UNOFFICIAL ENGLISH TRANSLATION

Government Regulation No 33 of 2026

Implementing Regulations for Law No 27 of 2022 on 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 preamble, Articles 1 to 225, and promulgation details. Pagination has been reset for this English edition.

legaltrans.id
Edited and formatted English edition

GOVERNMENT REGULATION OF THE REPUBLIC OF INDONESIA NUMBER 33 OF 2026

IMPLEMENTING REGULATIONS FOR LAW NO. 27 OF 2022 ON PERSONAL DATA PROTECTION

BY THE GRACE OF GOD, THE ALMIGHTY, THE PRESIDENT OF THE REPUBLIC OF INDONESIA,

Whereas that in order to implement the provisions of Article 10(2), Article 12(2), Article 13(3), Article 16(3), Article 34(3), Article 48(5), Article 54(3), Article 56(5), Article 57(5), and Article 61 of Law No. 27 of 2022 on Personal Data Protection, it is necessary to issue a Government Regulation on the Implementing Regulations of Law No. 27 of 2022 on Personal Data Protection;

1. Article 5, paragraph (2) of the 1945 Constitution of the Republic of Indonesia
2. Law No. 27 of 2022 on Personal Data Protection (State Gazette of the Republic of Indonesia of 2022, No. 196, Supplement to the State Gazette of the Republic of Indonesia, No. 6820);

HEREBY DECREES:

To enact: GOVERNMENT REGULATION ON IMPLEMENTING REGULATIONS FOR LAW NO. 27 OF 2022 ON PERSONAL DATA PROTECTION.

CHAPTER I

GENERAL PROVISIONS

Article 1

In this Government Regulation, 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 refers to details, statements, ideas, and signs that contain value, meaning, and messages - including data, facts, and their explanations - that can be seen, heard, or read, presented in various forms and formats in accordance with advancements in information and communication technology, whether electronic or non-electronic.
4. A Personal Data Controller is any individual, public agency, or international organization acting alone or jointly in determining the purposes of and exercising control over the processing of Personal Data.
5. A Personal Data Processor is any individual, public agency, or international organization that acts individually or jointly to process 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 an individual or a corporation.
8. A Public Body is an executive, legislative, or judicial institution, or any other body whose primary functions and duties relate to the administration of the state, and which is funded in whole or in part

by the state revenue and expenditure budget and/or the regional revenue and expenditure budget; or a nongovernmental organization, provided that it is funded in whole or in part by the state revenue and expenditure budget and/or the regional revenue and expenditure budget, public donations, and/or foreign sources.

9. An International Organization is an organization recognized as a subject of international law and possessing the capacity to enter into international agreements.
10. Personal Data Protection Mediation, hereinafter referred to as "Mediation," is a method of resolving Personal Data Protection Disputes related to Personal Data through a negotiation process to reach an agreement among the Disputing Parties with the assistance of a Mediator.
11. A Mediator is one or more individuals who possess the competencies established by the Agency and/or are registered with an arbitration body or mediation institution in accordance with applicable laws and regulations, and who are based within the territory of the Republic of Indonesia, to assist the disputing parties in seeking a possible resolution to a Personal Data Protection Dispute.
12. Arbitration is a method of resolving civil Personal Data Protection Disputes outside the general court system, based on a written arbitration agreement entered into by the Disputing Parties.
13. The disputing parties are the Personal Data Controller, the Personal Data Processor, or the Data Subject involved in the dispute.
14. A Settlement Agreement is an agreement resulting from mediation in the form of a document containing peace clauses and provisions for the resolution of Personal Data Protection disputes, and signed by the disputing parties and the mediator.
15. An Institution is an entity that administers Personal Data Protection as stipulated in the laws governing Personal Data Protection.
16. A Mediation Institution is an alternative dispute resolution institution for Personal Data Protection disputes that is legally established within the territory of the Republic of Indonesia in accordance with the provisions of laws and regulations.
17. A Personal Data Protection Dispute, hereinafter referred to as a Dispute, is a conflict of interests or disagreement between the Disputing Parties regarding the implementation or fulfillment of the Personal Data Protection rights and/or obligations of either party based on the legal relationship between them.
18. Failure of Personal Data Protection means a failure to protect an individual's Personal Data in terms of confidentiality, integrity, and availability, including a security breach, whether intentional or unintentional, leading to destruction, loss, alteration, disclosure of, or unauthorized access to Personal Data that is transmitted, stored, or processed.
19. Day means a working day.
20. Joint Controllers of Personal Data are two or more Personal Data Controllers that jointly determine the purposes of and exercise control over the processing of Personal Data.
21. A Child is any person who is under 18 (eighteen) years of age and unmarried.
22. A person with a disability is any person who has a long-term physical, intellectual, mental, and/or sensory impairment that, when interacting with the environment, may result in barriers and difficulties in fully and effectively participating with other citizens on the basis of equal rights.
23. Retention Period means the period of time during which Personal Data is processed as necessary to achieve the purposes of such processing or to comply with other legal obligations.

24. International Cooperation in the Field of Personal Data Protection, hereinafter referred to as International Cooperation, is a joint activity carried out bilaterally, regionally, or multilaterally for the purpose of providing Personal Data Protection.
25. Officials or Officers Carrying Out Personal Data Protection Functions, hereinafter referred to as PPDP, are officials or officers responsible for ensuring compliance with the principles of Personal Data Protection and mitigating the risk of Personal Data Protection violations.
26. 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.
27. A ministry or agency is a state administrative body tasked with overseeing and issuing regulations for its respective sector.

Article 2

This Government Regulation governs every Person, Public Body, and International Organization carrying out Personal Data Protection activities that are located:

a. within the jurisdiction of the Republic of Indonesia; and
b. outside the jurisdiction of the Republic of Indonesia that have legal consequences:
    1. within the jurisdiction of the Republic of Indonesia; and/or
    2. for Data Subjects who are Indonesian citizens outside the jurisdiction of the Republic of Indonesia.

Article 3

(1) Individuals who process Personal Data in the course of personal or household activities are not subject to the provisions regarding the processing of Personal Data as set forth in this Government Regulation.

(2) The processing of Personal Data in personal or household activities as referred to in paragraph (1) includes:

a. the processing of Personal Data carried out by an individual for personal or household purposes and to meet personal or household needs;
b. Personal Data processing activities that are not professional and/or commercial in nature; and/or
c. activities involving the processing of Personal Data that are not intended for the public.

Article 4

The scope of this Government Regulation covers:

a. Personal Data;
b. processing of Personal Data;
c. rights and obligations;
d. transfer of Personal Data outside the jurisdiction of the Republic of Indonesia;
e. International Cooperation;
f. public participation;

g. oversight of Personal Data Controller compliance;

h. administrative sanctions; and

i. Dispute Resolution.

CHAPTER II

PERSONAL DATA

Article 5

Personal Data consists of:

a. Specific Personal Data; and

b. General Personal Data.

Article 6

(1) Specific Personal Data as referred to in Article 5(a) includes:

a. Health data and information;

b. biometric data;

c. genetic data;

d. criminal records;

e. children's data;

f. personal financial data; and/or

g. other data as provided for by applicable laws and regulations.

(2) Other data in accordance with the provisions of laws and regulations as referred to in paragraph (1)(g) shall be determined by the Ministry or agency.

(3) In determining other data in accordance with laws and regulations as referred to in paragraph (2), the Ministry or agency shall coordinate with the Agency.

(4) The determination of other data in accordance with the provisions of laws and regulations as referred to in paragraph (1)(g) shall be carried out based on a consideration of Personal Data whose processing has the potential to cause a greater impact on the Data Subject.

Article 7

(1) General Personal Data as referred to in Article 5(b) includes:

a. full name;

b. gender;

c. nationality;

d. religion;

e. marital status; and/or

f. Personal Data that is combined to identify an individual.

(2) The combination referred to in paragraph (1)(f) is carried out through:

a. direct reference;
b. mapping references;
c. triangulation; and/or
d. other combinations.

(3) The combination referred to in paragraph (1)(f) includes the use of data available in the public domain.

(4) Further provisions regarding the combination of Personal Data as referred to in paragraph (2) are set forth in the Agency Regulations.

CHAPTER III

PROCESSING OF PERSONAL DATA

Section One

General

Article 8

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.

Part Two

Principles of Personal Data Protection

Article 9

The processing of Personal Data as referred to in Article 8 shall be conducted in accordance with the principles of Personal Data Protection, including:

a. the collection of Personal Data shall be 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 safeguards the rights of the Data Subject;
d. the processing of Personal Data is carried out accurately, completely, without misleading information, up-to-date, and in a manner for which accountability can be established;
e. the processing of Personal Data is carried out by protecting the security of Personal Data from unauthorized access, unauthorized disclosure, unauthorized alteration, misuse, destruction, and/or loss of Personal Data;

f. The processing of Personal Data is carried out by notifying the Data Subject of the purpose and activities of Personal Data processing, as well as any failures in the protection of Personal Data;

g. Personal Data is destroyed and/or deleted after the Retention Period expires or upon request by the Data Subject, unless otherwise specified by applicable laws and regulations; and

h. The processing of Personal Data is carried out responsibly and can be clearly substantiated.

Part Three

Parties Involved in the Processing of Personal Data

Article 10

The parties involved in the processing of Personal Data as regulated by this Government Regulation consist of:

a. the Data Subject;

b. Personal Data Controllers; and/or

c. Personal Data Processors.

Article 11

(1) The processing of Personal Data may be carried out by Joint Controllers of Personal Data.

(2) Where Personal Data is processed by Joint Controllers of Personal Data, the following minimum requirements must be met:

a. there is an agreement outlining the roles, responsibilities, and relationships among the Personal Data Controllers;

b. there are interrelated purposes and jointly determined methods of processing Personal Data; and

c. there is a jointly designated contact person.

(3) The agreement referred to in paragraph (2)(a) shall at least include:

a. the basis for the processing of Personal Data by each Personal Data Controller;

b. the relationship between the purposes of processing Personal Data controlled by each Personal Data Controller;

c. a statement of agreement on the method of processing Personal Data;

d. the types of Personal Data being processed;

e. the division of roles and responsibilities for fulfilling each Personal Data Controller's legal obligations in accordance with laws and regulations; and

f. a jointly designated contact person.

(4) The Joint Controllers of Personal Data are jointly responsible for ensuring that the processing of Personal Data is carried out in accordance with this Agreement and the provisions of applicable laws and regulations.

Article 12

The Joint Controllers of Personal Data as referred to in Article 11 shall be jointly and severally liable for the processing of Personal Data in accordance with the provisions of applicable laws and regulations.

Article 13

(1) Personal Data Controllers may appoint a Personal Data Processor.

(2) The Personal Data Processor must process Personal Data in accordance with the provisions of Government Regulation No.

(3) The processing of Personal Data by a Personal Data Processor appointed by the Personal Data Controller as referred to in paragraph (1) is the responsibility of the Personal Data Controller.

Article 14

The appointment of a Personal Data Processor as referred to in Article 13 shall be made pursuant to an agreement that includes at least:

a. the scope of the processing of Personal Data by the Personal Data Processor on behalf of the Personal Data Controller;
b. method of processing of Personal Data;
c. the types and purposes of Personal Data processing;
d. Types of Personal Data Processed;
e. categories of Data Subjects;
f. the duration of Personal Data processing;
g. the rights and obligations of the Personal Data Controller and the Personal Data Processor;
h. mechanisms for oversight, documentation, audit, and inspection;
i. dispute resolution;
j. the involvement of other Personal Data Processors in accordance with the agreement; and
k. the designation of a jointly appointed contact person.

Article 15

(1) A Personal Data Processor may engage another Personal Data Processor to process Personal Data.

(2) A Personal Data Processor must obtain written consent from the Personal Data Controller before engaging another Personal Data Processor.

(3) The Personal Data Processor referred to in paragraph (1) must ensure that the other Personal Data Processor involved processes Personal Data in accordance with the provisions of this Government Regulation.

(4) The appointment of other Personal Data Processors by a Personal Data Processor shall be governed by a written agreement, taking into account an equivalent level of Personal Data Protection as agreed upon in the agreement between the Personal Data Controller and Personal Data Processor.

(5) The processing of Personal Data by other processors is the responsibility of the Personal Data Controller.

Article 16

(1) Joint Controllers of Personal Data may designate a Data Processor.

(2) The provisions on the appointment of a Personal Data Processor by a Personal Data Controller as referred to in Articles 13 and 14 apply mutatis mutandis to the appointment of a Personal Data Processor by Joint Controllers of Personal Data.

Part Four

Installation of Visual Data Processing Devices

Article 17

(1) The installation of visual data processing or analysis devices in public places and/or at public service facilities is 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. information must be displayed in the area where the visual data processing devices are installed; and

c. They must not be used to identify an individual.

(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.

(3) The installation of visual data processing devices is the responsibility of the Personal Data Controller and/or the Personal Data Processor.

(4) The installation of visual data processing devices as referred to in paragraph (1) shall take privacy into account.

(5) The processing of Personal Data through visual data processing devices shall be carried out in accordance with this Government Regulation.

Article 18

(1) Personal Data Controllers and/or Personal Data Processors as referred to in Article 17(2) shall ensure that recording is carried out consistently and that Personal Data is protected in accordance with this Government Regulation.

(2) A Personal Data Controller and/or Personal Data Processor may only install and use visual data processing or monitoring devices as referred to in paragraph (1) to monitor the designated areas in accordance with the purpose of the monitoring.

Article 19

(1) In the event that a Personal Data Controller and/or Personal Data Processor installs visual data processing or monitoring devices in a public area or public place and conducts recording, the Personal Data Controller and/or Personal Data Processor must display information stating that visual data processing or monitoring devices are installed in that area.

(2) The information referred to in paragraph (1) must be conveyed clearly, specifically, and concisely, stating that visual data processing equipment is in operation.

(3) The information referred to in paragraph (1) must, at a minimum, include the following:

a. Information that the visual data processing or monitoring device is currently in operation; and

b. the contact information of the party responsible for the visual data processing device.

(4) The information referred to in paragraph (1) must:

a. be placed at the entrance to an enclosed area where visual data processing devices are installed; or

b. be placed in a location that is easily accessible and readable before entering the area monitored by the visual data processing or analysis equipment in an open area.

CHAPTER IV

RIGHTS AND OBLIGATIONS

Part One: General Provisions

Article 20

The exercise of the rights of a Data Subject shall be submitted through a recorded request submitted electronically or non-electronically to the Personal Data Controller in accordance with the provisions of applicable laws and regulations.

Article 21

(1) The Personal Data Controller must provide channels for requests to exercise the rights of the Data Subject, either electronically and/or non-electronically, that are easily accessible to the Data Subject.

(2) In the event that the Personal Data Controller processes Personal Data electronically, requests for the exercise of the rights of the Data Subject shall be submitted electronically.

(3) Data Controller shall provide notification of the exercise of the Data Subject's rights as requested, as referred to in paragraph (1), through:

a. the same communication medium used by the Data Subject at the time the request was submitted; or

b. other means of communication that the Data Subject can easily access.

Article 22

The time of receipt of a recorded application as referred to in Article 20 is determined as follows:

a. for applications submitted electronically, the time of receipt is calculated from the time the application enters the electronic system under the control of the Personal Data Controller; or

b. for requests submitted non-electronically, the time of receipt is calculated based on the date on the request receipt.

Article 23

Requests to exercise the rights of a Data Subject as referred to in Article 20 may be submitted by:

a. the Data Subject;

b. the parents and/or legal guardians of a Child;

c. the guardian of a Person with a Disability; or

d. an authorized representative of the Data Subject, in accordance with the provisions of laws and regulations.

