LAW OF THE REPUBLIC OF INDONESIA

NUMBER ... OF ...

ON

PERSONAL DATA PROTECTION[1]

BY THE GRACE OF GOD ALMIGHTY

PRESIDENT OF THE REPUBLIC OF INDONESIA,

Considering:

a. that personal data protection is one type of human rights which is a part of self-protection, it needs to be granted with robust legal basis to provide security over personal data, based on the 1945 Constitution of the Republic of Indonesia;
b. that personal data protection is aimed to ensure the rights of the citizens over self-protection and grow public mindset, as well as guarantee the recognition and respect on the importance of personal data protection;
c. that currently, frameworks on data protection available under several laws and regulations, thus in order to improve effectiveness in the implementation of personal data protection, it needs framework on personal data protection on law level;
d. that based on considerations as referred to in letter a, letter b, and letter c, it needs formulation of Law on Personal Data Protection;

In view of:

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

With the Mutual Agreement of

[*] This edition of Law on Personal Data Protection was published on 29 April 2019. This translation is created with the best effort as can be offered and by any means, does not constitute and should not be treated as official translation or sworn translation for legal proceeding purposes. The copyright owner: 1) Should not be held liable for any error which occurs in the source document; 2) Reserves the right to change and modify this translation, with subsequent notifications given to every clients in timely manner; and 3) May seek redress for any unlawful or unauthorized transfer or disclosure of this translation against any party.

HOUSE OF REPRESENTATIVES OF THE REPUBLIC OF INDONESIA

and

PRESIDENT OF THE REPUBLIC OF INDONESIA

HAVE DECIDED:

To enact:

LAW ON PERSONAL DATA PROTECTION.

CHAPTER 1
GENERAL PROVISIONS

Article 1

Under this Law, the following definitions are employed:

1. Personal Data is every data in regards to natural person, either identified and/or identifiable, individually or combined with another information, either directly or indirectly through electronic and/or non-electronic systems.
2. Information is statement, declaration, idea, and signs which contain value, meaning and message, either data, fact, or explanation which may be seen, heard, and read that is displayed in any container and format in accordance with the development of information-technology and communication, electronically or non-electronically.
3. Personal Data Controller is the party who determines the purpose and perform control on Personal Data processing.
4. Personal Data Processor is the party who perform Personal Data processing on behalf of Personal Data Controller.
5. Any Person is individual or Corporation.
6. Personal Data Owner is individual who acts as data subject who legally owns Personal Data.

7. Sectoral Supervisory and Regulatory Institution is institution who has the duty to supervise the implementation of certain sectoral duties and issue framework on such sector in accordance with provisions under laws and regulations.
8. Public Body is executive, legislative, judicative bodies, and other bodies which have the main functions and duties in relation to state organization, which part or all of its funds sourced from State Budget and/or Regional Budget, or non-governmental organizations insofar that a part or all of its funds sourced from State Budget and/or Regional Budget, public and/or international donations.
9. Corporation is an organized body of people and/or assets, both incorporated and unincorporated entities.
10. Minister is minister who organizes governmental affairs within communication and informatics sector.

Article 2

This Law prevails for Any Person, Public Body, and organization/institution which performs legal acts as addressed under this Law, either situated in the territories of the Unitary State of the Republic of Indonesia or outside the territories of the Unitary State of the Republic of Indonesia, which have legal effects in the territories of the Unitary State of the Republic of Indonesia and/or outside the territories of the Unitary State of the Republic of Indonesia and harm the interests of the Unitary State of the Republic of Indonesia.

CHAPTER 2
TYPES OF PERSONAL DATA

Article 3

(1) Personal Data consist of:
   a. General Personal Data; and
   b. Specific Personal Data.

(2) General Personal Data as referred to in paragraph (1) letter a may be generally obtained through public service access or as contained in the official identity, of which, any unlawful disclosure may harm Personal Data Owner.

(3) Specific Personal Data as referred to in paragraph (1) letter b refers to Personal Data which is sensitive toward the life security and convenience of Personal Data Owner, which acquisition may only be based on consent of Personal Data Owner, unless addressed otherwise based on this Law, of which, unlawful disclosure may breach the privacy of Personal Data Owner.

CHAPTER III
RIGHTS OF PERSONAL DATA OWNER

Article 4

Personal Data Owner has the right to request information on the clarity of identity, basis of legal interests, purpose of the request and utilization of Personal Data, and accountability of the party who requests Personal Data.

Article 5

Personal Data Owner has the right to complete its Personal Data before being processed by Personal Data Controller.

Article 6

Personal Data Owner has the right to access and obtain copy of its Personal Data.

Article 7

Personal Data Owner has the right to update and/or rectify error and/or inaccuracy of its Personal Data.

Article 8

Personal Data Owner has the right to terminate the processing, erase, and/or destruct its Personal Data.

Article 9

Personal Data Owner has the right to withdraw consent for the processing of its Personal Data which has been initially granted.

Article 10

Personal Data Owner has the right to file objection against surveillance acts and/or automatic profiling.

Article 11

Personal Data Owner has the right to choose or abstain from the processing of Personal Data through pseudonym mechanism for specific purposes.

Article 12

Personal Data Owner has the right to delay or restrict the processing of Personal Data proportionally in accordance with the purpose of the processing of Personal Data in question.

Article 13

Personal Data Owner has the right to claim and receive redress for its Personal Data breach in accordance with provisions under Laws and Regulations.

Article 14

(1) Personal Data Owner has the right to obtain its Personal Data in the form which is in accordance with the structure and/or storage format which is commonly used or readable by machine or hardware that is used within the interoperability among electronic systems.
(2) Personal Data Owner has the right to use and transfer its Personal Data to other Personal Data Controller, provided that such system may securely communicate with each other in accordance with Personal Data protection principles.

Article 15

Exercise of rights of Personal Data Owner as referred to under Article 6 up to Article 10 and Article 12 is invoked through written request to the Personal Data Controller.

