REGULATION OF THE MINISTER OF COMMUNICATION AND INFORMATICS OF THE REPUBLIC OF INDONESIA

NUMBER 20 OF 2016

ON

PERSONAL DATA PROTECTION WITHIN ELECTRONIC SYSTEM[1]

BY THE GRACE OF GOD ALMIGHTY

MINISTER OF COMMUNICATION AND INFORMATICS OF THE REPUBLIC OF INDONESIA,

Considering:

that in order to implement provisions under Article 15 paragraph (3) of Regulation of the Government Number 82 of 2012 on Organization of Electronic System and Transactions, it is deemed necessary to establish Regulation of the Minister of Communication and Informatics on Personal Data Protection within Electronic System;

In view of:

1. Law Number 11 of 2008 on Electronic Information and Transactions (State Gazette of the Republic of Indonesia of 2008 Number 58, Supplement to the State Gazette of the Republic of Indonesia Number 4843);
2. Law Number 39 of 2008 on State Ministry (State Gazette of the Republic of Indonesia of 2008 Number 166, Supplement to the State Gazette of the Republic of Indonesia Number 4916);
3. Regulation of the Government Number 82 of 2012 on Organization of Electronic System and Transactions (State Gazette of the Republic of Indonesia of 2012

Number 189, Supplement to the State Gazette of the Republic of Indonesia Number 5348);

4. Regulation of the President Number 7 of 2015 on Organization of State Ministry (State Gazette of the Republic of Indonesia of 2015 Number 8);
5. Regulation of the President Number 54 of 2015 on Ministry of Communication and Informatics (State Gazette of the Republic of Indonesia of 2015 Number 96);
6. Regulation of the Minister of Communication and Informatics Number 1 of 2016 on Organization and Working Procedures of Ministry of Communication and Informatics (Official Gazette of the Republic of Indonesia of 2016 Number 103);

HAS DECIDED:

To establish:

REGULATION OF THE MINISTER OF COMMUNICATION AND INFORMATICS ON PERSONAL DATA PROTECTION WITHIN ELECTRONIC SYSTEM.

CHAPTER 1

GENERAL PROVISIONS

Article 1

Under this Regulation of the Minister, the following definitions are employed:

1. Personal Data are certain individual data which are stored, preserved, and its veracity is maintained, as well as its confidentiality is protected.
2. Certain Individual Data are any accurate and actual statement which is attributed and identifiable, either directly or indirectly, to each individual, of which, its utilization is in accordance with provisions under laws and regulations.
3. Data Subject is individual who is attributed with Certain Individual Data.
4. Consent of Data Subject, hereinafter referred to as Consent, is written statement, either manually and/or electronically, which is given by Data Subject after receiving complete explanation on the measures of acquisition, collection, processing, analysis,

storage, display, publication, transfer, and dissemination, as well as confidentiality or non-confidentiality of Personal Data.

5. Electronic System is a set of electronic devices and procedures which has function to prepare, collect, process, analyze, store, display, publish, transfer, and/or disseminate electronic information.
6. Electronic System Provider is any Person, state organizer, Enterprise, and community which provide, manage, and/or operate Electronic System independently or jointly toward Electronic System User for its own needs and/or needs of others.
7. Electronic System User, hereinafter referred to as User, is any Person, state organizer, Enterprise, and community which utilize goods, services, facilities, or information as provided by Electronic System Provider.
8. Enterprise is individual company or partnership company, either taking form as incorporated entity or unincorporated entity.
9. Minister is minister who organizes governmental affairs within the sectors of communication and informatics.
10. Director General is director general whose duties and functions are within the sector of informatics application.

Article 2

(1) Personal Data Protection within Electronic System encompasses protection against acquisition, collection, processing, analysis, storage, display, publication, transfer, dissemination, and destruction of Personal Data.