Article 24

(1) A written request as referred to in Article 20 must include:

a. the identity of the party submitting the request;

b. an explanation of the Data Subject's rights and the Data Subject's interest in filing the request; and

c. a description of the Data Subject's request regarding the Personal Data processed by the Personal Data Controller.

(2) The identification referred to in paragraph (1)(a) must be accompanied by proof of identity.

Article 25

The Personal Data Controller must verify requests to exercise the rights of Data Subjects using a proportional mechanism.

Article 26

The Personal Data Controller shall determine the conditions for granting and/or rejecting a request by a Data Subject to exercise their rights in accordance with the provisions of laws and regulations.

Article 27

(1) In the event that the Personal Data Controller fails to fulfill its obligations regarding a request to exercise the rights of a Data Subject, the Data Subject may file a report with the Agency in accordance with the provisions of this Government Regulation.

(2) The Agency shall follow up on the report referred to in paragraph (1) in accordance with the provisions of this Government Regulation.

Article 28

(1) The Personal Data Controller must draft and establish provisions for the processing of Personal Data applicable within the Personal Data Controller's jurisdiction.

(2) The formulation and establishment of the provisions for the processing of Personal Data as referred to in paragraph (1) must be carried out in accordance with the guidelines for the formulation of provisions for the processing of Personal Data established by the Agency.

(3) The guidelines for drafting referred to in paragraph (2) contain provisions for the processing of Personal Data in accordance with the provisions of this Government Regulation.

(4) Personal Data Controllers may consult with the Agency in drafting the provisions governing the processing of Personal Data applicable internally.

Article 29

Personal Data Controllers and/or Personal Data Processors are required to carry out the Agency's instructions in implementing Personal Data Protection as regulated in the Law on Personal Data Protection.

Part Two

the Basis for the Processing of Personal Data

Paragraph 1

Article 30

(1) A Personal Data Controller must have a legal basis for processing Personal Data.

(2) The obligation to have a legal basis for the processing of Personal Data as referred to in paragraph (1) must be established before the Personal Data Controller processes Personal Data.

(3) 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 1 (one) or more specific purposes that have been communicated by the Personal 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, public service, or the exercise of the authority of the Personal Data Controller in accordance with laws and regulations; and/or

f. the fulfillment of other legitimate interests, taking into account the purposes, needs, and balance of interests between the Personal Data Controller and the rights of the Data Subject.

(4) The determination of the legal basis for the processing of Personal Data as referred to in paragraph (3) is based on the purpose, objectives, and needs of the Personal Data processing, in compliance with the provisions set forth in this Government Regulation.

Article 31

The Personal Data Controller must ensure that the processing of Personal Data is not discriminatory toward the Data Subject.

Paragraph 2

Explicit Consent

Article 32

(1) The Personal Data Controller may use valid explicit consent as the basis for processing Personal Data.

(2) Valid explicit consent as referred to in Article 30, paragraph (3), letter a, must be obtained from the Data Subject freely, knowingly, specifically, and unambiguously.

Article 33

(1) In the processing of Personal Data based on valid explicit consent from the Data Subject as referred to in Article 30, paragraph (3), letter a, the Personal Data Controller is required to provide information in accordance with the provisions of this Government Regulation.

(2) The information referred to in paragraph (1) shall be provided prior to obtaining consent from the Data Subject.

(3) The information referred to in paragraph (1) shall be provided to the Data Subject in a concise and accurate manner, and in accordance with the Personal Data processing activities carried out by the Data Controller.

Article 34

(1) The Personal Data Controller must provide a mechanism for obtaining the consent of the Data Subject.

(2) The mechanism for obtaining consent as referred to in paragraph (1) may be provided in either electronic or non-electronic form.

(3) The mechanism for obtaining consent as referred to in paragraph (2) is linked to the information as referred to in Article 33.

Article 35

(1) In the event that a Data Subject does not provide consent for the processing of Personal Data, the Personal Data Controller shall continue to provide goods, services, or other offerings to the Data Subject without reducing their quality, unless the provision of such goods, services, or offerings requires the processing of Personal Data.

(2) In the event that one of the purposes of processing Personal Data based on valid consent is explicitly for the purpose of offering goods and/or services, the Personal Data Controller must clearly state:

a. Information regarding the third parties that will receive the Personal Data;

b. Information regarding the form of the offer that will be provided; and

c. the mechanism for withdrawing consent and reporting if the offering activities continue after consent is withdrawn.

(3) The Personal Data Controller shall not request consent from the Data Subject in a manner that is deceptive and/or misleading to the Data Subject.

Article 36

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

(2) The obligation to provide evidence of consent as referred to in paragraph (1) is carried out in the context of accountability for the processing of Personal Data.

Article 37

The Personal Data Controller must ensure that the Data Subject's right to withdraw consent at any time is fulfilled through mechanisms provided by the Personal Data Controller.

Article 38

(1) The Personal Data Controller must take steps to identify Children in accordance with the purpose of Personal Data processing.

(2) The processing of a Child's Personal Data as referred to in paragraph (1) must obtain consent from the Child's parent and/or guardian in accordance with the provisions of laws and regulations.

(3) The Personal Data Controller may process the Personal Data of the child's parents and/or guardian in connection with the processing of the child's Personal Data in accordance with the provisions of applicable laws and regulations.

(4) The Personal Data Controller must verify the consent referred to in paragraph (2) by taking into account available technology.

(5) A child, the child's parent(s), and/or the child's guardian may submit a request for the fulfillment of the child's rights as a Data Subject to the Personal Data Controller in accordance with the provisions of applicable laws and regulations.

(6) In the event that a request for the fulfillment of a child's rights is submitted by the child as referred to in paragraph (5), the fulfillment of such rights shall be based on the Personal Data Controller's assessment of the child's capacity to understand the fulfillment of those rights.

(7) The fulfillment of the child's rights as referred to in paragraph (6) must be based on the consent of the child's parents and/or legal guardian, except for the child's rights related to the processing of Personal Data.

(8) The Personal Data Controller must provide a procedure for transitioning the mechanism for processing a Child's Personal Data when the Child has reached an age or meets criteria under which they are no longer considered a Child.

Article 39

(1) The Personal Data Controller must take steps to identify persons with disabilities in accordance with the purpose of processing Personal Data.

(2) The steps to identify 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 communication referred to in paragraph (2) shall be carried out by providing facilities that are easy for Data Subjects with disabilities to understand and use.

(4) The processing of Personal Data of Persons with Disabilities as referred to in paragraph (1) must obtain consent from the Person with a Disability and/or the Person with a Disability's guardian in accordance with the provisions of laws and regulations.

(5) Persons with disabilities and/or their legal guardians may submit requests to exercise their rights as Data Subjects in accordance with the provisions of regulations under applicable laws and regulations.

(6) The Personal Data Controller must provide special mechanisms to ensure accessibility for persons with disabilities when submitting requests to exercise their rights as Data Subjects.

Paragraph 3: Fulfillment of Contractual Obligations

Article 40

(1) A Personal Data Controller may use the fulfillment of contractual obligations as a basis for processing Personal Data in the following cases:

a. the Data Subject is a party to the agreement; or

b. fulfillment of a request by the Data Subject at the time of entering into an agreement.

(2) An agreement that requires the processing of Personal Data may include one or more purposes for the processing of Personal Data.

(3) The parties to the agreement must comply with the provisions set forth in this Government Regulation.

(4) The Personal Data Controller may not process Personal Data beyond what is specified in the agreement used as the basis for the processing of Personal Data as referred to in paragraph (1).

(5) An agreement used as the basis for processing Personal Data as referred to in paragraph (1) may not be regarded as replacing consent as a basis for processing Personal Data under laws and regulations in the field of Personal Data Protection.

Article 41

(1) The fulfillment of contractual obligations may be used as the basis for processing Personal Data where:

a. there is a valid agreement between the Personal Data Controller and the Data Subject in accordance with laws and regulations;

b. there is a need for the processing of Personal Data by the Personal Data Controller to carry out the agreement;

c. Personal Data Protection measures to be provided to the Data Subject have been fulfilled;

d. the risks associated with the processing of Personal Data to the Data Subject have been assessed; and

e. the ability to fulfill the rights of Data Subjects and to carry out the obligations of the Personal Data Controller in the processing of Personal Data in accordance with the provisions of this Government Regulation has been considered.

(2) A valid agreement between the Personal Data Controller and the Data Subject as referred to in paragraph (1)(a) regarding the processing of Personal Data of a Child or a Person with a Disability must be made with the consent of the Child's parent and/or guardian as referred to in Article 38 and the consent of the guardian of the Person with a Disability as referred to in Article 39.

Article 42

(1) The processing of Personal Data in fulfillment of a request by the Data Subject as referred to in Article 40 paragraph (1) letter b shall be carried out subject to the following conditions:

a. there is a written or recorded request from the Data Subject to the Data Controller;

b. the Personal Data Controller and the Data Subject shall enter into an agreement that requires the processing of Personal Data; and

c. The agreement to be entered into by the Data Subject and the Data Controller shall serve as the basis for the exercise of the rights and fulfillment of the obligations of the Data Subject and the Data Controller.

(2) Once the agreement has been concluded, it may be used as the basis for processing Personal Data in accordance with Articles 40 and 41.

Article 43

(1) The agreement referred to in Article 41 must contain at least:

a. a detailed description of the purposes and an explanation of the purposes of the processing of Personal Data;

b. a description of the relationship between the purposes of processing Personal Data and the purposes of the agreement to be fulfilled;

c. the rights of the Data Subject and the obligations of the Personal Data Controller;

d. the types and characteristics of the needs or services to be provided to the Data Subject;

e. Consequences in the event that the Personal Data Controller fails to process Personal Data;

f. impact of the processing of Personal Data on the protection of the rights of Data Subjects;

g. the guarantee by the Personal Data Controller to process Personal Data in accordance with the provisions of laws and regulations in the field of Personal Data Protection;

h. the guarantee by the Personal Data Controller to fulfill the rights of Data Subjects; and

i. the parties involved in the processing of Personal Data.

(2) In the event that the agreement does not meet the provisions referred to in paragraph (1), the Personal Data Controller may not rely on the fulfillment of contractual obligations as the basis for processing Personal Data.

Article 44

A Personal Data Controller may not include or insert contractual clauses that shift liability to the Data Subject in accordance with the provisions of applicable laws and regulations.

Paragraph 4: Compliance with Legal Obligations

Article 45

(1) A Personal Data Controller may use the fulfillment of the Data Controller's legal obligations as a basis for processing Personal Data in accordance with applicable laws and regulations.

(2) fulfillment of legal obligations as

referred to in paragraph (1) includes:

a. court orders and/or rulings; or

b. orders or decisions of civil service officials issued in accordance with the provisions of laws and regulations.

Paragraph 5

Fulfillment of the Protection of Vital Interests

Article 46

A Personal Data Controller may use the processing basis of Personal Data in the form of safeguarding the vital interests of the Data Subject in the following cases:

a. there is a threat to the life, physical well-being, and/or property/assets of the Data Subject or another party; and

b. it is difficult to obtain consent from the Data Subject as referred to in subparagraph (a).

Article 47

(1) The Personal Data Controller shall inform the Data Subjects of the processing of Personal Data as referred to in Article 46.

(2) The information referred to in paragraph (1) shall include:

a. actions taken after the purpose of processing Personal Data has been fulfilled;

b. the types of threats that would arise to the Data Subject or other parties if the processing of Personal Data were not carried out; and

c. Other information in accordance with the provisions of this Government Regulation.

Article 48

Further provisions regarding the protection of the vital interests of Data Subjects as a basis for processing Personal Data shall be regulated by Agency Regulation.

Paragraph 6

Performance of Duties in the Interest of the Public, Public Service, or the Exercise of Authority

Article 49

(1) A Personal Data Controller may use the basis for processing Personal Data in the form of the performance of duties in the context of:

a. the public interest;

b. public service; or

c. the exercise of authority, in accordance with laws and regulations.

(2) The performance of duties as referred to in paragraph (1) shall be carried out in the context of implementing provisions of laws and regulations that require the Personal Data Controller to take a specific action.

Article 50

(1) In carrying out the duties referred to in Article 49, the Personal Data Controller must have adequate policy documents.

(2) The policy documents referred to in paragraph (1) must at least cover:

a. the scope of the performance of duties; and

b. Purpose of Personal Data Processing.

(3) Provisions regarding the drafting of the policy document referred to in paragraph (1) are set forth in the Agency Regulations.

Article 51

(1) The Personal Data Controller shall provide information regarding the processing of Personal Data based on the performance of duties as referred to in Article 49 to the Data Subject.

(2) The provision of information as referred to in paragraph (1) shall be carried out at the time the processing of Personal Data begins.

(3) Where the provision of information referred to in paragraph (1) could interfere with the protection of the public interest or public services, the information shall be provided when the purpose of processing Personal Data has been fulfilled.

(4) Where the information referred to in paragraph (1) cannot be provided directly, the Personal Data Controller shall provide it through announcements in electronic and non-electronic media.

Article 52

Further provisions regarding the performance of duties in the public interest, public service, or the exercise of authority as a basis for processing Personal Data shall be regulated by Agency Regulation.

Paragraph 7

Fulfillment of Other Legitimate Interests

Article 53

A Personal Data Controller may use the basis for processing Personal Data in the form of fulfilling other legitimate interests provided that:

a. having conducted an analysis of the necessity, purpose, and balance between the rights of the Data Subject and the interests of the Personal Data Controller, with the results of the analysis indicating that the Personal Data Controller has a legitimate interest in processing Personal Data; and

b. has assessed that the processing of Personal Data based on the fulfillment of other legitimate interests does not have any legal implications or cause harm to the Data Subject, and the Data Controller has implemented mitigation measures in the event that such processing results in any adverse effects.

Article 54

The results of the analysis and assessment referred to in Article 53 shall be documented by the Personal Data Controller.

Article 55

(1) A Personal Data Controller that is a Public Body may rely on other legitimate interests as a basis for processing Personal Data.

(2) The use of other legitimate interests as referred to in paragraph (1) is limited to purposes of processing Personal Data other than the performance of duties in the public interest, public service, or the exercise of the authority of a Public Body.

Article 56

(1) A Data Subject may request an explanation from the Personal Data Controller regarding the use of Personal Data to fulfill other legitimate interests as referred to in Article 53.

(2) Based on the request referred to in paragraph (1), the Personal Data Controller must provide an explanation to the Data Subject.

Article 57

Further provisions regarding the use of other legitimate interests as the basis for the processing of Personal Data are set forth in Agency Regulations.

Part Three

Limited and Specific Processing of Personal Data

Article 58

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

Article 59

(1) The limitation and specificity referred to in Article 58 shall be achieved by minimizing the Personal Data that is processed.

(2) The minimization of Personal Data processed as referred to in paragraph (1) shall be carried out by taking into account:

a. the relationship between the Personal Data being processed and the purpose of processing the Personal Data;

b. the adequacy of the Personal Data processed to achieve the purpose of processing the Personal Data; and

c. the Personal Data processed does not exceed what is necessary to achieve the purpose of processing the Personal Data.

Article 60

(1) The transparency referred to in Article 58 shall be ensured by:

a. ensuring that the Data Subject is aware of the Personal Data being processed;

b. ensuring that Data Subjects are aware of how Personal Data is processed; and

c. providing information and communication regarding the processing of Personal Data that is easily accessible, understandable, and uses clear language.

(2) The transparent processing of Personal Data as referred to in paragraph (1) must be carried out honestly and in good faith.

Part Four

Requests for and Provision of Information

Article 61

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

Article 62

(1) The Personal Data Controller must provide information regarding:
   a. the legal basis for 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. Retention Period for Personal Data;
   e. Details regarding the information collected;
   f. the duration of Personal Data processing; and
   g. the rights of the Data Subject.