CHAPTER IV
PROCESSING OF PERSONAL DATA

Division One
General

Article 16

(1) Processing of Personal Data encompasses:
   a. acquisition and collection;
   b. processing and analysis;
   c. storage;
   d. rectification and update;
   e. display, publication, transfer, dissemination, or disclosure; and/or
   f. erasure or destruction.

(2) Processing of Personal Data as referred to in paragraph (1) is performed in accordance with Personal Data protection principles, encompassing:
   a. collection of Personal Data is performed in limited and specific manners, legally valid, fair, with the knowledge and consent from Personal Data Owner;
   b. processing of Personal Data is performed in accordance with its purpose;
   c. processing of Personal Data is performed by guaranteeing the rights of Personal Data Owner;
   d. processing of Personal Data is performed accurately, comprehensively, not misleading, update, accountable, and paying attention to the purpose of Personal Data processing;

e. processing of Personal Data is performed by protecting the security of Personal Data from any loss, misuse, unlawful access and disclosure, as well as modification or impairment of Personal Data;
f. processing of Personal Data is performed by notifying the purpose of collection, processing activity, and failure on Personal Data protection; and
g. processing of Personal Data is terminated and/or erased, unless it is still within retention period as suited with the needs based on provisions under Laws and Regulations.

(3) Technical implementation of Personal Data processing as referred to in paragraph (1) in accordance with the provisions under Laws and Regulations.

Division Two
Legal Prerequisites for Personal Data Processing

Article 17

(1) Processing of Personal Data as referred to under Article 16 must meet the provision on the existence of legitimate consent from Personal Data Owner for one or several specific purposes which have been informed to the Personal Data Owner.
(2) Asides from the existence of consent as referred to in paragraph (1), processing of Personal Data must meet provisions which are required for the:
a. fulfillment of contractual obligation in the event that the Personal Data Owner is one of the party or to meet the request of Personal Data Owner when the agreement will be performed;
b. fulfillment of legal obligation of Personal Data Controller in accordance with provisions under the laws and regulations;
c. fulfillment of protection of vital interest of Any Person or Personal Data Owner;
d. implementation of authority of Personal Data Controller;
e. fulfillment of obligation of Personal Data Controller in regards to public service for public interest; and/or
f. fulfillment of other legitimate interest of Personal Data Controller and/or Personal Data Owner.

Division Three
Prerequisites for Consent

Article 18

(1) Consent for the processing of Personal Data is performed through written or audio recorded consent.
(2) Written consent as referred to in paragraph (1) may be submitted electronically or non-electronically.
(3) Written and audio recorded consent as referred to in paragraph (1) have the same legal effect.
(4) In case the written agreement as referred to in paragraph (1) contains other purposes, the request of consent must meet the following provisions:
    a. clearly distinguishable with other matters;
    b. be made using understandable and easy-access format; and
    c. using simple and clear language.
(5) Consent which fails to meet provisions as referred to in paragraph (1) and paragraph (4) should be declared non-binding toward Personal Data Owner.

Article 19

Every contract for the request of Personal Data which does not contain explicit consent from Personal Data Owner which fails to meet Personal Data protection principles should be declared null and void.

Division Four
Processing of Specific Personal Data

Article 20

(1) During the performance of Personal Data processing, Personal Data Controller must keep the confidentiality of specific Personal Data as referred to under Article 3 paragraph (1) letter b.

(2) Provision as referred to in paragraph (1) should be exempted in cases:
   a. Personal Data Owner has given consent as referred to under Article 18;
   b. it is needed for the purpose of performing obligation and/or certain rights of Personal Data Controller or Personal Data Owner within manpower, social security, taxation, and/or social-welfare sectors which grant protection toward fundamental rights and interests of the Personal Data Owner;
   c. it is needed to protect the interests of Personal Data Owner who are not capable, either physically or legally;
   d. it is performed within the legal act of association which is in accordance with the code of conduct, provided that the Personal Data is not disseminated outside the scope of association;
   e. Personal Data Owner has published its own specific Personal Data; and/or
   f. it is needed for legal proceeding purposes.

(3) Exemptions as referred to in paragraph (2) should be carried out in accordance with provisions under Laws and Regulations.

Division Five

Visual Data Processing or Operating Device

Article 21

(1) Visual data processing or operating device may be installed at public places and/or at public-service facilities for the following purposes:
   a. prevention, preliminary investigation, and investigation of criminal activities;
   b. security;
   c. disaster prevention; and/or
   d. organization of traffic or collection, analysis and arrangement of traffic Information.

(2) Operator of visual data processing or operating device must display Information that, within the area in question, visual data processing or operating device as referred to in paragraph (1) has been installed.
(3) Information as referred to in paragraph (2) should be exempted in the event of law enforcement in accordance with provisions under Laws and Regulations.
(4) Operator of visual data processing or operating device must guarantee the security of Information on Personal Data.
(5) Operator of visual data processing or operating device may use voice recording function on such visual data processing or operating device for purposes as referred to in paragraph (1) in accordance with provisions under Laws and Regulations.

CHAPTER V
OBLIGATIONS OF PERSONAL DATA CONTOLLER AND PERSONAL DATA PROCESSOR IN REGARDS TO THE PROCESSING OF PERSONAL DATA

Division One
General

Article 22

Personal Data Controller and Personal Data Processor encompass:
a. Any Person;
b. Public Body; and
c. organization/institution.

Division Two
Obligations of Personal Data Controller

Article 23

(1) Personal Data Controller when processing Personal Data must obtain consent from Personal Data Owner as referred to under Article 18.

(2) To obtain consent as referred to in paragraph (1), Personal Data Controller must submit Information on:
   a. legality of Personal Data processing;
   b. purpose of Personal Data processing;
   c. relevancy on the types of Personal Data which will be processed;
   d. retention period of documents containing Personal Data;
   e. details on collected Information;
   f. periods for the processing and destruction of Personal Data; and
   g. rights of Personal Data Owner.

(3) Personal Data Controller must show consent which has been granted by Personal Data Owner as referred to in paragraph (1).