(2) In the course of enforcement of provisions as referred to in paragraph (1), it should be based on good Personal Data protection principles, encompassing:
   a. respect toward Personal Data as privacy;
   b. Personal Data is confidential in nature in accordance with Consent and/or based on provisions under laws and regulations;
   c. based on Consent;
   d. relevancy with the purpose of acquisition, collection, processing, analysis, storage, display, publication, transfer, and dissemination;
   e. feasibility of Electronic System which is used;

f. good faith in terms of expeditiously notify in writing to Data Subject on any failure of Personal Data protection;
g. availability of internal rules for management of Personal Data protection;
h. liability over Personal Data which are within the possession of User;
i. ease of access and correction of Personal Data by Data Subject; and
j. integrity, accuracy, and validity, as well as update of Personal Data.

(3) Privacy as referred to in paragraph (2) letter a is the freedom of Data Subject to declare confidential or not declare confidential of its Personal Data, unless deemed otherwise in accordance with provisions under laws and regulations.

(4) Consent as referred to in paragraph (2) letter b is given after Data Subject declares confirmation of accuracy, confidentiality status and purpose of management of Personal Data.

(5) Validity as referred to in paragraph (2) letter j is legality in the course of acquisition, collection, processing, analysis, storage, display, publication, transfer, dissemination, and destruction of Personal Data.

CHAPTER II

PROTECTION

First Division

General

Article 3

Personal Data Protection within Electronic System is performed toward the processes of:

a. acquisition and collection;
b. processing and analysis;
c. storage;
d. display, publication, transfer, dissemination, and/or open of access; and
e. destruction.

Article 4

(1) Electronic System which is used for processes as referred to under Article 3 must be certified.

(2) Performance of certification as referred to in paragraph (1) is in accordance with provisions under laws and regulations.

Article 5

(1) Any Electronic System Provider should have internal rules on Personal Data protection in order to carry out processes as referred to under Article 3.

(2) Any Electronic System Provider should formulate internal rules on Personal Data protection as a form of preventive measures in order to avoid the occurrence of failure of protection of Personal Data under its management.

(3) Formulation of internal rules as referred to in paragraph (1) and paragraph (2) should take regards the aspects of technology implementation, human resources, method, and fees, as well as referring to provisions under this Regulation of the Minister and other relevant laws and regulations.

(4) Other preventive measures in order to avoid the occurrence of failure of protection of Personal Data under its management should be performed by any Electronic System Provider, at least taking forms as the following activities:

a. increase awareness of human resources within its environment in order to provide Personal Data protection within Electronic System under its management; and

b. hold training on prevention of failure of Personal Data protection within Electronic System under its management for human resources within its environment.

Article 6

Electronic System Provider which performs processes as referred to under Article 3 must provide consent form in Indonesian Language in order to ask Consent from Data Subject in question.

Second Division

Acquisition and Collection of Personal Data

Article 7

(1) Acquisition and collection of Personal Data by Electronic System Provider should be restricted to information that is relevant and in accordance with its purpose, as well as must be performed accurately.

(2) Supervising Institution and Sectoral Supervisor may determine information that is relevant and in accordance with its purpose as referred to in paragraph (1).

Article 8

(1) In the course of acquiring and collecting Personal Data, Electronic System Provider should respect Data Subject for its Personal Data which are private in nature.

(2) Respect toward Data Subject for Personal Data which are private in nature as referred to in paragraph (1) is performed through the provision of option in Electronic System for Data Subject on:

a. confidentiality or non-confidentiality of Personal Data; and

b. modification, addition, or update of Personal Data.

(3) Option for Data Subject on confidentiality or non-confidentiality of Personal Data as referred to in paragraph (2) letter a does not apply if laws and regulations have explicitly addressed that Personal Data which are, specifically against several of its elements, declared to be confidential in nature.

(4) Option for Data Subject on modification, addition, or update of Personal Data as referred to in paragraph (2) letter b is in order to give opportunity for Data Subject if it wishes alteration of its Certain Individual Data.

Article 9

(1) Acquisition and collection of Personal Data by Electronic System Provider must be based on Consent or based on provisions under laws and regulations.

(2) Data Subject who gives Consent as referred to in paragraph (1) may declare its Certain Individual Data to be confidential in nature.