(2) The obligation to provide information applies to all grounds for the processing of Personal Data as referred to in Article 30, paragraph (3).

(3) The information referred to in paragraph (1) shall be provided through a Personal Data Protection notice that is easily accessible to the Data Subject and remains available for as long as the Personal Data Controller processes Personal Data.

(4) The obligation to provide the information referred to in paragraph (2) shall be fulfilled by the Personal Data Controller prior to the processing of Personal Data.

(5) In the event of a change to the information referred to in paragraph (1), the Personal Data Controller is required to notify the Data Subject before the change takes effect.

Article 63

(1) The obligation to provide information as referred to in Article 62 also applies to the processing of Personal Data by Joint Data Controllers.

(2) In fulfilling the obligation to provide information as referred to in paragraph (1), the Joint Personal Data Controller shall also provide additional information containing at least:
   a. Information regarding the Joint Data Controllers involved in the joint processing of Personal Data;
   b. the relationship between the purposes of processing Personal Data controlled by each Personal Data Controller;
   c. the methods of processing Personal Data; and
   d. the jointly designated contact person.

Article 64

In the event that Personal Data is obtained indirectly from the Data Subject, the Personal Data Controller shall fulfill the obligation to provide the information as referred to in Article 62 paragraph (1) no later than 30 (thirty) days after the Personal Data is collected or obtained.

Article 65

The Personal Data Controller may not include an exoneration clause in the Personal Data Protection notice in accordance with the provisions of applicable laws and regulations.

Article 66

Further provisions regarding requests and the provision of information are regulated in Agency Regulations.

Part Five

Processing of Personal Data in Accordance with the Purpose

Article 67

(1) A Personal Data Controller is required to process Personal Data in accordance with the purpose of such processing.

(2) The purpose of processing Personal Data referred to in paragraph (1) must:

a. be limited to fulfilling specific purposes that have been explicitly and clearly communicated to the Data Subject; and

b. take into account the balance of interests of the Data Subject against the purposes of processing Personal Data.

(3) The Personal Data Controller shall identify the purposes of processing Personal Data as referred to in paragraph (2).

(4) In the event there are additional purposes and/or new purposes that differ from the original purpose of Personal Data processing, the Personal Data Controller is required to comply with the provisions set forth in this Government Regulation.

Article 68

(1) In fulfilling the obligations referred to in Article 67 paragraph (1), the Personal Data Controller must document the purposes of Personal Data processing and any changes thereto.

(2) In documenting as referred to in paragraph (1), the Personal Data Controller must explicitly state the purposes of processing Personal Data in:

a. the Personal Data Controller's internal policies; and

b. a Personal Data Protection notice that is easily accessible to the Data Subject.

Part Six

Accuracy, Completeness, and Consistency of Personal Data

Article 69

(1) The Personal Data Controller is obligated to ensure the accuracy, completeness, and consistency of Personal Data in accordance with 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.

(3) In fulfilling the obligation to conduct verification as referred to in paragraph (2), the Personal Data Controller shall first establish mechanisms and/or standards for data quality assurance.

(4) The verification referred to in paragraph (2) shall be conducted periodically and/or from time to time in accordance with the provisions of laws and regulations.

(5) The verification referred to in paragraph (2) shall be conducted at a minimum with respect to:

a. the accuracy and/or reliability of Personal Data;

b. the completeness of the Personal Data required to fulfill the purposes of processing Personal Data;

c. the type or uniformity of form, type, or format of Personal Data acceptable to the Personal Data Controller; and

d. the Data Controller's need to verify Personal Data periodically.

(6) Where the verification process requires the processing of Personal Data, the Personal Data Controller is obligated to implement Personal Data Protection in accordance with laws and regulations.

(7) In conducting the verification referred to in paragraph (2), the Personal Data Controller may cooperate with other Personal Data Controllers.

(8) The Personal Data Controller shall document the results of the verification of Personal Data as referred to in paragraph (2).

(9) Further provisions regarding the implementation of verification are set forth in the Agency Regulations.

Part Seven

Completion, Updates, and/or Corrections

Article 70

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

Article 71

(1) The Personal Data Controller is required to 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 to update and/or correct the Personal Data.

(2) In fulfilling the obligation to update and/or correct errors and/or inaccuracies in Personal Data as referred to in paragraph (1), the Personal Data Controller shall verify the exercise of the Data Subject's rights to ensure compliance with the purposes of Personal Data processing.

(3) The Personal Data Controller shall update and/or correct the Personal Data by replacing the original Personal Data with new Personal Data after the request referred to in paragraph (1) has been verified.

(4) In the event that it is not possible to replace the original Personal Data as referred to in paragraph (3), the update and/or correction of Personal Data may be carried out by creating an additional note.

(5) The Personal Data Controller may reject requests to update and/or correct Personal Data.

(6) The Personal Data Controller is required to notify the Data Subject of the results of the update and/or correction of Personal Data.

(7) A rejection of a request to update and/or correct Personal Data as referred to in paragraph (5) must be communicated to the Data Subject along with the reasons therefor in accordance with the provisions of laws and regulations.

Article 72

(1) In the event there are other Personal Data Controllers and/or Personal Data Processors, the obligation to update and/or correct Personal Data as referred to in Article 71 paragraph (1) includes the transmission of such updates and/or corrections to other Personal Data Controllers and/or Personal Data Processors.

(2) The disclosure of Personal Data by a Personal Data Controller to another Personal Data Controller as referred to in paragraph (1) is exempted if such disclosure is deemed impractical or would involve a disproportionate effort on the part of the Personal Data Controller.

Article 73

Further provisions regarding the completion, updating, and/or correction of Personal Data are set forth in the Agency Regulations.

Part Eight

Recording of Personal Data Processing Activities

Article 74

(1) The Personal Data Controller is required to maintain records of all Personal Data processing activities.

(2) The records of Personal Data processing activities referred to in paragraph (1) shall at a minimum include:

a. the name and contact details of the Personal Data Controller, Joint Personal Data Controller, and/or Personal Data Processor;

b. PPDP contact;

c. source collection and destination of Personal Data;

d. the basis for processing Personal Data;

e. the purpose of processing Personal Data;

f. Types of Personal Data;

g. Categories of Data Subjects;

h. parties other than the Personal Data Controller who may access Personal Data;

i. fulfillment of the Data Subject's rights;

j. mapping of Personal Data flows;

k. Retention Period;

l. technical and organizational measures to secure Personal Data; and

m. details of Personal Data transfers.

(3) In the event that the Personal Data Controller appoints a Personal Data Processor, the Personal Data Controller must ensure that the Personal Data Processor records the activities related to the processing of Personal Data.

(4) The record-keeping referred to in paragraph (3) does not eliminate the obligation of the Personal Data Controller to maintain records as referred to in paragraph (1).

(5) The record of Personal Data processing activities maintained by the Personal Data Processor as referred to in paragraph (3) shall at a minimum include:

a. the name and contact information of the Personal Data Processor;

b. the scope of Personal Data processing activities;

c. details of Personal Data transfers; and

d. a general description of the organizational and technical measures for securing Personal Data.

(6) The records of Personal Data processing activities as referred to in paragraph (1) shall be stored and managed in written form, either electronically or non-electronically.

(7) The records of Personal Data processing activities must be updated in the event of changes to Information as referred to in paragraphs (2) and (5).

(8) The records referred to in paragraphs (2) and (5), along with any amendments thereto as referred to in paragraph (7), shall be stored and managed by the Personal Data Controller and/or the Personal Data Processor in accordance with the provisions of applicable laws and regulations.

(9) If requested by the Agency, the Personal Data Controller and/or the Personal Data Processor must provide documentation of the records of Personal Data processing activities.

(10) When required for audit and oversight purposes, the Personal Data Controller and/or Personal Data Processor must provide the records of Personal Data processing activities.

Article 75

(1) The Personal Data Controller shall establish the Retention Period through a Retention Period policy document.

(2) The Retention Period policy document referred to in paragraph (1) shall contain at least:

a. definitions and periods of the Retention Period;

b. provisions governing the Retention Period under records retention rules and other provisions;

c. Regulated Data Subjects;

d. the types and components of Personal Data covered;

e. provisions regarding de-identification, if used for statistical and scientific research purposes;

f. methods of destruction by electronic and non-electronic means;

g. provisions for Personal Data Processors;

h. data controller;

i. documentation and notification; and

j. the legal basis for the regulation, if the retention period is due to a legal obligation in accordance with applicable laws and regulations.

Part Nine

Access to and Copies of Personal Data

Article 76

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

(2) Copies of Personal Data as referred to in paragraph (1) shall only be provided for Personal Data that does not affect the disclosure of other individuals' Personal Data.

Article 77

(1) The Personal Data Controller is obligated to grant access to the Data Subject within a period of no later than 3 x 24 (three times twenty-four) hours, calculated from the time the Personal Data Controller receives the access request from the Data Subject.

(2) The Personal Data Controller shall grant access to the Data Subject after verifying the access request as referred to in paragraph (1).

(3) The provision of access as referred to in paragraph (1) shall include at least:

a. access to the Personal Data being processed, along with the audit trail of Personal Data processing in accordance with the retention period for Personal Data;

b. Information provided by the Personal Data Controller regarding confirmation of access requests; and

c. access to and correction of Personal Data.

(4) The Personal Data Controller is required to refuse to grant the Data Subject access to or the right to amend Personal Data in the following cases:

a. endanger the safety, physical health, or mental health of the Data Subject and/or others;

b. resulting in the disclosure of another person's Personal Data; and/or

c. contradicts with the interests of national defense and national security.

Article 78

(1) Upon receipt of a request for a copy of Personal Data as referred to in Article 76(1), the Personal Data Controller must provide the applicant with a copy of the Personal Data at the earliest opportunity.

(2) In fulfilling the request for a copy as referred to in paragraph (1), the Personal Data Controller shall also confirm the request and notify the Data Subject of the timeframe required to provide the copy

of the Personal Data no later than 3 x 24 (three times twenty-four) hours from the time the request is received and verified.

(3) Where the requested copy of Personal Data cannot be provided, the Personal Data Controller shall notify the requester and provide the reasons.

Part Ten

Termination of Processing, Deletion, and Destruction of Personal Data

Article 79

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

(2) The erasure and/or destruction of Personal Data as referred to in paragraph (1) may be requested by the Data Subject concurrently with the termination of the Processing of Personal Data.

Article 80

(1) The Personal Data Controller is required to cease the processing of Personal Data in the following cases:

a. the Retention Period has been reached;

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 81

(1) The termination of the processing of Personal Data by the Personal Data Controller as referred to in Article 80 paragraph (1) shall be carried out by ceasing the processing of such Personal Data.

(2) The obligation to terminate the processing of Personal Data by the Personal Data Controller as referred to in paragraph (1) applies even if the processing of Personal Data involves other Personal Data Controllers and/or Personal Data Processors.

(3) The Personal Data Controller must notify the Data Subject of the termination of the processing of Personal Data as referred to in paragraph (1).

Article 82

(1) The Personal Data Controller is required to erase Personal Data in the following cases:

a. the Personal Data is no longer necessary to achieve the purpose 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. Personal Data was obtained and/or processed in an unlawful manner.

(2) The obligation to delete Personal Data obtained and/or processed unlawfully as referred to in paragraph (1)(d) shall apply where:

a. the collection and/or processing of Personal Data carried out by the Personal Data Controller constitutes an act that is unlawful in accordance with the provisions statutory regulations;

b. the Agency imposes an administrative sanction in the form of deletion; or

c. there is a court decision that has become final and binding.

(3) The obligation to delete Personal Data as referred to in paragraphs (1) and (2) applies even when the deletion of Personal Data involves other Personal Data Controllers and/or Personal Data Processors.

(4) The deletion of Personal Data as referred to in paragraphs (1) shall be carried out by deleting the Personal Data so that such Personal Data can no longer be accessed by anyone other than the Personal Data Controller.

Article 83

A Data Subject may not submit a request for the erasure of Personal Data if the withdrawal of consent for the processing of Personal Data, followed by the erasure of Personal Data, has already been carried out by the Data Controller as referred to in Article 82, paragraph (1), letter b.

Article 84

(1) The Personal Data Controller is required to destroy Personal Data in the following cases:

a. the Retention Period has expired and it is marked for destruction based on the records retention schedule;

b. there is a request from the Data Subject;

c. it is not related to the resolution of legal proceedings in a case; and/or

d. Personal Data is obtained and/or processed in an unlawful manner.

(2) The destruction of Personal Data as referred to in paragraph (1) shall be carried out by removing, erasing, or destroying Personal Data, whether electronic or non-electronic, so that it can no longer be used to identify the Data Subject.

(3) The obligation to destroy Personal Data by the Personal Data Controller as referred to in paragraphs (1) and (2) applies even when the destruction of Personal Data involves other Personal Data Controllers and/or Personal Data Processors.

Article 85

(1) The destruction of Personal Data upon request by the Data Subject as referred to in Article 84 paragraph (1)(b) may be carried out if the Retention Period has not yet expired.

(2) The Data Subject may not request the cancellation of the destruction or the restoration of Personal Data if the destruction of Personal Data based on the Data Subject's request has already been carried out by the Data Controller.

Article 86

(1) The deletion of Personal Data as referred to in Article 82 and/or loss of Personal Data as referred to in Article 84 shall be carried out in accordance with the provisions of applicable laws and regulations.

(2) The deletion and/or destruction referred to in paragraph (1) shall be carried out by at least:

a. identifying the Personal Data to be deleted and/or destroyed;
b. identifying the location(s) where the Personal Data to be deleted and/or destroyed is stored;
c. separating the Personal Data to be deleted and/or destroyed to prevent accidental deletion and/or destruction;
d. selection of an appropriate method for deleting or destroying Personal Data;
e. deletion and/or secure destruction of Personal Data;
f. preparation of a report on the deletion and/or destruction of Personal Data in an official record of deletion and/or destruction;
g. periodic audits to ensure that such Personal Data has been permanently deleted and/or destroyed;
h. reporting to the Agency in the event of a Failure of Personal Data Protection during the process of deleting and/or destroying Personal Data; and
i. periodic evaluation of the policy on the deletion and/or destruction of Personal Data and making changes as necessary to ensure compliance with applicable laws and regulations.

Article 87

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

(2) The notification of the deletion and/or destruction of Personal Data as referred to in paragraph (1) shall at a minimum include:
a. The Data Subject;
b. Information regarding the deletion and/or destruction Personal Data;
c. the types of Personal Data deleted and/or destroyed;
d. reason for deletion and/or destruction of Personal Data;
e. the effective date of deletion and/or destruction of Personal Data; and
f. Contact information for the Personal Data Controller.

(3) Notification to the Data Subject shall be provided before and after deletion and/or destruction of Personal Data in the cases referred to in Article 82(1)(a) and (d), and Article 84(1)(a), (c), and (d).

(4) Notification of the deletion and/or destruction of Personal Data to the Data Subject shall be provided after the deletion and/or destruction has been carried out in the cases referred to in Article 82(1)(b) and (c) and Article 84(1)(b).

(5) The notification referred to in paragraph (1) shall be provided no later than 3 x 24 (three times twenty-four) hours before or after the deletion and/or destruction of Personal Data is carried out.

(6) The deletion and/or destruction of Personal Data shall be carried out by the Personal Data Controller after the request from the Data Subject has been verified.

Article 88

(1) In the event that the Personal Data Controller appoints a Personal Data Processor, the Personal Data Controller must notify the Personal Data Processor and instruct the Personal Data Processor to delete and/or destroy the Personal Data.

(2) The notification to the Personal Data Processor as referred to in paragraph (1) must be provided prior to the notification to the Data Subject.

Article 89

Further provisions regarding the mechanisms for terminating the processing, deletion, and destruction of Personal Data are regulated by Agency Regulations.