(4) Consent as referred to in paragraph (1) should be exempted in case:
   a. it is needed to protect Personal Data Owner from threats against life safety;
   b. reach the purpose of fulfillment every rights and obligations in accordance with provisions under laws and regulations;
   c. legal proceedings in accordance with provisions under Laws and Regulations;
   d. implementation of duties and functions of various parties who have the authorities in accordance with provisions under Laws and Regulations;
   e. specific Personal Data have been in public domain because of acts as committed by Personal Data Owner;
   f. there is provision under Laws and Regulations which obliges the processing of Personal Data; and/or
   g. it is needed for the performance of agreement with Personal Data Owner.

(5) In case there is modification of Information on Personal Data processing as referred to in paragraph (2), Personal Data Controller must notify Personal Data Owner no later than 7 (seven) days since the modification of Information took place.

Article 24

(1) Personal Data Controller must terminate the processing of Personal Data in case Personal Data Owner withdraws the consent for the processing of Personal Data.

(2) Termination of Personal Data processing as referred to in paragraph (1) should be performed no later than 3 x 24 (three times twenty four) hours starting since the Personal Data Controller received request for the withdrawal of Personal Data processing.

Article 25

(1) Personal Data Controller must delay and restrict the processing of Personal Data, either partly or wholly, no later than 2 x 24 (two times twenty four) hours starting since the Personal Data Controller received request for the delay and restriction on processing of Personal Data.

(2) Delay and restriction of Personal Data processing as referred to in paragraph (1) should be exempted in cases:

a. there are laws and regulations which make the delay and restriction of Personal Data processing impossible;

b. it may endanger the safety of other parties; and/or

c. Personal Data Owner is bound with written agreement which makes the delay and restriction of Personal Data processing impossible.

Article 26

Personal Data Controller must protect and ensure the security of Personal Data which it processes by performing:

a. formulation and implementation of technical operational steps to protect Personal Data from interruption to Personal Data processing which is in contradiction with provisions under Laws and Regulations; and

b. determination of security level of Personal Data with regards given to the nature and risk of Personal Data which must be protected during the processing of Personal Data.

Article 27

Personal Data Controller must perform supervision against every parties who are involved in the processing of Personal Data under the control of Personal Data Controller.

Article 28

Personal Data Controller must ensure the protection of Personal Data from unlawful Personal Data processing.

Article 29

(1) Personal Data Controller must prevent Personal Data to be unlawfully accessed.
(2) Prevention as referred to in paragraph (1) is performed by using security system on Personal Data which is processed and/or processing of Personal Data using electronic system in reliable, secure, and responsible manners.
(3) Prevention as referred to in paragraph (2) should be performed in accordance with provisions under Laws and Regulations.

Article 30

Personal Data Controller must perform recordation of every Personal Data processing activities.

Article 31

Personal Data Controller must grant access to Personal Data Owner on Personal Data which is processed, along with track record on Personal Data processing, no later than 3 x 24 (three times twenty four) hours starting since the date when the access request was received in accordance with the storage period of Personal Data.

Article 32

Personal Data Controller must refuse to grant access for the modification of Personal Data to Personal Data Owner in case it is discovered or it should have been expected to:

a. threaten the security or physical health or mental health of Personal Data Owner and/or other person;
b. lead to the disclosure of Personal Data of other person; and/or
c. be in contradictory with national defence and security.

Article 33

(1) Personal Data Controller must update and/or rectify error and/or inaccuracy of Personal Data no later than 1 x 24 (one time twenty four) hours starting since the receipt request for update and/or rectification of Personal Data.
(2) Personal Data Controller must notify the result of update and/or rectification of Personal Data to Personal Data Owner.

Article 34

(1) Personal Data Controller must ensure the accuracy, completeness, and consistency of Personal Data in accordance with provisions under Laws and Regulations.
(2) In ensuring the accuracy, completeness, and consistency of Personal Data as referred to in paragraph (1), Personal Data Controller must perform verification.

Article 35

Personal Data Controller must perform Personal Data processing in accordance with the purpose of Personal Data processing as consented by Personal Data Owner.

Article 36

(1) Personal Data Controller must terminate Personal Data processing if:
    a. retention period has been reached;
    b. purpose of Personal Data processing has been achieved; or
    c. there is a request from Personal Data Owner.
(2) Termination of Personal Data processing as referred to in paragraph (1) should be performed in accordance with provisions under Laws and Regulation.

Article 37

(1) Personal Data Controller must erase Personal Data if:
    a. Personal Data is no longer required for the fulfillment of the purpose of Personal Data processing;
    b. Personal Data Owner has withdrawn consent for Personal Data processing;
    c. Personal Data is unlawfully obtained and/or processed; and/or

d. there is a request from Personal Data Owner.

(2) Erasure of Personal Data as referred to in paragraph (1) should be performed in accordance with provisions under Laws and Regulations.

(3) Personal Data which has been erased as referred to in paragraph (1) may be restored or redisplayed as a whole in case there is a written request from Personal Data Owner.

(4) Request as referred to in paragraph (3) may be filed in case the retention period has not elapsed in accordance with provisions under Laws and Regulations.

Article 38

(1) Personal Data Controller must destruct Personal Data if:

a. it no longer has use value;

b. the retention period has elapsed and shows information to be destructed based on archive retention period;

c. there is a request from Personal Data Owner; and/or

d. it does not correlated with the dispute settlement of legal proceedings.

(2) Destruction of Personal Data as referred to in paragraph (1) should be performed in accordance with provisions under Laws and Regulations.

Article 39

(1) In case there is a failure of Personal Data protection, Personal Data Controller must deliver written notification no later than 3 x 24 (three times twenty four) hours to:

a. Personal Data Owner; and

b. Minister or Sectoral Supervisory and Regulatory Institution in accordance with provisions under Laws and Regulations.

(2) In case the Sectoral Supervisory and Regulatory Institution receives notification as referred to in paragraph (1), Sectoral Supervisory and Regulatory Institution should coordinate with the Minister.

