accordance with the provisions of laws and regulations.

Article 60**Letter a**

In formulating and enacting Personal Data Protection policies, the agency shall involve business organizations in accordance with the provisions of laws and regulations.

Letter b

Self-explanatory.

Letter c

Self-explanatory.

Letter d

Self-explanatory.

Letter e

Self-explanatory.

Letter f

Self-explanatory.

Letter g

Self-explanatory.

Letter h

Self-explanatory.

Letter i

Self-explanatory.

Letter j

Self-explanatory.

Letter k

Self-explanatory.

Letter l

Self-explanatory.

Letter m

Self-explanatory.

Letter n

Self-explanatory.

Letter o

Self-explanatory.

Article 61

Self-explanatory.

Article 62

Self-explanatory.

Article 63

Self-explanatory.

Article 64

Self-explanatory.

Article 65

Self-explanatory.

Article 66

Self-explanatory.

Article 67

Self-explanatory.

Article 68

Self-explanatory.

Article 69

Self-explanatory.

Article 70

Self-explanatory.

Article 71

Self-explanatory.

Article 72

Self-explanatory.

Article 73

Self-explanatory.

Article 74

Self-explanatory.

Article 75

Self-explanatory.

Article 76

Self-explanatory.

**SUPPLEMENT TO THE STATE GAZETTE OF THE REPUBLIC OF INDONESIA NO.
6820**