Section Eleven: Withdrawal of Consent

Article 90

(1) 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 Personal Data Controller.

(2) Withdrawal of consent as referred to in paragraph (1) shall be carried out with ease of access and freedom of choice.

(3) The Personal Data Controller must provide a mechanism for the Data Subject to withdraw consent as referred to in paragraph (1).

Article 91

(1) The withdrawal of consent for the processing of Personal Data by the Data Subject does not invalidate the results of Personal Data processing that has already been carried out by the Personal Data Controller.

(2) The results of Personal Data processing that have been carried out by the Personal Data Controller prior to the withdrawal by the Data Subject as referred to in paragraph (1) may only be used in accordance with the provisions of laws and regulations.

Article 92

(1) The Personal Data Controller is obligated to cease the processing of Personal Data in the event that the Data Subject withdraws their consent to the processing of Personal Data.

(2) The cessation of Personal Data processing as referred to at 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 notification of the withdrawal of consent for the processing of Personal Data.

(3) The Personal Data Controller shall cease processing Personal Data after the request referred to in paragraph (2) has been verified.

(4) The Personal Data Controller must notify the Data Subject that the cessation of Personal Data processing has been carried out.

Part Twelve

Objections to Automated Processing

Article 93

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.

Article 94

(1) The Personal Data Controller must have mechanisms in place to respond to requests to object to decisions based solely on automated processing.

(2) The Personal Data Controller must provide adequate information regarding the technology used for decision-making based on automated processing and the consequences that the Data Subject will face.

(3) In response to a verified and accepted objection as referred to in Article 93, the Personal Data Controller shall provide an alternative method of processing Personal Data that involves human intervention and/or is not based on the results of automated processing.

Article 95

(1) The Personal Data Controller may reject an objection in the following cases:

a. there are no legal consequences and/or significant impacts on the Data Subject; and

b. the Personal Data Controller has excellent system accuracy and mitigation measures in place to prevent any impact on the Data Subject.

(2) The Personal Data Controller's rejection of an objection does not preclude the Data Subject's right to withdraw previously granted consent to the processing of Personal Data.

(3) The Personal Data Controller must notify the Data Subject of the rejection referred to in paragraph (1).

Article 96

Further provisions regarding automated processing shall be regulated by Agency Regulation.

Part Thirteen

Suspension and Restriction of Personal Data Processing

Article 97

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 98

The right referred to in Article 97 may be exercised where:

a. The Data Subject disputes the accuracy or truthfulness of the Personal Data processed by the Data Controller for a period of time sufficient to allow the Data Controller to verify the accuracy or truthfulness of said Personal Data;

b. The Personal Data was obtained and/or processed unlawfully, and the Data Subject does not request the erasure of the Personal Data but requests the suspension or restriction of the processing of the Personal Data; or

c. the Data Subject has a legal interest in bringing, pursuing, or defending against legal claims.

Article 99

(1) The Personal Data Controller is required to suspend and restrict the processing of Personal Data, in part or in full, no later than 3 x 24 (three times twenty-four) hours from receipt of the 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 of laws and regulations that do not permit the postponement or 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 postponement or restriction of the processing of Personal Data.

(3) The suspension and restriction of the processing of Personal Data as referred to in paragraph (1) shall be carried out by the Personal Data Controller after the Data Subject's request has been verified.

Article 100

(1) Based on the exceptions referred to in Article 99(2), the Personal Data Controller shall reject a request to suspend or restrict the processing of Personal Data, accompanied by reasons and consequences.

(2) The rejection referred to in paragraph (1) shall be communicated no later than 3 x 24 (three times twenty-four) hours from the time the verified request is received.

Article 101

When suspending and restricting the processing of Personal Data, the Personal Data Controller may only retain the Data Subject's Personal Data until the suspension and restriction expire or are terminated by the Data Subject.

Article 102

(1) In implementing the suspension and restriction of the processing of Personal Data as referred to in Article 101, the Personal Data Controller may:

a. temporarily transfer Personal Data to another system that is not connected to other Personal Data processing operations;

b. make the Personal Data inaccessible to other parties;

c. temporarily remove published Personal Data from websites managed by the Personal Data Controller; and/or

d. take other relevant corrective measures.

(2) Personal Data that has been marked as suspended and restricted Personal Data must be clearly identified in the system storing the Personal Data.

Article 103

(1) 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.

(2) The notification referred to in paragraph (1) shall be provided no later than 3 x 24 (three times twenty-four) hours after the suspension and restriction of the processing of Personal Data are carried out by the Personal Data Controller.

Article 104

Further provisions regarding the mechanism for postponing and restrictions on the processing of Personal Data are set forth in Agency Regulations.

Part Fourteen: Lawsuits and Compensation

Article 105

A Data Subject has the right to file a lawsuit and receive compensation for violations in the processing of Personal Data concerning him or her in accordance with the provisions of applicable laws and regulations.

Article 106

(1) A claim for damages arising from a violation in the processing of Personal Data shall be filed by the Data Subject with the Personal Data Controller.

(2) When filing a claim for compensation as referred to in paragraph (1), the Data Subject shall provide, at a minimum, the following information:

a. the identity of the Data Subject;

b. data, information, and/or documents provided as evidence by the Data Subject to file the claim for compensation; and

c. the legal relationship between the Data Subject and the Data Controller regarding the processing of Personal Data.

Article 107

The Personal Data Controller must have mechanisms and policies for handling claims for compensation.

Article 108

(1) The Personal Data Controller shall assess the request for compensation as referred to in Article 106.

(2) Based on the assessment referred to in paragraph (1), the Personal Data Controller shall provide a response to the request for compensation to the Data Subject.

(3) In the event that:

a. the response from the Personal Data Controller as referred to in paragraph (2) rejects the request for compensation; or

b. If no agreement is reached regarding compensation, the Data Subject may file a lawsuit in accordance with the provisions of applicable laws and regulations.

Article 109

Submission of a claim for compensation for a violation in the processing of Personal Data to the Personal Data Controller and/or Personal Data Processor that is a state public agency shall be carried out in accordance with the provisions of laws and regulations in the field of public administration.

Article 110

Further provisions regarding the handling and settlement of claims are governed by the Agency Regulations.

Part Fifteen

Portability and Interoperability of Personal Data

Article 111

(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 that is consistent with the structure and/or format commonly used or readable by an electronic system.

(2) The data subject has the right to use and transfer Personal Data concerning him or her to another Personal Data Controller, provided that the systems used can communicate with one another securely in accordance with the principles of Personal Data Protection.

(3) The exercise of the rights as referred to in paragraph (2) shall be made subject to the following provisions:

a. The basis for the processing of Personal Data is:

1. valid explicit consent from the Data Subject; or
2. the fulfillment of contractual obligations where the Data Subject is a party to the agreement or to fulfill a request from the Data Subject at the time of entering into the agreement; and

b. processing is carried out automatically.

Article 112

In fulfilling the right to obtain and/or use Personal Data as referred to in Article 111(1), and the right to use and transfer Personal Data as referred to in Article 111(2), the Personal Data Controller must take into account:

a. the ability of the Personal Data Controller to fulfill the rights of the Data Subject as communicated by the Personal Data Controller to the Data Subject; and

b. the provisions of laws and regulations regarding the prohibition of monopolistic practices and unfair business competition.

Article 113

Further provisions regarding the mechanisms for exercising the right to obtain and use portability and interoperability are set forth in the Agency Regulations.

Part Sixteen Notification of Failures of Personal Data Protection

Article 114

(1) In the event of a Failure of Personal Data Protection, 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 Agency.

(2) The notification period referred to in paragraph (1) shall be calculated from the time the Failure of Personal Data Protection is known with certainty, duly, and reasonably.

(3) The notification referred to in paragraph (1) shall contain at least the following:

a. the Personal Data disclosed;

b. when and how Personal Data was disclosed; and

c. measures taken by the Personal Data Controller to address and remedy the disclosure of Personal Data.

(4) The notification referred to in paragraph (1) must also include information regarding the PPDP or a contact person designated by the Personal Data Controller.

Article 115

(1) The Personal Data Controller is required to notify the public of a Failure of Personal Data Protection in the event that:

a. the Failure of Personal Data Protection disrupts public services; and/or

b. The Failure of Personal Data Protection has a serious impact on the public interest.

(2) The obligation to notify the public as referred to in paragraph (1) shall be carried out generally through electronic and/or non-electronic media.

Article 116

(1) The Personal Data Controller shall prepare documentation regarding the occurrence of a Failure of Personal Data Protection, which shall include at least the following:

a. the Personal Data affected by the Failure of Personal Data Protection;

b. a description of the Failure of Personal Data Protection;

c. the impact or consequences of the Failure of Personal Data Protection on the Data Subjects and the Personal Data Controller;

d. mitigation and recovery measures that have been, are being, and will be taken; and

e. the timeframe for notifying the Data Subjects and the Agency.

(2) Documentation regarding the occurrence of a Failure of Personal Data Protection prepared by the Data Controller as referred to in paragraph (1) shall be submitted to the Agency.

Article 117

(1) The Personal Data Controller shall establish and implement policies, procedures, and/or guidelines regarding the prevention and handling of Failures of Personal Data Protection that apply internally within the Personal Data Controller's organization.

(2) The policies, procedures, and/or guidelines referred to in paragraph (1) shall at a minimum include:

a. a division of roles and responsibilities for handling Failures of Personal Data Protection;

b. mechanisms for conducting analysis, classification, prioritization, monitoring, handling, and resolution of Failures of Personal Data Protection, including post-incident actions;

c. documentation of the handling of Failures of Personal Data Protection and mechanisms for reporting to Data Subjects and the Agency; and

d. periodic review and updating of the process for handling Failures of Personal Data Protection.

Article 118

In the event of a Failure of Personal Data Protection in the processing of Personal Data carried out by a Personal Data Processor, the Personal Data Processor must report the Failure of Personal Data Protection to the Personal Data Controller at the earliest opportunity.

Article 119

Further provisions regarding the notification of a Failure of Personal Data Protection are set forth in the Agency Regulations.

Part Seventeen

Personal Data Protection Impact Assessment

Article 120

(1) A 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) 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 the Data Subject;

b. processing of specific types of Personal Data;

c. processing of Personal Data on a large scale;

d. processing of Personal Data for systematic evaluation, scoring, or monitoring of Data Subjects;

e. the processing of Personal Data for the matching or merging of a group of data;

f. the use of new technologies in the processing of Personal Data; and/or

g. processing of Personal Data that restricts the exercise of Data Subjects' rights.

Article 121

(1) The obligation to conduct a Personal Data Protection Impact Assessment as referred to in Article 120, paragraph (1), shall be carried out prior to the processing of Personal Data.

(2) The Personal Data Protection Impact Assessment referred to in paragraph (1) shall at a minimum include:

a. a description of the Personal Data processing activities and the purposes of such processing, including the interests of the Personal Data Controller in processing the Personal Data;

b. an assessment of the necessity and proportionality between the purposes and activities of Personal Data processing;

c. an assessment of the risks to the rights of the Data Subject; and

d. measures taken by the Personal Data Controller to protect Data Subjects from the risks of processing Personal Data.

(3) The Personal Data Controller shall implement Personal Data Control Measures to protect Data Subjects from the risks associated with the processing of Personal Data as referred to in paragraph (2)(d) at the time such processing is carried out.

(4) The Personal Data Controller shall document the Personal Data Protection Impact Assessment along with the measures used by the Personal Data Controller to protect Data Subjects from the risks associated with the processing of Personal Data.

(5) The Personal Data Controller must review the Personal Data Protection Impact Assessment if there are changes in the risks associated with the processing of Personal Data.

(6) Where a PPDP has been appointed, the Personal Data Controller must consider and document the PPDP's advice when conducting the Personal Data Protection Impact Assessment.

Article 122

(1) A Personal Data Controller conducting a Personal Data Protection impact assessment as referred to in Article 121(1) may consult with the Agency in the event that:

a. The processing of personal data causes material and/or immaterial harm to the data subject; and/or

b. the unavailability of technical and operational measures.

(2) Further provisions regarding the Personal Data Protection impact assessment are set forth in the Agency Regulations.

Part Eighteen: Personal Data Security

Article 123

(1) The Personal Data Controller is obligated to protect and ensure the security of the Personal Data it processes by:

a. developing and implementing technical and operational measures to protect Personal Data from interference with the processing of Personal Data that is contrary to the provisions of laws and regulations; and

b. determining the security level of Personal Data by taking into account the nature and risks associated with the Personal Data to be protected during the processing of Personal Data.

(2) The development and implementation of the technical and operational measures referred to in paragraph (1)(a) shall be carried out by applying:

a. pseudonymization, encryption of Personal Data, and/or other technical measures capable of preventing or protecting against the risk of a Failure of Personal Data Protection;

b. ensuring that the systems and services used consistently provide Personal Data security and resilience in processing Personal Data;

c. ensuring that the systems and services used have the capability to restore access to and availability of Personal Data in a timely manner in the event of a physical or technical incident; and/or

d. having processes in place to conduct periodic testing, evaluation, and assessment to determine the level of effectiveness of technical and operational measures so as to ensure the security of Personal Data processing.

(3) The determination of the level of security for Personal Data as referred to in paragraph (1)(b) shall be made when there is a potential impact on the Data Subject, including at a minimum:

a. the unauthorized destruction of Personal Data;

b. unauthorized loss, alteration, or disclosure of Personal Data;

c. access to Personal Data that is stored, transmitted, or processed in any other form; and/or

d. violations in the processing of Personal Data.

(4) The formulation and implementation of technical and operational measures to protect Personal Data from the breaches of Personal Data processing referred to in paragraph (1)(a) shall be carried out in accordance with the security level determined by the Personal Data Controller.

(5) The Personal Data Controller shall conduct a compliance assessment of the formulation and implementation of the technical and operational measures referred to in paragraph (1)(a).

(6) The formulation and implementation of security levels shall be carried out in accordance with laws and regulations.

(7) The Agency shall formulate technical and operational measures and determine security levels in accordance with laws and regulations.

Article 124

(1) The formulation and implementation of technical and operational measures to protect Personal Data as referred to in Article 123(1)(a) shall begin at the planning stage of the Personal Data processing system and continue through the implementation of Personal Data processing.

(2) In carrying out the formulation and implementation of the measures referred to in paragraph (1), the Personal Data Controller must:

a. take into account technology, implementation costs, the nature, scope, context, and purposes of Personal Data processing, as well as the risks posed by such processing;

b. ensure, by default, that the Personal Data processed is limited to the Personal Data necessary for the purposes of processing; and

c. conduct risk assessments and implement the necessary safeguards to protect Personal Data on a regular and consistent basis.

Article 125

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

(2) The obligation to maintain the confidentiality of Personal Data as referred to in paragraph (1) includes ensuring that the Personal Data Processor appointed by the Personal Data Controller is capable of supporting the Personal Data Controller's obligation to maintain the confidentiality of Personal Data.

Article 126

(1) The Personal Data Controller is required to supervise every party involved in processing Personal Data under the Personal Data Controller's control.

(2) Parties involved in the processing of Personal Data and under the control of the Data Controller including:

a. Personal Data Processors;

b. a party that is a unit, work unit, or representative of the Personal Data Controller that carries out Personal Data processing activities on its own; and/or

c. other Personal Data Controllers involved in the processing of Personal Data.

Article 127

In carrying out the oversight obligations referred to in Article 126(1), the Personal Data Controller must have:

a. policies regarding the processing of Personal Data;

b. a Personal Data processing manual that sets forth the obligations and responsibilities regarding Personal Data protection; and

c. a reporting channel for the public.

Article 128

Further provisions regarding supervision by the Personal Data Controller as referred to in Article 126 and Article 127 are set forth in the Agency Regulations.