(3) Written notification as referred to in paragraph (1) on:

a. disclosed Personal Data;

b. when and how the Personal Data is disclosed; and

c. mitigation and restitution efforts toward the disclosure of Personal Data by Personal Data Controller.

(4) In certain events, Personal Data Controller must notify the public on failure of Personal Data protection as referred in paragraph (1).

Article 40

Personal Data Controller must be responsible for all processing of Personal Data.

Division Three

Obligations of Personal Data Processors

Article 41

(1) In case Personal Data Controller appoints Personal Data Processor, the Personal Data Processor must perform Personal Data processing based on instructions or orders from Personal Data Controller, unless it is deemed otherwise based on provisions under Laws and Regulations.

(2) Processing of Personal Data as referred to in paragraph (1), is performed with regards given to provisions on Personal Data processing based on this Law.

(3) Processing of Personal Data as referred to in paragraph (1) falls under the liability of Personal Data Controller.

(4) In case the Personal Data Processor performs Personal Data processing beyond the instructions or orders and purpose as determined by the Personal Data Controller, the Personal Data Processing becomes the liability of Personal Data Processor.

Article 42

Obligations as referred to under Article 20 paragraph (1), Article 26, Article 27, Article 28, Article 29, Article 30, and Article 34, also prevail for Personal Data Processor.

Division Four

Official or Officer Who Performs Personal Data Protection Functions

Article 43

(1) In certain events, Personal Data Controller and Personal Data Processor must appoint an official or officer who performs Personal Data protection functions.

(2) In certain events as referred to in paragraph (1) encompass:

a. processing of Personal Data for public service purposes;

b. core activities of Personal Data Controller have the nature, scope, and/or purpose which require regular and systematic monitoring over big-scale of Personal Data; and

c. core activities of Personal Data Controller encompass processing of big-scale of Personal Data for specific Personal Data and/or Personal Data which correlate with criminal activities.

(3) Official or officer who performs Personal Data protection functions as referred to in paragraph (1) must be appointed based on professional quality, legal knowledge and Personal Data protection practices, and ability to fulfill its duties.

(4) Official or officer who performs Personal Data protection functions as referred to in paragraph (3) may be originated from the internal and/or external of Personal Data Controller or Personal Data Processor.

Article 44

(1) Official or officer who performs Personal Data protection functions have the following duties at minimum:

a. informs and gives suggestions for Personal Data Controller or Personal Data Processor to comply with provisions under this Law;

b. monitors and ensures the compliance to this Law and policies of Personal Data Controller or Personal Data Processor, including assignment, responsibility, increase in awareness and training of parties involved in the processing of Personal Data, and relevant audits;

c. gives suggestions on Personal Data protection impact assessment and monitors the performance of Personal Data Controller and Personal Data Processor;

d. coordinates with Sectoral Supervisory and Regulatory Institution; and

e. acts as the contact person with Sectoral Supervisory and Regulatory Institution for issues in relation to the processing of Personal Data, including performing consultations on risk mitigation and/or other matters.

(2) When performing duties as referred to in paragraph (1), official or officer who performs Personal Data protection functions must notice the risks in relation to the operation of Personal Data processing, by taking the nature, scope, context and purpose of processing into considerations.

(3) Further provisions on official or officer who performs Personal Data protection functions should be addressed under Regulation of the Minister.

Division Five
Administrative Sanctions

Article 45

(1) Violations of provisions under Article 20 paragraph (1), Article 23 paragraph (1), paragraph (2), paragraph (3), and paragraph (5), Article 24 paragraph (1), Article 25 paragraph (1), Article 26, Article 27, Article 28, Article 29 (1), Article 30, Article 31, Article 32, Article 33, Article 34, Article 35, Article 36 paragraph (1), Article 37 paragraph (1), Article 38 paragraph (1), Article 39 paragraph (1) and paragraph (4), Article 40, Article 41 paragraph (1), Article 42, and Article 43 paragraph (1) shall be imposed with administrative sanctions.

(2) Administrative sanctions as referred to in paragraph (1) in the forms of:
   a. temporary suspension of Personal Data processing activities;
   b. erasure or destruction of Personal Data;
   c. redress; and/or
   d. administrative fines.

(3) The handing down of administrative sanctions as referred to in paragraph (2) shall be imposed by the executives of respective Sectoral Supervisory and Regulatory Institutions.

(4) Provisions on the procedures for the imposition of administrative sanctions as referred to in paragraph (3) should be carried out in accordance with provisions under Laws and Regulations.

CHAPTER VI
TRANSFER OF PERSONAL DATA

Division One
Transfer of Personal Data Within the Legal Territories of Unitary State of the Republic of Indonesia

Article 46

(1) Personal Data Controller may transfer Personal Data within the legal territories of Unitary State of the Republic of Indonesia.
(2) Transfer of Personal Data as referred to in paragraph (1) is performed after the Personal Data Controller has obtained written consent from Personal Data Owner.
(3) Personal Data Controller who transfers Personal Data and who receives transfer of Personal Data must perform Personal Data protections as referred to in this Law.

Article 47

(1) Personal Data Controller in the forms of incorporated entities who performs merger, split, acquisition, or consolidation of incorporated entities must submit notification on the handover of Personal Data to Personal Data Owner.
(2) Notification on the handover of personal data as referred to in paragraph (1) should be performed prior and subsequent to the merger, split, acquisition, or consolidation of incorporated entities.

Division Two
Transfer of Personal Data to Outside of Legal Territories of Unitary State of the Republic of Indonesia

Article 48

Personal Data Controller may transfer Personal Data to Personal Data Controller outside of legal territories of Unitary State of the Republic of Indonesia after obtaining written consent from Personal Data Owner.

Article 49

Transfer of Personal Data to outside of legal territories of Unitary State of the Republic of Indonesia as referred to under Article 49 may be performed with the following provisions:

a. jurisdiction or international organization which receives the transfer of Personal Data has level of Personal Data protection which is adequate with or higher than this Law;
b. there is contract between Personal Data Controller with party who receives the transfer at outside of legal territories of Unitary State of the Republic of Indonesia with regards given to Personal Data protection aspects; and/or
c. there is bilateral treaty.

CHAPTER VII
PROHIBITIONS IN THE UTILIZATION OF PERSONAL DATA

Article 50

Personal Data Controller and/or Personal Data Processor are prohibited from unlawfully disclosing specific Personal Data to other party.

Article 51

Any Person is prohibited from unlawfully installing and/or operating visual data processing or operating device at public places or public-service facilities which may threaten and/or breach Personal Data protection.

Article 52

(1) Any Person is prohibited from unlawfully replacing visual data processing or operating device which is installed at public places and/or public-service facilities which is used for the following purposes:

a. prevention, preliminary investigation, and investigation of criminal activities;
b. security;
c. disaster prevention; and/or
d. organization of traffic or collection, analysis and arrangement of traffic Information,

to other places.

(2) Any Person is prohibited from unlawfully using voice recording function on visual data processing or operating device that is installed at public places and/or public-service facilities other than for purposes as referred to in paragraph (1).

Article 53

Personal Data Controller is prohibited from transferring Personal Data to outside of legal territories of Unitary State of the Republic of Indonesia:

a. without consent of Personal Data Owner; or
b. fails to meet the following provisions:
   1. jurisdiction or international organization which receives the transfer of Personal Data has level of Personal Data protection which is adequate with or higher than this Law;
   2. there is contract between Personal Data Controller with party who receives the transfer at outside of legal territories of Unitary State of the Republic of Indonesia with regards given to Personal Data protection aspects; and/or
   3. there is bilateral treaty.

Article 54

Personal Data Controller and Personal Data Processor are prohibited from performing Personal Data processing for commercial and/or profiling purposes, unless based on consent of Personal Data Owner.

Article 55

Any Person is prohibited from unlawfully disclosing or utilizing Personal Data which is not under its ownership.

Article 56

(1) Any person is prohibited from forging Personal Data with the intention to enrich itself or other person or which may cause losses for other person.
(2) Any person is prohibited from selling or purchasing Personal Data.

CHAPTER VIII
FORMULATION OF CODE OF CONDUCT FOR PERSONAL DATA CONTROLLER

Article 57

(1) Association of businesses may formulate code of conduct for Personal Data Controller.
(2) Association of businesses, when formulating code of conduct for Personal Data Controller as referred to in paragraph (1), must take into considerations:
    a. purpose of Personal Data processing;
    b. Personal Data protection principles; and
    c. interests of Personal Data Owner or representative association.
(3) Code of conduct for Personal Data Controller as referred to in paragraph (1) must have level of protection that is adequate with or higher than this Law.
(4) Code of conduct for Personal Data Controller as referred to in paragraph (3) should not be in contradiction with this Law.

CHAPTER IX
EXEMPTIONS FROM PERSONAL DATA PROTECTION

Article 58

(1) Provisions on Personal Data protection under this Law are exempted in cases:
    a. for national defence and/or security purposes;
    b. for legal proceeding purposes;
    c. for state organization and public interest purposes;

d. for professional ethic code enforcement; or
e. for data aggregation which processing is designated for statistic and scientific research purposes.

(2) Exemptions as referred to in paragraph (1) should be implemented only in the events of implementation of provisions of Law and/or ratified treaties.

CHAPTER X
DISPUTE SETTLEMENT

Article 59

(1) Dispute settlement for Personal Data Protection may be performed:
a. out-of-court; or
b. in court.

(2) Dispute settlement as referred to in paragraph (1) should be performed in accordance with provisions under laws and regulations.

CHAPTER XI
INTERNATIONAL COOPERATION

Article 60

(1) International cooperation is performed by the Government with government of other jurisdictions or international organizations in relation to Personal Data protection.

(2) International cooperation in the events of implementation of this Law is performed in accordance with provisions under laws and regulations and international law principles.

CHAPTER XII
PUBLIC PARTICIPATION

Article 61

(1) For the sake of public interest and/or national interest, State Attorney acting as state counsel has the authority to act for and on behalf of the state or government for breach of Personal Data protection, both committed domestically and overseas.
(2) Enforcement of authority as referred to in paragraph (1) should be implemented both in court or out-of-court.

Article 62

(1) Public may actively participate, either directly or indirectly, in supporting the organization of Personal Data protection in accordance with provisions under this Law.
(2) Implementation of public participation as referred to in paragraph (1) may be carried out through education, training, advocacy, technical counsel, and/or socialization.

CHAPTER XIII
CRIMINAL PROVISIONS

Article 63

Personal Data Controller and/or Personal Data Processor, who deliberately and unlawfully disclose specific Personal Data to other party as referred to under Article 50, shall be sentenced with criminal fines in sum of IDR 5,000,000,000.00 (five billion rupiahs) at maximum.

Article 64

Any person who deliberately and unlawfully installs and/or operate visual data processing or operating device at public places or public-service facilities which may threaten or breach Personal Data protection as referred to under Article 51, shall be sentenced with criminal fines in sum of IDR 500,000,000.00 (five hundred million rupiahs) at maximum.

Article 65

(1) Any person who deliberately and unlawfully moves visual data processing or operating device that is installed at public places or public-service facilities which is

used for the purposes of prevention, preliminary investigation, and investigation of criminal activities, security, disaster prevention, and/or organization of traffic or collection, analysis and arrangement of traffic Information to other places as referred to under Article 52 paragraph (1) shall be sentenced with criminal fines in sum of IDR 500,000,000.00 (five hundred million rupiahs) at maximum.

(2) Any person who deliberately and unlawfully uses voice recording function on visual data processing or operating device that is installed at public places or public-service facilities, unless for the purposes of prevention, preliminary investigation, and investigation of criminal activities, security, disaster prevention, and/or organization of traffic or collection, analysis and arrangement of traffic Information as referred to under Article 52 paragraph (2) shall be sentenced with criminal fines in sum of IDR 500,000,000.00 (five hundred million rupiahs) at maximum.