Article 129

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

Article 130

(1) The Personal Data Controller is required to prevent unauthorized access to Personal Data.

(2) Prevention as referred to in paragraph (1) shall be carried out in respect of Personal Data processed using electronic systems and/or processed electronically by using reliable, secure, and accountable electronic systems.

(3) The prevention measures referred to in paragraph (2) shall be carried out in accordance with the provisions of applicable laws and regulations.

Part Nineteen

Transfer of Personal Data in the Merger, Division, Acquisition, Consolidation, and/or Dissolution of a Legal Entity

Article 131

(1) The transfer of Personal Data may be carried out from the former Personal Data Controller to the new Personal Data Controller.

(2) The transfer of Personal Data as referred to in paragraph (1) shall be carried out in the event of a merger, demerger, acquisition, consolidation, or dissolution of a legal entity.

(3) Before the transfer referred to in paragraph (2) is carried out, the Personal Data Controller must assess:

a. the rights of Data Subjects that the Personal Data Controller is still obligated to fulfill during and/or after the process of merger, division, acquisition, consolidation, or dissolution of a legal entity; and

b. the obligations of the Personal Data Controller in the field of Personal Data Protection that must still be fulfilled by the Personal Data Controller during and/or after the process of merger, separation, acquisition, consolidation, or dissolution of a legal entity.

(4) The Personal Data Controller as referred to in Article 120 is required to update the Personal Data Protection impact assessment in accordance with the results of the assessment of the rights and obligations referred to in paragraph (3).

(5) Based on the assessment referred to in paragraph (3) and the Personal Data Protection Impact Assessment referred to in paragraph (4), the Personal Data Controller shall formulate technical and operational measures for transferring Personal Data from the former Personal Data Controller to the new Personal Data Controller where the Controller's obligations and/or the Data Subject's rights must be fulfilled during and/or after the merger, demerger, acquisition, or consolidation of a legal entity.

(6) The legal relationship between the former and new Personal Data Controllers in a merger, demerger, acquisition, consolidation, or dissolution of a legal entity as referred to in paragraph (2) shall be that of Joint Controllers of Personal Data until the process is deemed complete in accordance with laws and regulations.

Article 132

In the event that a Personal Data Controller in the form of a legal entity is dissolved or liquidated, the storage, transfer, or destruction of Personal Data shall be carried out in accordance with the provisions of applicable laws and regulations.

Article 133

(1) A Personal Data Controller in the form of a legal entity that undergoes a merger, demerger, acquisition, consolidation, or dissolution must provide notice of the transfer of Personal Data to the Data Subject.

(2) The obligation to notify the transfer of Personal Data as referred to in paragraph (1) applies to both the former and the new Personal Data Controller.

(3) The notice of transfer of Personal Data by the former Personal Data Controller as referred to in paragraph (2) shall at a minimum include:

a. Information that there will be a transfer of Personal Data from the former Personal Data Controller to the new Personal Data Controller;

b. the Personal Data processing activities that will be and have been carried out in connection with the merger, separation, acquisition, consolidation, or dissolution of a legal entity;

c. the name of the responsible legal entity, address, telephone number, and other contact information of the new Personal Data Controller;

d. the methods and procedures for submitting objections and/or requests to cease the processing of Personal Data, or for a Data Subject to refuse the transfer of Personal Data to the new Data Controller;

e. Information regarding when the processing of Personal Data for the purposes of the new Personal Data Controller's activities will begin;

f. Information that Personal Data may be accessed by the new Personal Data Controller and/or other parties involved in the merger, division, acquisition, consolidation, or dissolution of a legal entity; and

g. a statement that the former Personal Data Controller will destroy the Personal Data that has been transferred to the new Personal Data Controller upon the completion of the merger, division, acquisition, consolidation, or dissolution of the legal entity.

(4) The notice of transfer of Personal Data by the new Personal Data Controller as referred to in paragraph (2) shall contain at least the following:

a. Information that a transfer of Personal Data has occurred from the Data Controller to the new Data Controller;

b. the Personal Data processing activities that will be and have been carried out in connection with the merger, demerger, acquisition, consolidation, or dissolution of a legal entity;

c. The name of the responsible legal entity, address, phone number, and other contact information held by the new Personal Data Controller;

d. Information that the processing of Personal Data has been carried out in accordance with the original purpose by the former Personal Data Controller;

e. Information regarding when the processing of Personal Data for the purposes of the new Personal Data Controller's activities will begin;

f. the methods, procedures, and timeframes for submitting objections and/or requests to cease the processing of Personal Data, or the Data Subject's refusal to have their Personal Data transferred to the new Personal Data Controller; and

g. Information that Personal Data may be accessed by the new Personal Data Controller and/or other parties involved in the merger, division, acquisition, consolidation, or dissolution of a legal entity.

(5) The notification by the Personal Data Controller as referred to in paragraph (1) shall be provided before and after the merger, division, acquisition, consolidation, or dissolution of a legal entity takes effect.

(s) The former Personal Data Controller shall prepare the terms and conditions for access to Personal Data by other parties involved in the merger, division, acquisition, consolidation, or dissolution of a legal entity.

Article 134

(1) In a transfer of Personal Data resulting from a merger, demerger, acquisition, or consolidation of legal entities, the former and new Personal Data Controllers must enter into an agreement on Personal Data Protection.

(2) Agreement as referred to in paragraph (1) shall contain at least:

a. the basis for the processing of Personal Data by each Personal Data Controller;

b. compliance with the principles of Personal Data Protection;

c. compliance with the rights of Data Subjects; and

d. the division of duties and responsibilities among the former Personal Data Controller, the new Personal Data Controller, and parties involved in the processing of Personal Data.

(3) The agreement referred to in paragraph (1) may form part of the agreement underlying the merger, demerger, acquisition, or consolidation of legal entities.

(4) The agreement referred to in paragraph (1) must still comply with the provisions of the agreement that must be drafted and executed by the Joint Personal Data Controllers in accordance with the provisions of laws and regulations.

Article 135

(1) The obligation to process Personal Data in accordance with the purposes of Personal Data processing as referred to in Article 67 also applies to the new Personal Data Controller.

(2) A new Personal Data Controller may process Personal Data for the purposes of the new Personal Data Controller after the period for filing an objection by the Data Subject regarding the storage and processing of Personal Data by the most recent new Personal Data Controller has expired.

Article 136

(1) A Personal Data Controller in the form of a legal entity that is being dissolved must, in addition to transferring Personal Data as referred to in Article 133, also provide a notice to the Data Subject containing at least the following information:

a. that the dissolution of the Personal Data Controller has occurred, resulting in the deletion and/or destruction of Personal Data;

b. other parties that collaborate with the Personal Data Controller to process Personal Data; and

c. a contact person or Data Protection Officer (PPDP) designated to respond to questions or requests for information regarding the processing of Personal Data for a reasonable period of time.

(2) A Personal Data Controller that has been dissolved may appoint another party to serve as the contact person as referred to in paragraph (1)(c).

Article 137

(1) A Data Subject has the right to exercise the rights as provided for in applicable laws and regulations in the event of a merger, demerger, acquisition, consolidation, or dissolution of a legal entity.

(2) The exercise of a Data Subject's rights is carried out by submitting a request to exercise such rights, as provided for by applicable laws and regulations, to:

a. the former Personal Data Controller after the former Personal Data Controller has sent a notice regarding the impending merger, division, acquisition, consolidation, or dissolution of the legal entity, until such time as the merger, division, acquisition, consolidation, or dissolution of the legal entity takes effect; and

b. the new Personal Data Controller after the former Personal Data Controller has submitted notice that the merger, demerger, acquisition, consolidation, or dissolution of the legal entity has occurred.

Part Twenty

Responsible and Verifiable Processing of Personal Data

Article 138

(1) The Personal Data Controller is obligated to be accountable for the processing of Personal Data and to demonstrate accountability in fulfilling the obligations to implement the principles of Personal Data Protection.

(2) In fulfilling the accountability referred to in paragraph (1), the Personal Data Controller must, at a minimum:

a. establish and implement appropriate technical and organizational measures to fulfill accountability requirements;

b. document all activities Personal Data processing;

c. respond to requests for information from the Agency;

d. demonstrate compliance and provide documentation of all Personal Data processing activities; and

e. conducting internal and external Personal Data Protection audits.

Part Twenty-One

Obligations of the Personal Data Processor

Article 139

(1) In the event that the Personal Data Controller appoints a Personal Data Processor, the Personal Data Processor is obligated to process Personal Data in accordance with the instructions of the Personal Data Controller.

(2) The obligation to process Personal Data in accordance with the instructions of the Personal Data Controller as referred to in paragraph (1) must be documented and carried out in accordance with the agreement between the Personal Data Processor and the Personal Data Controller.

(3) In the event that a Personal Data Processor processes Personal Data outside the scope of the instructions and purposes specified by the Personal Data Controller, the processing of Personal Data becomes the responsibility of the Personal Data Processor.

Article 140

The provisions regarding the obligations of the Personal Data Controller as referred to in Article 69, Article 74, Article 123, Article 125, Article 126, Article 129, and Article 130 also apply to the Personal Data Processor.

Article 141

(1) The Personal Data Processor shall be responsible for the processing of Personal Data and shall demonstrate accountability in fulfilling its obligations in accordance with the provisions of laws and regulations.

(2) In carrying out the accountability referred to in paragraph (1), a Personal Data Processor must:

a. document all Personal Data processing activities;

b. respond to requests for information from the Agency;

c. demonstrate compliance and provide evidence of documentation for all Personal Data processing activities; and

d. conducts audits.

Part Twenty-Two

PPDP

Article 142

(1) The Personal Data Controller and the Personal Data Processor are required to appoint a PPDP to carry out personal data protection functions in the following matters:

a. the processing of Personal Data for the purposes of public services;

b. the core activities of the Personal Data Controller have a nature, scope, or purpose that requires regular and systematic monitoring of Personal Data on a large scale; and/or

c. the core activities of the Personal Data Controller consist of large-scale processing of specific Personal Data and/or Personal Data related to criminal offenses.

(2) Provisions regarding the obligation to appoint a Personal Data Protection Officer (PPDP) as referred to in paragraph (1) are further regulated in the Agency Regulations.

Article 143

(1) The PPDP who performs the Personal Data Protection functions as referred to in Article 142 paragraph (1) shall be appointed based on professionalism, knowledge of the law, Personal Data Protection practices, and the ability to fulfill their duties.

(2) Provisions regarding the professionalism and competence of the PPDP performing personal data protection functions are further regulated in the Agency Regulations.

Article 144

(1) The obligation to appoint a PPDP by a Personal Data Controller and/or a Personal Data Processor must take into account the structure, size, and organizational needs of the Personal Data Controller and the Personal Data Processor.

(2) The PPDP referred to in paragraph (1) may consist of an individual or several individuals from within and/or outside the Personal Data Controller or Personal Data Processor.

(3) Provisions regarding the appointment of the PPDP as referred to in paragraphs (1) and (2) are further regulated in the Agency Regulations.

Article 145

(1) The PPDP shall have at least the following duties:

a. informing and advising the Personal Data Controller or Personal Data Processor to comply with the provisions of the Law on Personal Data Protection;

b. monitor and ensure compliance with the provisions of laws and regulations in the field of Personal Data Protection 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), the PPDP shall take into account the risks associated with the processing of Personal Data, considering the nature, scope, context, and purpose of such processing.

Article 146

(1) To ensure the effective performance of the PPDP's duties as referred to in Article 145, the Personal Data Controller and/or Personal Data Processor must:

a. ensure that the PPDP is involved in all Personal Data processing activities;

b. ensure that the PPDP has direct reporting access to the highest level of management;

c. ensure that the PPDP operates objectively, free from interference, and independently in carrying out its duties in accordance with the provisions of laws and regulations;

d. provide adequate resources to enable the PPDP to fulfill its duties and maintain its level of expertise;

e. ensure that the PPDP has appropriate access to Personal Data processing activities;

f. providing appropriate access to other services to obtain important information related to the processing of Personal Data;

g. seek advice from the PPDP when conducting a Personal Data Protection Impact Assessment; and

h. document in detail the activities related to the PPDP's performance of duties.

(2) The Personal Data Controller and/or Personal Data Processor must ensure that the PPDP's duties do not result in a conflict of interest.

Article 147

(1) The PPDP must cooperate with the units, officials, or parties responsible for the processing of Personal Data.

(2) In cooperating with the parties referred to in paragraph (1), the PPDP must:

a. provide recommendations and advice to the units, officials, or parties responsible for the security of the processing of Personal Data processed by the Personal Data Controller so that the security of the processing of Personal Data is carried out in accordance with the provisions of laws and regulations;

b. take the necessary measures to ensure that units, officials, or parties responsible for the security of Personal Data processing carried out by the Personal Data Controller implement technical and operational measures that take into account the protection of the rights and freedoms of Data Subjects; and

c. report the performance of the units, officials, or parties responsible for the security of Personal Data processing to the leadership within the Personal Data Controller regarding the assessment by such units, officials, and/or parties of the implementation of technical and operational measures taking into account the protection of Data Subjects as required by the Personal Data Controller.

Section Twenty-Three: Exceptions to Rights and Obligations

Article 148

(1) The rights of Data Subjects as referred to in Article 79(1), Article 90(1), Article 93, Article 97, and Article 111 paragraph (1) and paragraph (2) are exempted for:

a. national defense and security interests;

b. the interests of the law enforcement process;

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 the Law.

(3) In the event of the implementation of the exceptions referred to in paragraph (1), the Agency may actively provide input in the drafting of sectoral regulations that contain exceptions to the rights of Data Subjects.

Article 149

(1) Obligations of Data Controller of Data as referred to in Article 71, paragraph (1) and paragraph (6), Article 77, paragraph (1), Article 80, Article 82, paragraph (1), subparagraph (a) through subparagraph (c), Article 84(1)(b), Article 87(1), Article 114(1)(a), and Article 125(1) shall not apply to:

a. national defense and security interests;

b. the interests of law enforcement;

c. the public interest in the context of state administration; or

d. the interests of oversight of the financial services, monetary, and payment systems sectors, and financial system stability, carried out in the context of state administration.

(2) The exemptions referred to in paragraph (1) shall be implemented solely for the purpose of enforcing the provisions of the Act.

(3) In the event of the implementation of the exceptions referred to in paragraph (1), the Agency may actively provide input in the drafting of sectoral regulations that include exceptions to the obligations of Personal Data Controllers.

Article 150

The application of exemptions to the rights of Data Subjects for the purposes of national defense and security as referred to in Article 148 paragraph (1) letter a and exemptions from the obligations of Personal Data Controllers for the purposes of national defense and security as referred to in Article 149 paragraph (1) letter a must meet the following criteria:

a. the processing of Personal Data is reasonably necessary and carried out in a proportionate manner, limited to fulfilling the interests of national defense and security;

b. there must be a lawful basis for the processing of Personal Data, and it must be demonstrated that the processing of Personal Data is carried out in accordance with the provisions of laws and regulations in the field of Personal Data Protection;

c. conducts an assessment of the balance between compliance with the provisions of laws and regulations in the field of Personal Data Protection and potential risks to national defense and security;

d. obtain a letter of certification from the relevant agency, ministry, or institution responsible for government affairs in the field of defense and security; and

e. have safeguards in place to prevent the unlawful misuse, transfer, and/or access to Personal Data.