Article 66

Personal data controller who deliberately transfers Personal Data to outside of legal territories of Unitary State of the Republic Indonesia:

a. without written consent from Personal Data Owner; or
b. fails to meet the following provisions:
    1. jurisdiction or international organization which receives the transfer of Personal Data has level of Personal Data protection which is adequate with or higher than this Law;
    2. there is contract between Personal Data Controller with party who receives the transfer at outside of legal territories of Unitary State of the Republic of Indonesia with regards given to Personal Data protection aspects; and/or
    3. there is bilateral treaty,

as referred to under Article 53 shall be sentenced with criminal fines in sum of IDR 50,000,000,000.00 (fifty billion rupiahs) at maximum.

Article 67

Personal Data Controller and Personal Data Processor who deliberately perform Personal Data processing for commercial and/or profiling purposes without consent from

Personal Data Owner as referred to under Article 54 shall be sentenced with criminal fines in sum of IDR 100,000,000,000.- (one hundred billion rupiahs) at maximum.

Article 68

Any person who deliberately and unlawfully discloses or utilizes Personal Data which is not under its ownership as referred to under Article 55 shall be sentenced with criminal fines in sum of IDR 10,000,000,000.00 (ten billion rupiahs) at maximum.

Article 69

(1) Any person who deliberately forges personal data with the intention of enriching itself or other person or which may cause losses for other person as referred to under Article 56 paragraph (1) shall be sentenced with criminal fines in sum of IDR 3,000,000,000.00 (three billion rupiahs) at maximum.
(2) Any person who deliberately sells or purchases personal data which is not under its ownership as referred to under Article 56 paragraph (2) shall be sentenced with criminal fines in sum of IDR 5,000,000,000.00 (five billion rupiahs) at maximum.

Article 70

Asides from being sentenced with criminal sanctions as referred to under Article 63 up to Article 69, the defendant may also be imposed with additional criminal sanctions in the form of seizure of profits and/or assets which are obtained or resulted from criminal activities.

Article 71

(1) In case the criminal activities as referred to under Article 63 up to Article 69 are committed by Corporation, the criminal sanctions may be imposed to its management, controlling personnel, and/or Corporation.
(2) Criminal fines which are imposed to Corporation should not be greater than 3 (three) times of the maximum criminal fines as initially addressed.

(3) Asides from being sentenced with primary criminal sanctions as referred to in paragraph (2), Corporation may be sentenced with additional criminal sanctions in the forms of:

a. seizure of profits and/or assets derived from criminal activities;
b. suspension of whole or part of business of Corporation;
c. permanent prohibition from performing certain activities;
d. shut down of the whole or part of place of business and/or activities of Corporation;
e. performance of obligation which has been neglected; or
f. payment of redress.

CHAPTER XIV
TRANSITIONAL PROVISIONS

Article 72

When this Law comes into effect, parties who have performed Personal Data processing, must make adjustments with provisions on Personal Data protection based on this Law no later than 2 (two) years since this Law has been promulgated.

CHAPTER XV
CLOSING PROVISIONS

Article 73

When this Law comes into effect, all provisions under Laws and Regulations which address Personal Data protection are still declared in effect, insofar that they are not in contradictory with provisions under this Law.

Article 74

This Law comes into effect on the promulgation date.

For the purposes of public cognizance, it has been ordered that the promulgation of this Law should be achieved through its publication in the State Gazette of the Republic of Indonesia.

Enacted in Jakarta
on ...

PRESIDENT OF THE REPUBLIC OF INDONESIA,

JOKO WIDODO

Promulgated in Jakarta
on ...

MINISTER OF LAW AND HUMAN RIGHTS
OF THE REPUBLIC OF INDONESIA,

YASONNA H LAOLY

STATE GAZETTE OF THE REPUBLIC OF INDONESIA OF ... NUMBER ...

DRAFT ELUCIDATION OF
LAW OF THE REPUBLIC OF INDONESIA
NUMBER ... OF ...
ON
PERSONAL DATA PROTECTION

I. GENERAL

Development of information technology and communication which rapidly moves forward has created various opportunities and challenges. Information technology enables human to be interconnected without being limited with state territorial borders, so that it becomes one of the push factors for globalization. Various sectors in life have utilized information-technology system, such as the organization of electronic commerce (e-commerce) within trading/business sector, electronic education (e-education) within education sector, electronic health (e-health) within health sector, electronic government (e-government) within governmental sector, as well as information technology which has been utilized within other sectors. Utilization of such information technology causes personal data of a person to be easily collected and moved from one party to another without being noticed by personal data owner, thus threatening the privacy right of a person.

Protection of Personal Data is classified within the protection of human rights, hence, framework concerning privacy right over personal data is the manifestation of recognition and protection of fundamental human rights. Existence of a Law on Protection of Personal Data is a must and cannot be postponed anymore because it is very urgent for various national interests. Indonesian international communities take part in demanding the existence of protection of Personal Data. Such protection may improve trading, industry, investment which are transnational in nature.

Draft Bill on Personal Data Protection is a mandate from Article 28G paragraph (1) of 1945 Constitution of the Republic of Indonesia which states that: “any person has the right for protection of itself, family, honor, dignity, and assets which are belong under its possession, and right of security and protection sense from fear of threats to perform or not to perform an act which is human right”. Matters on protection of

personal data arise because of concerns on breach of privacy which may be experienced by person and or incorporated entity. Such breach of privacy may cause losses which, not only materially in nature, but also morally, namely the ruining of reputation of a person or agency.

Formulation on rules on privacy of Personal Data is comprehensible because there are needs to protect individual rights within the public in connection with the processing and Personal Data Processing, either performed electronically or manually using data-processing device. Adequate protection of privacy in relation to personal data will be able to grant trust for the public to provide Personal Data for greater various interests of the public without being misused or violating its individual rights. Therefore, this framework will create a balance between individual and public rights whose interests are represented by the state. This framework on privacy of Personal Data will give huge contribution for the inception of order and advancement in information society.

In order to reduce overlapping provisions on Personal Data Protection, thus, essentially provisions under this Law are general standards of data protection, either processed partly or wholly using electronic and manual means, whereas each sectors may implement Personal Data Protection in accordance with the characteristics of the relevant sectors, including provisions on Personal Data which have been addressed under provisions on profession.

The basis for the formulation of norms and implementation within Personal Data Protection is based on protection principle, legal certainty principle, public interest principle, beneficial principle, precautionary principle, balance principle, and accountability principle. Protection principle is aimed to give protection for Personal Data Owner on its Personal Data and rights of such Personal Data, so that it is not misused. Legal certainty principle is aimed as the legal basis for Personal Data Protection, as well as everything which supports its organization that obtains legal recognition both inside and outside of the court. Public interest principle means that when enforcing Personal Data Protection, one must regard the interests of the public or society in helicopter view. Such public interests include interests of state organization and national defence and security. Beneficial principle means that

personal data protection framework must be beneficial for national interests, specifically in achieving public-welfare idea. Precautionary principle is aimed so that parties relating to the processing and supervision of personal data must notice entire aspects which potentially trigger losses. Balance principle is personal data protection efforts to balance between rights of personal data on one hand with rights of the state which are legal based on public interests. Meanwhile, accountability principle is aimed so that every parties relating to the processing and supervision of personal data to act accountably, hence they are able to ensure the balance between rights and obligations of related parties, including data subject.

Personal Data protection framework aims to, among others, protect and ensure fundamental citizen rights in relation to personal data protection, ensure the public to obtain services from the government, corporation, business, and other organization/institution, push the development of digital economy and information-technology and communication industry, and support the improvement of domestic industrial competitiveness.

II. ARTICLE BY ARTICLE

Article 1

Self-explanatory.

Article 2

Self-explanatory.

Article 3

Paragraph (1)

Personal Data as referred to in this Law encompasses, among others, individual data as addressed under Law on Residency Administration.

Paragraph (2)

General Personal Data refers to, among others, complete name, gender, nationality, and religion, or Personal Data which must be combined to make the identification of a person possible.

Paragraph (3)

Specific personal data encompasses:

a. medical data and information, namely records or information of individuals relating to:
    1) physical health;
    2) mental health; and/or
    3) medical treatment;
b. biometric data, namely data in relation to physical, physiological, or behavioral characteristic of individuals which makes unique identification on individuals possible, such as image of the face or dactyloscopy[2] data. Biometric data also explains unique nature and/or characteristic of a person which must be secured and preserved, including but not limited to:
    1) fingerprint record;
    2) eye retina; and
    3) DNA sample.
c. genetic data, namely every data, any types concerning characteristics of an individual which are inherited or obtained during the early prenatal development;
d. sexual life/orientation;
e. political opinion;
f. criminal record;
g. data on child;
h. personal financial data, including but not limited to data on amount of saving at the bank, including:
    1) saving;
    2) time deposit; and
    3) data on credit card.

[2] Translator's note: dactyloscopy refers to identification by comparison of fingerprints (Merriam-Webster).

i. other data in accordance with provisions under laws and regulations which are combined, so that it is possible to identify a person specifically.

Article 4

Self-explanatory.

Article 5

Self-explanatory.

Article 6

Self-explanatory.

Article 7

Self-explanatory.

Article 8

Self-explanatory.

Article 9

Self-explanatory.

Article 10

"Profiling" refers to any types of automatic Personal Data processing which uses Personal Data to evaluate aspects on work history, economic condition, health, personal preference, interest, reliability, behavior, location or movement of Personal Data Owner electronically.

Article 11

"Pseudonym mechanism" refers to Personal Data processing, in such a way, so that Personal Data can no longer be linked to certain Personal Data Owner without

using additional Information which is given to ensure that Personal Data can no longer be linked to Personal Data Owner who is identified or identifiable.

Article 12

Self-explanatory.

Article 13

Self-explanatory.

Article 14

Self-explanatory.

Article 15

"Written request" refers to recorded application which is submitted, either electronically or non-electronically.

Article 16

Paragraph (1)

Letter a

Self-explanatory.

Letter b

Self-explanatory.

Letter c

Self-explanatory.

Letter d

Self-explanatory.

Letter e

"Transfer" refers to movement, delivery, and/or multiplication of Personal Data, either manually or electronically, from Personal Data Owner to other party.

Letter f

Self-explanatory.

Paragraph (2)

Self-explanatory.

Paragraph (3)

"Provisions under laws and regulations" refer to sectoral Laws and Regulations in accordance with the purpose of personal data processing.

Article 17

Paragraph (1)

"Legitimate consent" refers to consent that is explicitly submitted, cannot be hidden or based on mistake/negligence.

Paragraph (2)

Letter a

Self-explanatory.

Letter b

Self-explanatory.

Letter c

"Vital interest" refers to needs/necessity to protect a very important matter on the existence of a person.

Letter d

Self-explanatory.

Letter e

Self-explanatory.

Article 18

Self-explanatory.

Article 19

Self-explanatory.

Article 20

Paragraph (1)

Self-explanatory.

Paragraph (2)

Letter a

Self-explanatory.

Letter b

Self-explanatory.

Letter c

Self-explanatory.

Letter d

Self-explanatory.

Letter e

"Published" refers to actively distribute Personal Data and/or make it available to be accessed by the public.

Letter f

Self-explanatory.

Paragraph (3)

Self-explanatory.

Article 21

Paragraph (1)

"Visual data processing or operating device" refers to video camera tool that is used to record or observe natural person at a space or certain place, including Closed Circuit Television (CCTV) and/or all surveillance and monitoring devices which are continuously develop in accordance with technology development, which accountability and accuracy are maintained.

Paragraph (2)

"Operator" refers to Personal Data Processor who has the duty to secure, serve, and operate visual data processing or operating device.

Paragraph (3)

Self-explanatory.

Paragraph (4)

"Security of Information on Personal Data" encompasses confidentiality, integrity, availability, authenticity, and non-repudiation.

Paragraph (5)

Self-explanatory.