Article 151

The application of exceptions to the rights of Data Subjects for the purposes of law enforcement as referred to in Article 148(1)(b) and exceptions to the obligations of Data Controllers for the purposes of law enforcement as referred to in Article 149(1)(b) must meet the following criteria:

a. the processing of Personal Data is reasonably necessary and carried out in a proportionate and limited manner to fulfill the purposes of law enforcement;

b. has a valid basis for processing Personal Data and can demonstrate that the processing of Personal Data is carried out in accordance with the provisions of laws and regulations in the field of Personal Data Protection;

c. conduct a balancing assessment between compliance with laws and regulations in the field of Personal Data Protection and the potential risks to law enforcement interests; and

d. has safeguards in place to prevent the misuse, transfer, and/or unlawful access to Personal Data.

Article 152

The application of exceptions to the rights of Data Subjects in the public interest for the purposes of state administration as referred to in Article 148(1)(c) and exceptions to the obligations of Data Controllers in the public interest for the purposes of state administration as referred to in Article 149(1)(c) must meet the following criteria:

a. the processing of Personal Data is reasonably necessary and carried out in a proportionate manner, limited to fulfilling the public interest in the context of the administration of the state;
b. there must be a valid basis for the processing of Personal Data, and it must be demonstrated that the processing of Personal Data is carried out in accordance with the provisions of laws and regulations in the field of Personal Data Protection;
c. it must conduct a balancing assessment between compliance with the provisions of laws and regulations in the field of Personal Data Protection and the potential risks to the public interest in the context of state administration; and
d. have safeguards in place to prevent the unlawful misuse, transfer, and/or access to Personal Data.

Article 153

Application of exceptions to the rights of Data Subjects for the purposes of oversight of the financial services, monetary, and payment systems sectors, as well as financial system stability, carried out in the context of state administration as referred to in Article 148 paragraph (1) letter d and the exemption of the obligations of the Personal Data Controller for the purposes of supervising the financial services, monetary, and payment systems sectors and financial system stability carried out in the context of state administration as referred to in Article 149 paragraph (1) letter d must meet the following criteria:

a. The processing of Personal Data is reasonably necessary and carried out in a proportionate and limited manner to fulfill the interests of oversight of the financial services sector, the monetary sector, payment systems, and financial system stability, which are carried out in the context of the administration of the state;
b. have a lawful basis for the processing of Personal Data and be able to demonstrate that the processing of Personal Data is carried out in accordance with the provisions of laws and regulations in the field of Personal Data Protection;
c. conduct a balancing assessment between compliance with the provisions of laws and regulations in the field of Personal Data Protection and the potential risks to the supervisory interests of the financial services, monetary, and payment systems sectors, as well as financial system stability, carried out in the context of state administration; and
d. have safeguards in place to prevent the unlawful misuse, transfer, and/or access to Personal Data.

Article 154

The application of the exception to rights for statistical and scientific research purposes as referred to in Article 148(1)(e) must meet the following criteria:

a. statistical and scientific research interests of a noncommercial nature;
b. having a lawful basis for the processing of Personal Data and being able to demonstrate that the processing of Personal Data is carried out in accordance with the provisions of laws and regulations in the field of Personal Data Protection;

c. conducting a balancing test between the purpose of processing Personal Data for statistical and scientific research purposes and the need to exempt the rights of the Data Subject;

d. the statistical or scientific research results are not used to evaluate or make decisions related to the Data Subject; and

e. have safeguards in place to prevent the misuse, transfer, and/or unlawful access to Personal Data.

Article 155

(1) For the purposes of handling criminal cases involving the protection of Personal Data, investigators, public prosecutors, or judges are authorized to request the Personal Data Controller and/or Personal Data Processor to provide the Personal Data they have processed in accordance with the provisions of laws and regulations.

(2) The request for Personal Data as referred to in paragraph (1) must be submitted in writing in a Personal Data request letter that clearly and specifically states at least the following:

a. the name and position of the investigator, public prosecutor, or judge;

b. the identity of the party indicated as a suspect or defendant;

c. a brief description of the alleged or charged criminal offense;

d. the types of Personal Data requested and their relevance to the handling of the criminal case regarding the Protection of Personal Data;

e. the retention period for Personal Data;

f. a statement confirming that the entity has established and implemented appropriate and adequate protection and security mechanisms in processing Personal Data in accordance with the provisions of laws and regulations in the field of Personal Data Protection; and

g. the legal basis for requesting Personal Data.

(3) The type of Personal Data requested as referred to in paragraph (2)(d) must be limited and relevant to the handling of the alleged or charged criminal case involving Personal Data Protection.

(4) The letter requesting Personal Data as referred to in paragraph (2) must be signed by:

a. the Chief of the Indonesian National Police, the regional police chief, the district police chief, or a designated official in the event the request is submitted by an investigator from the Indonesian National Police;

b. the head of an agency or institution, or a designated official in cases where the request is submitted by an investigator other than an investigator from the Indonesian National Police;

c. the Attorney General, the head of a high prosecutor's office, the head of a district prosecutor's office, the head of a branch of a district prosecutor's office, or a designated official in cases where the request is submitted by a prosecutor and/or a public prosecutor; or

d. the Chief Justice of the Supreme Court, the chief judge of a high court, or the chief judge of a district court hearing the case in question, if the request is submitted by a judge.

(5) A copy of the request letter referred to in paragraph (4) shall be sent to the head of the Agency.

Article 156

(1) Investigators, public prosecutors, or judges as referred to in Article 155 paragraph (1) may request assistance from the Agency in handling cases involving criminal offenses related to the Protection of Personal Data.

(2) The Agency provides assistance by offering opinions or recommendations, the implementation of which is carried out in accordance with the provisions of laws and regulations.

Article 157

(1) For the purposes of handling criminal cases involving the Protection of Personal Data, the Personal Data Controller and/or Personal Data Processor shall provide the processed Personal Data upon request from an investigator, public prosecutor, or judge as referred to in Article 155.

(2) The provision of Personal Data as referred to in paragraph (1) shall be carried out by ensuring the protection and security of the Personal Data provided in accordance with the provisions of laws and regulations.

Article 158

(1) In connection with the processing of Personal Data provided by the Personal Data Controller and/or Personal Data Processor in the handling of criminal cases involving the Protection of Personal Data as referred to in Article 157, the investigator, public prosecutor, and judges who process Personal Data for the purpose of handling criminal cases involving the Protection of Personal Data shall be deemed to be the Data Controllers of the Personal Data they process.

(2) The processing of Personal Data in the handling of criminal cases involving the Protection of Personal Data as referred to in paragraph (1) shall be carried out in accordance with the provisions of this Government Regulation.

Article 159

The exchange of personal data among law enforcement agencies in the handling of criminal cases involving the protection of personal data shall be carried out through mechanisms agreed upon based on cooperation among law enforcement agencies in accordance with the provisions of laws and regulations and the fulfillment of the obligation to protect personal data.

CHAPTER V

TRANSFER OF PERSONAL DATA OUTSIDE THE JURISDICTION OF THE REPUBLIC OF INDONESIA

Part One: General Provisions

Article 160

(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 Law on Personal Data Protection.

(2) In transferring Personal Data as referred to in paragraph (1), the Personal Data Controller making the transfer and the recipient of the transfer are required to ensure the protection of Personal Data in accordance with the provisions of laws and regulations in the field of Personal Data Protection.

(3) The transfer of Personal Data referred to in paragraph (1) shall meet the following criteria:

a. carried out by the Personal Data Controller in accordance with the provisions of laws and regulations;

b. The Personal Data Controller makes Personal Data available to the Personal Data Controller and/or the Personal Data Processor that receives the Personal Data; and

c. The Personal Data Controller and/or the Personal Data Processor receiving the Personal Data is located outside the jurisdiction of the Republic of Indonesia.

(4) In the event of a subsequent transfer of Personal Data, the Personal Data Controller and/or Personal Data Processor referred to in paragraph (2) must comply with the provisions of applicable laws and regulations.

Article 161

In carrying out the transfer of Personal Data as referred to in Article 160, the Personal Data Controller and/or Personal Data Processor must:

a. document and monitor the Personal Data transfer cycle and its implications;

b. ensure that the transferred Personal Data is adequate, relevant, and limited in accordance with the purpose of the transfer of Personal Data;

c. identify the instruments that are used as references for the Personal Data transfer process in accordance with the provisions of laws and regulations;

d. assess the effectiveness of the legal instruments used for the Personal Data transfer process to be carried out before transferring Personal Data;

e. use supplementary instruments if necessary, whether in the form of contractual, technical, and/or organizational instruments;

f. implementing procedural steps to be taken when utilizing supplementary instruments; and

g. conduct periodic re-evaluations at appropriate intervals.

Article 162

(1) The Personal Data Controller must conduct a legal instrument assessment before transferring Personal Data.

(2) The assessment of legal instruments referred to in paragraph (1) shall be conducted by taking into account:

a. the applicable regulatory basis;

b. the purpose of the transfer and processing of Personal Data;

c. the parties involved in the processing of Personal Data;

d. the scope of the sectors to which Personal Data is transferred;

e. the categories of Personal Data being transferred;

f. the chosen mechanism for transferring Personal Data;

g. storage location of Personal Data and access to Personal Data;

h. the format of the Personal Data to be transferred, for example, in plain text, hashed, or encrypted;

i. the possibility that Personal Data may be further transferred from the receiving country to another country;

j. measures to assess the risks or impacts on the rights of Data Subjects resulting from the transfer of Personal Data;

k. The Personal Data transferred is adequate, relevant, and limited to what is necessary for the purposes of the transfer; and

l. supplementary, procedural, and evaluation measures concerning the implementation of the transfer of Personal Data.

Article 163

The Personal Data Controller must assess the necessity of the transfer of Personal Data and the impact of such transfer on the rights of the Data Subject through a risk assessment of the transfer of Personal Data.

Article 164

(1) The Personal Data Controller must provide information to the Data Subject regarding the transfer of Personal Data before the transfer takes place.

(2) The information provided to the Data Subject regarding the transfer of Personal Data prior to the transfer, as referred to in paragraph (1), shall at a minimum include:

a. the purpose of transferring Personal Data outside the jurisdiction of the Republic of Indonesia;

b. the existence of Personal Data Protection mechanisms;

c. protection mechanisms related to the transfer of Personal Data to ensure that Data Subjects can exercise their rights; and

d. the risks associated with the transfer of Personal Data and the risk mitigation mechanisms implemented by the Personal Data Controller.

(3) In cases where the transfer of Personal Data is carried out to protect the vital interests of the Data Subject, the information referred to in paragraph (1) may be provided after the transfer of Personal Data has been carried out.

Article 165

(1) When transferring Personal Data as referred to in Article 160, the Personal Data Controller must ensure that the country where the Personal Data Controller and/or the 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 the Law on Personal Data Protection.

(2) In the event that the requirement referred to in paragraph (1) is not met, the Personal Data Controller must ensure that there is adequate and binding Personal Data Protection.

(3) Where the requirements in paragraphs (1) and (2) are not met, the Personal Data Controller must obtain the consent of the Data Subject.

(4) The Agency is authorized to assess fulfillment of the requirements for transferring Personal Data as referred to in paragraphs (1), (2), and (3).

Article 166

In the event that the exchange of Personal Data among law enforcement agencies takes place outside the jurisdiction of the Republic of Indonesia, the exchange of Personal Data shall be carried out in accordance with the provisions on the transfer of Personal Data in this Government Regulation.

Part Two

Equivalent or Higher Level of Personal Data Protection

Article 167

The assessment of an equivalent or higher level of Personal Data Protection as referred to in Article 165 paragraph (1) shall be conducted by the Agency.

Article 168

(1) The assessment of the level of personal data protection deemed equivalent or higher as referred to in Article 165(1) shall be conducted based on:

a. the country where the Personal Data Controller and/or Personal Data Processor receiving the transfer of Personal Data is located has laws and regulations in the field of Personal Data Protection;

b. the country where the Personal Data Controller and/or Personal Data Processor receiving the transfer of Personal Data is located has a Personal Data Protection supervisory agency or authority; and

c. the country where the Personal Data Controller and/or Personal Data Processor receiving the transfer of Personal Data is located has international commitments or is subject to other obligations arising from international agreements or legally binding instruments, as well as from its participation in multilateral or regional systems related to Personal Data Protection.

(2) In assessing the level of Personal Data Protection deemed equivalent or higher as referred to in paragraph (1), the Agency must establish a list of countries and/or international organizations that have an equivalent or higher level of Personal Data Protection.

(3) In the event that a transfer of Personal Data is made to a country and/or international organization included in the list referred to in paragraph (2), the Personal Data Controller may carry out the transfer of Personal Data while ensuring that it is conducted in accordance with the provisions of applicable laws and regulations.

(4) Further provisions regarding the procedures for assessing the level of Personal Data Protection deemed equivalent or higher as referred to in paragraph (1) are set forth in the Agency Regulations.

Part Three

Adequate and Binding Personal Data Protection

Article 169

(1) Adequate and legally binding Personal Data Protection as referred to in Article 165 paragraph (2) may take the form of:

a. a legally binding instrument that is enforceable against agencies or authorities based on their authority in accordance with the provisions of laws and regulations.

b. standard clauses for Personal Data Protection contracts;

c. binding corporate rules for a corporate group; and/or

d. other adequate and binding personal data protection instruments recognized by the Agency.

(2) The Personal Data Controller must demonstrate accountability in fulfilling the obligations to implement adequate and binding Personal Data Protection as referred to in paragraph (1) in the form of written and/or recorded documents submitted to the Agency.

(3) The existence of the documents as stipulated in paragraph (2) does not eliminate or diminish the Agency's authority to assess compliance with the requirements for the transfer of Personal Data.

Article 170

(1) The standard contract clauses for Personal Data Protection as referred to in Article 169 paragraph (1)(b) shall be established by the Agency.

(2) The standard Personal Data Protection contract clauses established by the Agency shall include at least:

a. definitions or terms;

b. Legal basis for the processing of Personal Data;

c. Personal Data Protection Clauses;

d. the obligation to provide notification in the event of a Failure of Personal Data Protection; and

e. the obligation to conduct due diligence on other parties receiving the transfer of Personal Data.

(3) In addition to the contractual clauses referred to in paragraph (2) that have been established by the Agency as referred to in paragraph (1), the Personal Data Controller may add provisions regarding the transfer of Personal Data in accordance with the needs of the transfer, provided that such provisions do not conflict with the Law on Personal Data Protection.

(4) In adding provisions regarding the transfer of Personal Data as referred to in paragraph (3), the Personal Data Controller may consult with the Agency.

Article 171

(1) Corporate regulations binding a corporate group as referred to in Article 169 paragraph (1)(c) shall at a minimum contain:

a. the obligation of the Personal Data Controller and/or Personal Data Processor receiving the transfer of Personal Data to provide Personal Data Protection that is equivalent to or higher than that stipulated in laws and regulations in the field of Personal Data Protection;

b. the parties bound by the binding corporate rules;

c. the determination of the destination countries and regions for the transfer of Personal Data based on such binding corporate rules; and

d. determining the division of roles, rights, and obligations of the parties involved.

(2) Binding corporate rules may only be used where:

a. the receiving Personal Data Controller controls or is controlled by the sending Personal Data Controller; and

b. the recipient's Personal Data Controller and the sender's Personal Data Controller are under the control of the same party.

(3) The use of binding corporate rules as referred to in paragraph (1) is subject to obtaining approval from the Agency prior to transferring Personal Data.

Article 172

Further provisions regarding the implementation of adequate Personal Data Protection that are binding are set forth in the Agency Regulations.

Part Four

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

Article 173

(1) In obtaining the consent of the Data Subject as referred to in Article 165 paragraph (3), the Personal Data Controller shall continue to fulfill its obligations in accordance with the provisions of laws and regulations.