Article 22

Letter a

Self-explanatory.

Letter b

Self-explanatory.

Letter c

"Organization/institution" refers to, among others, social organization.

Article 23

Paragraph (1)

Self-explanatory.

Paragraph (2)

Letter a

Self-explanatory.

Letter b

Self-explanatory.

Letter c

Self-explanatory.

Letter d

Self-explanatory.

Letter e

Self-explanatory.

Letter f

Time period for Personal Data processing prevails so long that there is a legitimate legal interest.

Letter g

Self-explanatory.

Paragraph (3)

Obligation to show consent which has been given by Personal Data Owner is performed for the fulfillment of legal requirement for Personal Data processing.

Paragraph (4)

Letter a

"Life safety" refers to the rescue of Personal Data Owner from criminal threats which are identified by law enforcers which will target Personal Data Owner in question.

Letter b

Self-explanatory.

Letter c

Self-explanatory.

Letter d

Self-explanatory.

Letter e

Self-explanatory.

Letter f

Self-explanatory.

Letter g

Self-explanatory.

Letter h

Self-explanatory.

Paragraph (5)

Self-explanatory.

Article 24

Paragraph (1)

Self-explanatory.

Paragraph (2)

Withdrawal of consent for processing of Personal Data contains, among others, reasons of withdrawal and be enclosed with evidence.

Article 25

Paragraph (1)

Request on the delay and restriction on Personal Data processing which is filed by Personal Data Owner contains, among others, reasons of delay and restriction of Personal Data processing and be enclosed with evidence.

Paragraph (2)

Self-explanatory.

Article 26

Self-explanatory.

Article 27

Self-explanatory.

Article 28

Self-explanatory.

Article 29

Self-explanatory.

Article 30

Self-explanatory.

Article 31

Self-explanatory.

Article 32

Letter a

"Threaten the security or physical health or mental health of Personal Data Owner and/or other person" refers to, among others, modification of history of illness which potentially threatens the security of oneself and/or other person.

Letter b

"Lead to disclosure of Personal Data of other person" refers to, among others, modification of Personal Data of customer which leads to the disclosure of Personal Data of another person.

Letter c

Self-explanatory.

Article 33

Self-explanatory.

Article 34

Self-explanatory.

Article 35

Self-explanatory.

Article 36

Self-explanatory.

Article 37

Self-explanatory.

Article 38

Paragraph (1)

"Destruct Personal Data" refers to the destruction of Personal Data, so that it can no longer be identified as Personal Data of a person.

Paragraph (2)

Self-explanatory.

Article 39

Paragraph (1)

Self-explanatory.

Paragraph (2)

Self-explanatory.

Paragraph (3)

Self-explanatory.

Paragraph (4)

"In certain events" refers to, among others, if the failure of Personal Data protection interferes public services and/or has serious impact on interests of the public.

Article 40

Self-explanatory.

Article 41

Paragraph (1)

Self-explanatory.

Paragraph (2)

Self-explanatory.

Paragraph (3)

Self-explanatory.

Paragraph (4)

When Personal Data Processor acts beyond the instructions or orders and purposes as determined by Personal Data Controller, then at that time, Personal Data Processor has transformed into Personal Data Controller for other purposes, hence it becomes the liability of the party in question.

Article 42

Self-explanatory.

Article 43

Paragraph (1)

"Official or officer who performs Personal Data protection functions" refers to official or officer who is responsible to ensure the fulfillment of compliance to Personal Data principles and risk mitigation on violation of Personal Data protection.

Paragraph (2)

Self-explanatory.

Paragraph (3)

Self-explanatory.

Paragraph (4)

Self-explanatory.

Article 44

Self-explanatory.

Article 45

Self-explanatory.

Article 46

Paragraph (1)

Self-explanatory.

Paragraph (2)

Written consent to perform transfer of Personal Data is expressed in the form that is separate from terms and conditions form for the utilization of Personal Data.

Paragraph (3)

Self-explanatory.

Article 47

Self-explanatory.

Article 48

Written consent may be submitted in electronic or non-electronic forms.

Article 49

Letter a

Self-explanatory.

Letter b

Self-explanatory.

Letter c

Development of framework on transfer of Personal Data in other jurisdictions has required every jurisdiction to have protection that is equivalent with its national provisions and adopt approach that is implemented in many jurisdictions, but in its implementation, it cannot yet be strictly applied, therefore Bilateral treaty is still required.

Article 50

Self-explanatory.

Article 51

Self-explanatory.

Article 52

Paragraph (1)

"To other places" encompasses changing direction and/or range of visualization of visual data processing or operating device.

Paragraph (2)

Self-explanatory.

Article 53

Self-explanatory.

Article 54

“Commercial purposes” refers to processing of Personal Data in order to generate profits.

Article 55

Self-explanatory.

Article 56

Self-explanatory.

Article 57

Self-explanatory.

Article 58

Paragraph (1)

Self-explanatory.

Letter a

“National defence and/or security purposes” encompasses state intelligence.

Letter b

Self-explanatory.

Letter c

“State organization and public interest purposes” encompasses the organization of residency administration, social security, monetary, payment system, financial-system stability, and taxation.

Letter d

Self-explanatory.

Letter e

Data Aggregation refers to a collection of data which is linked to the personality of a person that cannot and/or not designated to identify a person, both directly and indirectly.

Paragraph (2)

Self-explanatory.

Article 59

Self-explanatory.

Article 60

Self-explanatory.

Article 61

Self-explanatory.

Article 62

Self-explanatory.

Article 63

Self-explanatory.

Article 64

Self-explanatory.

Article 65

Self-explanatory.

Article 66

Self-explanatory.

Article 67

Self-explanatory.

Article 68

Self-explanatory.

Article 69

Self-explanatory.

Article 70

Self-explanatory.

Article 71

Self-explanatory.

Article 72

Self-explanatory.

Article 73

Self-explanatory.

Article 74

Self-explanatory.

SUPPLEMENT TO THE STATE GAZETTE OF THE REPUBLIC OF INDONESIA ...