(2) The transfer of Personal Data based on the consent of the Data Subject may only be carried out under the following conditions:

a. the transfer of Personal Data is not recurring;

b. the transfer of Personal Data involves a limited number of Data Subjects;

c. the transfer of Personal Data is necessary to fulfill the provisions that do not override the interests, rights, or freedoms of the Data Subject;

d. The Personal Data Controller has assessed the risks and implemented appropriate Personal Data Protection measures; and

e. The Personal Data Controller has informed the relevant authorities and the Data Subjects about the Personal Data transfer and the compelling legitimate interests served by such transfer.

Article 174

Further provisions regarding the implementation of consent for the transfer of Personal Data outside the jurisdiction of the Republic of Indonesia are set forth in the Agency Regulations.

CHAPTER VI

INTERNATIONAL COOPERATION

Article 175

International cooperation shall be carried out by the Government with the governments of other countries or international organizations regarding the protection of personal data.

Article 176

(1) International cooperation in the context of implementing this Government Regulation shall be carried out in accordance with the provisions of laws and regulations and the principles of international law.

(2) In carrying out the international cooperation referred to in paragraph (1), the Agency may provide input to the Ministry or other agencies.

(3) Provisions regarding the requirements and procedures for International Cooperation as referred to in paragraph (1) and the provision of input as referred to in paragraph (2) are regulated in the Agency Regulations.

Article 177

The Agency may cooperate with personal data protection agencies of other countries in resolving alleged cross-border personal data protection violations.

Article 178

(1) In carrying out the cooperation referred to in Article 177, the Agency may:

a. develop working procedures that facilitate the implementation of statutory provisions in the field of Personal Data Protection;

b. carry out cooperation in the form of mutual assistance; and/or

c. engage in other forms of cooperation for the purpose of resolving alleged cross-border violations of Personal Data Protection.

(2) Further provisions regarding cooperation related to Personal Data Protection as referred to in paragraph (1) are set forth in the Agency Regulations.

CHAPTER VII

PUBLIC PARTICIPATION

Article 179

(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 laws and regulations.

(3) Further provisions regarding the public's role as referred to in paragraph (2) are set forth in the Agency Regulations.

CHAPTER VIII

OVERSIGHT OF COMPLIANCE BY PERSONAL DATA CONTROLLERS

Article 180

(1) The Agency has the authority to supervise the compliance of Personal Data Controllers.

(2) Supervision of compliance as referred to in paragraph (1) includes monitoring, control, inspection, and investigation regarding alleged violations of Personal Data Protection.

(3) In carrying out compliance oversight as referred to in paragraph (2), the Agency may coordinate with ministries or agencies and/or involve public participation in accordance with the provisions of laws and regulations.

(4) Further provisions regarding the implementation of compliance oversight are set forth in the Agency Regulations.

Article 181

(1) The Agency has authority to issue orders to Personal Data Controllers and/or Personal Data Processors to follow up on the results of oversight.

(2) The orders referred to in paragraph (1) shall be issued in writing.

(3) The orders referred to in paragraph (1) are issued to:

a. fulfill the rights of Data Subjects;

b. fulfill the obligations of the Personal Data Controller and/or the Personal Data Processor;

c. cease or restrict the processing of Personal Data;

d. terminate or amend an agreement between the Personal Data Controller and the Personal Data Processor with a third party that is suspected of harming the Data Subject or the public;

e. to perform or refrain from performing certain activities in order to comply with the provisions of laws and regulations in the field of Personal Data Protection; and/or

f. to undertake or refrain from undertaking certain activities to prevent or mitigate harm to the Data Subject or the public.

(4) The Agency shall determine the timeframe for the implementation of orders in connection with follow-up actions on the results of supervision as referred to in paragraph (1).

(5) The timeframe referred to in paragraph (4) shall be determined based on supervisory needs and/or consideration of the complexity and scope of the order issued.

(6) In issuing the order referred to in paragraph (1), the Agency may require compliance with:

a. the formulation of an action plan and the implementation of the action plan; and/or

b. the submission of reports on the progress of the action plan's implementation, by the Personal Data Controller and/or the Personal Data Processor in following up on the order as part of the follow-up to the results of supervision.

(7) Further provisions regarding the issuance of orders as referred to in paragraph (1) are set forth in the Agency Regulations.

Article 182

In issuing the orders referred to in Article 181 to a Personal Data Controller that is a Public Agency, the Agency must take into account the provisions of laws and regulations that form the basis for the performance of the Public Agency's duties and functions.

Article 183

(1) The Agency is authorized to publish the results of Personal Data Protection oversight in accordance with laws and regulations.

(2) The publication shall be carried out through an open announcement and shall be accessible to the public.

CHAPTER IX

ADMINISTRATIVE SANCTIONS

Part One

Article 184

(1) Violations of Article 15(2), Article 29, Article 30(1), Article 33(1), Article 36(1), Article 38(2), Article 39(4), Article 58, Article 62(1) and (5), Article 67(1), Article 69(1) and (2), Article 71(1) and (6), Article 74(1), Article 77(1) and (4), Article 80(1), Article 82(1), Article 84(1), Article 87(1), Article 92(1), Article 99(1), Article 103(1), Article 114(1), Article 115(1), Article 120(1), Article 123(1), Article 125(1), Article 126(1), Article 129, Article 130(1), Article 133(1), Article 138(1), Article 139(1), Article 140, Article 142(1), Article 160(2), and Article 165(1), (2), and (3) 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. administrative fines.

(3) The competent authority may impose administrative sanctions on the Personal Data Controller and/or Personal Data Processor for administrative violations in accordance with the provisions of laws and regulations in the field of Personal Data Protection.

(4) The head of the Agency may delegate the authority referred to in paragraph (3) to an official of the Agency.

(5) The imposition of administrative sanctions as referred to in paragraph (3) may be carried out in coordination with the relevant Ministry or agency.

(6) The imposition of administrative sanctions as referred to in paragraph (2) shall be carried out by taking into consideration:

a. the severity or impact of the violation committed by the Personal Data Controller and/or the Personal Data Processor;

b. the continuity of business operations or public services of the Personal Data Controller and/or Personal Data Processor;

c. the compliance and/or compliance history of the Personal Data Controller and/or Personal Data Processor with the provisions of laws and regulations in the field of Personal Data Protection;

d. clear grounds and reasons; and

e. considerations other than those listed in subparagraphs a through d as determined by the Agency.

(7) Violations of the provisions referred to in paragraph (1) may be subject to more than one administrative sanction simultaneously.

(8) The administrative sanctions referred to in paragraph (2) may be imposed with or without the prior imposition of an administrative sanction in the form of a written warning.

Article 185

(1) An administrative sanction in the form of an administrative fine as referred to in Article 184(2)(d) shall be imposed at a maximum of 2% (two percent) of the annual income or annual receipts of the Personal Data Controller and/or Personal Data Processor, taking into account the variables of the violation.

(2) The violation variable referred to in paragraph (1) is calculated based on:

a. the negative impact caused by the violation;

b. the duration of the violation;

c. the type of Personal Data affected;

d. the number of affected Data Subjects;

e. the process of identifying the breach;

f. the level of transparency and cooperation of the Personal Data Controller and/or Personal Data Processor during the investigation;

g. the scale of operations of the Data Controller and/or Data Processor;

h. the ability of the Personal Data Controller and/or Personal Data Processor to pay;

i. the compliance of the Personal Data Controller and/or Personal Data Processor; and/or

j. other relevant variables determined by the Agency.

(3) Subject to certain considerations, the administrative fine referred to in paragraph (1) may be set as low as Rp0.00 (zero rupiah) or 0% (zero percent).

(4) The administrative fine referred to in paragraph (1) shall be calculated in accordance with laws and regulations on non-tax state revenue.

Article 186

(1) Administrative sanctions in the form of fines set forth in a decision of the Agency, which has become final and binding, constitute a payment obligation for the party subject to the administrative sanction and shall be deposited into the state treasury as non-tax state revenue.

(2) The settlement of the payment obligation referred to in paragraph (1) shall be carried out in accordance with the provisions of laws and regulations in the field of non-tax state revenue and in the field of state receivables.

Article 187

Further provisions regarding the procedures for imposing administrative sanctions shall be regulated by an Agency Regulation.

Part Two

Procedures for Handling Alleged Violations of Personal Data Protection

Paragraph 1

General

Article 188

The handling of alleged violations of Personal Data Protection shall be carried out through the following stages:

a. complaints or reports regarding alleged violations of Personal Data Protection, as well as the results of Personal Data Protection oversight;

b. examination and investigation of documents related to complaints or reports regarding alleged violations of Personal Data Protection;

c. examination and investigation of alleged violations of Personal Data Protection; and

d. the imposition and enforcement of decisions imposing administrative sanctions.

Paragraph 2

Complaints or Reports of Alleged Violations of Personal Data Protection

Article 189

(1) Alleged violations of Personal Data Protection may arise from:

a. complaints or reports; and/or

b. the results of Personal Data Protection oversight.

(2) The complaints or reports referred to in paragraph (1)(a) shall be submitted to the Agency.

(3) The information or report referred to in paragraph (1)(a) shall be submitted in writing and shall contain at least the following information:

a. the identity of the party filing the complaint or report;

b. the identity of the Personal Data Controller and/or Personal Data Processor who is the subject of the complaint or report;

c. the alleged Personal Data Protection violation, accompanied by the provisions of laws and regulations that have been violated; and

d. statements and/or evidence containing facts, data, or indications of the occurrence of a Personal Data Protection violation.

(4) Under certain circumstances, the identity of the party filing the complaint or report may be kept confidential.

(5) Further provisions regarding the procedures for filing complaints or reports of alleged violations of Personal Data Protection are set forth in the Agency Regulations.

Paragraph 3

Examination and Investigation of Complaint or Report Documents Regarding Alleged Violations of Personal Data Protection

Article 190

(1) The Agency shall examine and investigate complaint or report documents regarding alleged violations of Personal Data Protection as referred to in Article 188(a) within a maximum of 3 (three) days from the receipt of the complaint or report.

(2) If the examination referred to in paragraph (1) reveals insufficient information as referred to in Article 189(3), the Agency shall notify the complainant or reporter in writing to supplement the information.

(3) If the results of the investigation referred to in paragraph (1) require clarification or explanation regarding matters contained in the information as referred to in Article 189, paragraph (3), the Agency may summon the complainant or reporter to provide an explanation.

(4) If the results of the examination referred to in paragraph (1) conclude that there is sufficient information to follow up on the complaint or report of an alleged violation of Personal Data Protection, the Agency shall conduct an investigation.

(5) If the results of the examination referred to in paragraph (1) conclude that there is insufficient information to follow up on the complaint or report regarding an alleged violation of Personal Data Protection, the Agency may terminate the examination and notify the complainant or reporter.

(6) If the results of the investigation referred to in paragraph (1) conclude that the Agency lacks the authority to continue the investigation, the Agency shall convey the results of the investigation to the complainant or reporter, along with an explanation.

Article 191

In the event that a suspected violation of Personal Data Protection arises from the results of Personal Data Protection oversight as referred to in Article 189(1)(b), the Agency shall follow up by conducting an investigation and inquiry.

Paragraph 4

Investigation Based on an Inquiry into an Alleged Violation of Personal Data Protection

Article 192

(1) The Agency shall conduct an investigation and inquiry into alleged violations of Personal Data Protection as referred to in Article 190, paragraph (4), and Article 191.

(2) The inspection and investigation referred to in paragraph (1) shall be conducted against the Personal Data Controller and/or Personal Data Processor suspected of committing a Personal Data Protection violation.

(3) In conducting the examination and investigation referred to in paragraph (1), the Agency may:

a. summon and require the appearance of any person and/or public agency related to the alleged violation of Personal Data Protection;

b. request statements, data, information, and documents from any person and/or public agency regarding the alleged violation of personal data protection;

c. summon and have appear any experts necessary for the examination and investigation related to alleged violations of Personal Data Protection;

d. conduct inspections and investigations of electronic systems, facilities, rooms, and/or locations used by the Personal Data Controller and/or the Personal Data Processor, including gaining access to data and/or appointing third parties; and/or

e. taking actions to exercise its authority in accordance with the provisions of laws and regulations.

(4) In conducting inspections and investigations of Personal Data Controllers and/or Personal Data Processors as referred to in paragraph (2), the Agency may summon the Personal Data Controller and/or Personal Data Processor.

(5) The summons of the Personal Data Controller and/or Personal Data Processor as referred to in paragraph (4) shall be issued in writing no later than 3 (three) Days prior to the date of the inspection and audit of the Personal Data Controller and/or Personal Data Processor.

(6) The summons of any person and/or public entity related to an alleged violation of personal data protection as referred to in paragraph (3)(a) and/or experts required for the investigation and inquiry regarding an alleged violation of personal data protection as referred to in paragraph (3)(c) shall be issued in writing no later than 3 (three) days prior to the date of the investigation and inquiry into any individual, public agency, and/or expert.

(7) Inspections and investigations of electronic systems, facilities, rooms, and/or premises used by the Personal Data Controller and/or Personal Data Processor as referred to in paragraph (3)(d) must be conducted in a proportionate manner, accompanied by documents containing at least the following information:

a. legal basis;

b. purpose and scope;

c. a list of the electronic systems , facilities, premises, and/or locations used; and

d. the relevance between the electronic systems, means, spaces, and/or locations used and the alleged violation of Personal Data Protection by the Personal Data Controller and/or Personal Data Processor.

(8) In the event that the Agency requests the Personal Data Controller and/or Personal Data Processor to grant access to the data referred to in paragraph (3)(d), the request for access shall be made by providing information that includes, at a minimum:

a. the legal basis;

b. the purpose and scope;

c. a description of the types of Personal Data to which access is requested;

d. a description of the method of access to Personal Data; and

e. the period of access to Personal Data.

(9) In the event that the Agency appoints a third party to conduct inspections and investigations of the electronic systems, facilities, rooms, and/or premises used by the Personal Data Controller and/or Personal Data Processor as referred to in paragraph (3)(d), such appointment must be accompanied by a letter of assignment from the Agency.

(10) Inspection and investigation of alleged violations of Personal Data Protection shall be completed no later than 14 (fourteen) days from the date the inspection and investigation commence.

(11) If necessary, the period for the examination and investigation of an alleged violation of Personal Data Protection as referred to in paragraph (10) may be extended for a maximum of 60 (sixty) days.

Article 193

In the event that the results of the investigation and inquiry into the alleged violation of Personal Data Protection are not substantiated, the Agency shall:

a. terminate the investigation and inquiry process; and

b. notify in writing the party who filed the complaint or report, as well as the Personal Data Controller and/or Personal Data Processor who is the subject of the complaint or report.

Article 194

Further provisions regarding the procedures for investigation and inquiry into alleged violations of Personal Data Protection are set forth in the Agency Regulations.

Paragraph 5

Imposition and Enforcement of Decisions on the Imposition of Administrative Sanctions

Article 195

(1) The Agency shall issue a decision imposing administrative sanctions based on the results of the investigation and inquiry into alleged violations of Personal Data Protection no later than 30 (thirty) days from the date the investigation and inquiry are completed.

(2) The decision to impose administrative sanctions as referred to in paragraph (1) shall be announced on the Agency's official media.

(3) The announcement referred to in paragraph (2) shall be made in coordination with the relevant Ministry or agency.

(4) The decision to impose administrative sanctions as referred to in paragraph (1) shall be communicated to the Personal Data Controller and/or the Personal Data Processor.

(5) The Personal Data Controller and/or Personal Data Processor subject to administrative sanctions must implement the decision no later than 30 (thirty) days from the date of announcement.

(6) A Personal Data Controller and/or Personal Data Processor may request the Agency to extend the deadline for implementing the decision imposing administrative sanctions as referred to in paragraph (5).

(7) The extension of the period for implementing the decision to impose administrative sanctions as referred to in paragraph (6) is subject to the Agency's approval.

Article 196

A decision imposing administrative sanctions as referred to in Article 195 shall at a minimum contain:

a. the name and address of the Personal Data Controller and/or Personal Data Processor;

b. the type of Personal Data Protection violation;

c. the provisions violated;

d. the type of administrative sanction imposed on the Personal Data Controller and/or Personal Data Processor;

e. a description of the obligations or orders that must be carried out by the Personal Data Controller and/or Data Processor; and

f. the timeframe for fulfilling the obligations or instructions to be carried out by the Personal Data Controller and/or the Personal Data Processor.

Article 197

(1) A Personal Data Controller and/or Personal Data Processor subject to an administrative sanction may file a written objection with the head of the Agency no later than 14 (fourteen) days from the date of receiving notification of the decision.

(2) The filing of an objection as referred to in paragraph (1) does not suspend the enforcement of the administrative sanction.

(3) Based on the filing referred to in paragraph (1), the head of the Agency shall issue a decision on the objection no later than 14 (fourteen) days from the date the objection is received.

(4) The decision on the objection referred to in paragraph (3) shall be:

a. accepting the objection in part or in full; or

b. rejecting the objection accompanied with reason for the rejection.

(5) The decision on the objection shall be communicated to the Personal Data Controller and/or Personal Data Processor no later than 7 (seven) days from the date the decision is made.

(6) If the head of the Agency does not issue a decision on the objection within the time period referred to in paragraph (3), the objection shall be deemed granted.

(7) The deeming of the objection as granted, as referred to in paragraph (6), shall be carried out in accordance with the provisions of laws and regulations.

(8) In the event that the objection is rejected, the relevant Personal Data Controller and/or Personal Data Processor may file a lawsuit with the administrative court in accordance with the provisions of laws and regulations.

(9) The Head of the Agency may delegate the authority referred to in paragraph (3) to an official of the Agency.

Article 198

The Agency may submit a request for legal assistance to the public prosecutor's office for the purpose of following up on the implementation of a decision imposing administrative sanctions.

Article 199

Further provisions regarding the procedures for imposing and enforcing decisions on administrative sanctions are set forth in the Agency Regulations.

CHAPTER X

DISPUTE RESOLUTION

Part One

General

Article 200

(1) Dispute resolution shall be conducted through arbitration, court proceedings, or other alternative dispute resolution institutions in accordance with the provisions of laws and regulations.

(2) The applicable procedural law in dispute resolution and/or judicial proceedings regarding Personal Data Protection as referred to in paragraph (1) shall be carried out in accordance with the applicable procedural law as stipulated by laws and regulations.

Part Two

Facilitation of Dispute Resolution by Institutions

Article 201

(1) In the event of a dispute, the Data Subject, the Data Controller, and/or the Data Processor involved in the dispute may, in good faith, submit a report regarding the dispute to the Agency.

(2) The report referred to in paragraph (1) shall be submitted along with complete and accurate supporting documents and information, including:

a. the identity of the party submitting the report and the identity of the reported party;

b. a summary of the issue and a chronological account of the dispute;

c. a statement that there is no duplication of reports previously submitted to the Agency;

d. evidence related to the issue or dispute; and

e. an explanation or evidence of the complainant's legal standing.

(3) The report referred to in paragraph (2) shall be submitted in writing through an electronic or non-electronic system.

(4) Based on the report referred to in paragraph (3), the Agency shall assign a registration number to the party submitting the report.

(5) If the report does not meet the requirements referred to in paragraph (2), the Agency may refuse to follow up on the report.

Article 202

(1) Based on the report referred to in Article 201, the Agency shall verify the documents and information.

(2) In verifying the documents and information contained in the report referred to in paragraph (1), the Agency may:

a. summon the disputing parties;

b. request additional documents or information; and/or

c. exercise its powers in accordance with the provisions of laws and regulations.

(3) The results of the verification of documents and information regarding the report referred to in paragraph (1) shall be recorded in a written report.

(4) Further provisions regarding the verification procedure are set forth in the Agency Regulations.

Article 203

(1) Where verification of the documents and information in the report referred to in Article 202(1) reveals elements of a criminal violation of Personal Data Protection, the Agency may request the reporter to report the alleged offense to the Indonesian National Police.

(2) Reports of alleged criminal violations may be followed up with assistance provided by the Agency.

(3) The Agency shall provide the assistance referred to in paragraph (2) by submitting the results of the verification, the conduct of which shall be carried out in accordance with the provisions of laws and regulations.

Article 204

If the results of the verification of documents and information regarding the report referred to in Article 202, paragraph (1), reveal elements of an administrative violation, the Agency shall process the report for the purpose of administrative law enforcement.

Article 205

If the results of the verification of documents and information regarding the report referred to in Article 202, paragraph (1), do not reveal any elements of a criminal offense and/or elements of an administrative violation, the Agency shall facilitate the disputing parties in the resolution of the dispute.

Part Three

Dispute Resolution Efforts

Article 206

(1) The Agency's facilitation of dispute resolution shall prioritize Mediation.

(2) The Institution shall facilitate the resolution of disputes through mediation based on reports and the results of verification regarding the disputes between the disputing parties, as referred to in Article 205.

(3) The dispute resolution process referred to in paragraph (1) is exempted in the following cases:

a. the matter in dispute is not included in the Dispute; or

b. The Disputing Parties have specified a dispute resolution mechanism in the agreement.

(4) In facilitating the resolution of Disputes through Mediation, the Agency determines which Disputes may be resolved through Mediation.

Article 207

(1) In the mediation process, the disputing parties may appoint a mediator to resolve the dispute.

(2) The Mediator referred to in paragraph (1) must be from:

a. a Mediator registered with the Agency; or

b. a mediation institution registered with the Agency.

(3) The disputing parties may appoint a mediator registered with the Agency to resolve the dispute.

(4) In the event that the Agency does not yet have a Mediator or a Mediator is not available, the parties may appoint a Mediator from a Mediation Institution as referred to in paragraph (2)(b).

(5) A Mediator as referred to in paragraph (1) must report the appointment to the head of the Agency in writing through an electronic or non-electronic system.

(6) Provisions regarding the procedures for registration of Mediation Institutions are set forth in the Agency Regulations.

Article 208

(1) In the event that the disputing parties fail to reach an agreement on the appointment of a Mediator, the disputing parties shall submit the matter of appointing a Mediator to the head of the Agency to appoint a Mediator from the list of Mediators as referred to in Article 207 paragraph (2).

(2) The head of the Agency shall issue a decision containing an order to conduct Mediation and appointing a Mediator.

(3) The head of the Agency may delegate the authority referred to in paragraphs (1) and (2) to an official of the Agency.

Article 209

(1) Resolution of Disputes through Mediation must be based on the principle of:

a. low cost;

b. effectiveness;

c. beneficial;

d. affordable access;

e. prioritizing a balance between the interests of the Disputing Parties;

f. confidential and private; and

g. fairness and propriety.

(2) The mediator may conduct dispute resolution in person or online, allowing the disputing parties to see and hear one another and participate in the meeting.

(3) In-person mediation as referred to in paragraph (2) shall be conducted at the Agency's office or another location designated by the Agency's leadership.

(4) In the event that the disputing parties appoint a mediator from a mediation institution as referred to in Article 207, paragraph (2), letter b, the disputing parties must conduct the mediation process in accordance with the procedures and rules set forth in this Government Regulation.

Article 210

Mediator fees and mediation administration costs from:

a. the Agency; or

b. the Agency Mediation, as referred to in Article 207, paragraph (2), is governed by the Agency.

Part Four: Mediation Procedures

Article 211

(1) The mediator shall determine the date of the first mediation session.

(2) The first meeting referred to in paragraph (1) shall be scheduled no later than 10 (ten) days after the mediator is appointed.

(3) At the first mediation session attended by the disputing parties, the mediator may request the disputing parties to resolve the dispute between them through negotiation.

(4) The negotiations referred to in paragraph (3) shall be conducted no later than 14 (fourteen) days after the request for negotiations is received.

Article 212

(1) The negotiation process shall be closed and confidential.

(2) During the negotiation process, the disputing parties may draft joint minutes or notes of the negotiations based on a mutual agreement among the disputing parties.

(3) If the disputing parties reach an agreement during the negotiation process, they shall draft and sign a settlement agreement.

(4) The Disputing Parties shall submit the Settlement Agreement referred to in paragraph (3) to the Mediator for signature by the Disputing Parties and the Mediator.

(5) The Mediator must ensure that the Settlement Agreement does not contain provisions that:

a. contradict the law, public order, and/or public morality;

b. are detrimental to a third party; or

c. are unenforceable.

(6) The Settlement Agreement referred to in paragraph (4) is binding on the Disputing Parties.

(7) The Disputing Parties, through the Mediator, may submit the Settlement Agreement to the competent court to obtain a settlement deed in accordance with the provisions of applicable laws and regulations.

Article 213

(1) In the event that the Disputing Parties fail to reach an agreement during the negotiation process, the Disputing Parties must notify the Mediator of such disagreement in writing via electronic or non-electronic means.

(2) Based on the notification referred to in paragraph (1), the Mediator shall schedule a follow-up mediation session.

(3) Within a maximum period of 5 (five) days from the date the follow-up mediation session is scheduled, each party must submit a summary of the issues to the other party and to the Mediator.

(4) The disputing parties may submit the minutes or notes of the negotiations as referred to in Article 212, paragraph (2).

(5) The Mediator may use the minutes or notes of the negotiations referred to in paragraph (4) for the purposes of the mediation.

Article 214

In a follow-up mediation session as referred to in Article 213(2), the Mediator must explain to the Disputing Parties at least:

a. the definition and benefits of mediation;

b. the principles of mediation and the role of the mediator;

c. the stages of mediation;

d. the obligation of the disputing parties to attend the mediation session in person, as well as the legal consequences of acting in bad faith during the mediation process;

e. costs that may arise in connection with the appointment of a mediator; and

f. the obligation of the disputing parties to sign the mediation agreement and explanation forms.

Article 215

(1) The disputing parties must attend mediation sessions in person, with or without their legal counsel.

(2) The online participation of the disputing parties shall be considered their in-person participation in the mediation process and meetings.

Article 216

(1) The absence of one of the disputing parties from the mediation process is permitted only for valid reasons.

(2) Valid reasons as referred to in paragraph (1) include:

a. health conditions that prevent attendance at the mediation session, as evidenced by a doctor's certificate;

b. a Data Subject who is a minor or under guardianship, and the relevant guardian is unable to attend the meeting for a valid reason; and/or

c. the performance of official duties, professional obligations, or work that cannot be abandoned.

Article 217

(1) The Disputing Parties, with or without their legal representatives, must participate in mediation in good faith.

(2) The mediator may declare that a disputing party, the disputing parties, and/or their legal representatives are acting in bad faith in the matter at hand:

a. failing to appear after being duly summoned 2 (two) consecutive times to a mediation session without a valid reason as referred to in Article 216(2);

b. attending the first mediation session but failing to attend subsequent sessions despite having been duly summoned two (2) times in a row without a valid reason as referred to in Article 216 paragraph (2);

c. repeated absence that disrupts the mediation session schedule without a valid reason as referred to in Article 216(2);

d. attending a mediation session but failing to submit and/or respond to the other party's case summary; and/or

e. failing to sign the draft Settlement Agreement that has been agreed upon without a valid reason as referred to in Article 216(2).

(3) The mediator may terminate the mediation and declare that the mediation has failed to reach an agreement if any party fails to act in good faith as referred to in paragraph (2).

(4) The mediator shall submit a written report on the results of the mediation via an electronic or non-electronic system as referred to in paragraph (3) to the head of the Agency.

(5) The submission of the report to the head of the Agency as referred to in paragraph (4) does not constitute a violation of the principles of mediation as referred to in Article 209, paragraph (1).

(6) The disputing parties may follow up on the results of mediation that failed to reach an agreement and was terminated as referred to in paragraph (3) by:

a. resolving the dispute through arbitration or in court; or

b. discontinuing the dispute.

Article 218

(1) Mediation shall be conducted within a maximum period of 30 (thirty) days from the date of the first mediation session.

(2) The mediation period referred to in paragraph (1) may be extended one (1) time based on an agreement between the disputing parties.

(3) The extension referred to in paragraph (2) shall be submitted by the Mediator to the head of the Agency no later than 7 (seven) Days before the period referred to in paragraph (1) expires, by submitting:

a. the agreement of the disputing parties to extend the mediation period; and

b. the reasons for the extension.

(4) Based on the request for an extension as referred to in paragraph (3), the head of the Agency may grant an extension of the mediation for a maximum of 30 (thirty) days , effective as of the expiration of the period referred to in paragraph (1).

(5) In the event that the Disputing Parties are unable to resolve the Dispute through Mediation within the time period referred to in paragraph (4), the Mediation shall be deemed to have failed to reach an agreement.

(6) The mediator shall submit a written report on the results of the mediation via an electronic or non-electronic system to the head of the institution.

(7) Submission of the report referred to in paragraph (6) does not constitute a violation of the principles of Mediation as referred to in Article 209(1).

Article 219

(1) With the consent of the disputing parties and/or their legal representatives, the mediator may call upon one or more experts, third parties, and/or community leaders.

(2) Before the Mediator calls upon experts, third parties, and/or community leaders, the Disputing Parties must first reach an agreement regarding whether the explanations and/or assessments of the experts, third parties, and/or community leaders shall be binding or non-binding.

Article 220

(1) If the disputing parties successfully reach an agreement through mediation, they shall set forth such agreement in writing in a Settlement Agreement with the assistance of the Mediator, and it shall be signed by the disputing parties and the Mediator.

(2) In drafting the Settlement Agreement as referred to in paragraph (1), the Mediator shall ensure that the Settlement Agreement does not contain any provisions that:

a. contravene the law, public order, and/or public morals;

b. are detrimental to third parties; or

c. are unenforceable.

(3) In the event that the mediation process is represented by legal counsel for the disputing parties, the Settlement Agreement may only be signed if there is a written statement from the disputing parties containing their consent to the agreement reached.

(4) The Settlement Agreement referred to in paragraph (1) is binding on the Disputing Parties.

(5) The disputing parties, through the mediator, may submit the settlement agreement to the competent court to obtain a settlement deed in accordance with the provisions of applicable laws and regulations.

Article 221

(1) The Agency may request legal assistance from the public prosecutor's office in resolving disputes.

(2) A request for legal assistance from the prosecutor's office as referred to in paragraph (1) shall be carried out in accordance with the provisions of applicable laws and regulations.

Article 222

Further provisions regarding the resolution of disputes through the Agency and the competence of mediators are set forth in the Agency Regulations.

CHAPTER XI

TRANSITIONAL PROVISIONS

Article 223

Until the enactment of the Agency Regulations regarding the processing of Personal Data, the Personal Data Controller and/or the Personal Data Processor shall process Personal Data provided that such processing does not conflict with the provisions of this Government Regulation.

CHAPTER XII

FINAL PROVISIONS

Article 224

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

Article 225

This Government Regulation shall take effect 6 (six) months from the date of its promulgation.

To ensure that everyone is aware of this, I hereby order the promulgation of this Government Regulation and its publication in the Official Gazette of the Republic of Indonesia.

Issued in Jakarta

on July 16, 2026

THE PRESIDENT OF THE REPUBLIC OF INDONESIA

signed

PRABOWO SUBIANTO

Promulgated in Jakarta on July 16, 2026

MINISTER OF STATE SECRETARY OF THE REPUBLIC OF INDONESIA

signed

PRASETYO HADI

OFFICIAL GAZETTE OF THE REPUBLIC OF INDONESIA, YEAR 2026, NUMBER 88

[Certification appearing in the Indonesian source copy]

Certified true copy

MINISTRY OF THE STATE SECRETARIAT

REPUBLIC OF INDONESIA

Deputy for Legislation and Legal Administration

Anna Djaman