(3) In case Consent as referred to in paragraph (2) does not include Consent for disclosure of confidentiality of Personal Data, thus:

a. any Person who performs acquisition and collection of Personal Data; and

b. Electronic System Provider;

should maintain confidentiality of such Personal Data.

(4) Provisions to maintain confidentiality of Personal Data for any Person and Electronic System Provider as referred to in paragraph (3) also prevail for Personal Data which are declared confidential in accordance with provisions under laws and regulations.

Article 10

(1) Personal Data which are acquired and collected directly should be verified with Data Subject.

(2) Personal Data which are acquired and collected indirectly should be verified based on processing result from various data sources.

(3) Data sources in the course of acquisition and collection of Personal Data as referred to in paragraph (2) should have valid legal ground.

Article 11

(1) Electronic System which is used to accommodate acquisition and collection of Personal Data should:

a. have the interoperability and compatibility features; and

b. use legal software (*perangkat lunak*).

(2) Interoperability and compatibility features as referred to in paragraph (1) letter a are in accordance with provisions under laws and regulations.

(3) Interoperability as referred to in paragraph (2) is the feature of different Electronic Systems to operate in integration.

(4) Compatibility as referred to in paragraph (2) is the conformity of the Electronic System with another Electronic System.

Third Division
Processing and Analysis of Personal Data

Article 12

(1) Personal Data may only be processed and analyzed in accordance with the needs of Electronic System Provider which have been clearly declared when acquiring and collecting them.

(2) Processing and analysis of Personal Data as referred to in paragraph (1) are performed based on Consent.

Article 13

Provisions as referred to under Article 12 paragraph (2) do not apply if such Personal Data which are processed and analyzed are originated from Personal Data which have been displayed or published openly by Electronic System for public services.

Article 14

Personal Data which are processed and analyzed should be Personal Data which have been verified on its accuracy.

Fourth Division
Storage of Personal Data

Article 15

(1) Personal Data which are stored within Electronic System should be Personal Data which have been verified on its accuracy.

(2) Personal Data which are stored within Electronic System should be in the forms of encrypted data.

(3) Personal Data as referred to in paragraph (1) must be stored within Electronic System:

a. in accordance with provisions under laws and regulations addressing obligation for time period for storage of Personal Data within respective Supervising Institution and Sectoral Regulator; or
b. for 5 (five) years at minimum, if provisions under laws and regulations which specifically address such matter are yet to be available.

Article 16

If Data Subject no longer acts as User, Electronic System Provider must store such Personal Data in accordance with timeframe as referred to under Article 15 paragraph (2) since the last date when Data Subject acts as User.

Article 17

(1) Data center (*pusat data*) and disaster recovery center (*pusat pemulihan bencana*) of Electronic System Provider for public services as used for Personal Data protection process as referred to under Article 3 must be placed within the territories of the Republic of Indonesia.
(2) Data center (*pusat data*) as referred to in paragraph (1) is a facility that is used to place Electronic System and its related components for the purposes of placement, storage, and processing of data.
(3) Disaster recovery center (*pusat pemulihan bencana*) as referred to in paragraph (1) is a facility that is used to restore data or information, as well as important functions of Electronic System which are interrupted or damaged due to disaster as caused by the nature and/or human.
(4) Further provisions on obligation for the placement of data center and disaster recovery center in Indonesian territories as referred to in paragraph (1) are addressed by relevant Supervising Institution and Sectoral Regulator in accordance with provisions under laws and regulations after coordinating with Minister.

Article 18

(1) Storage of Personal Data within Electronic System should be performed in accordance with provisions on security procedures and means of Electronic System.

(2) Security procedures and means of Electronic System as referred to in paragraph (1) are in accordance with provisions under laws and regulations.

Article 19

If the storage period for Personal Data has exceeded timeframe as referred to under Article 15 paragraph (2), Personal Data within Electronic System may be erased, unless such Personal Data will still be used or utilized in accordance with initial purpose of its acquisition and collection.

Article 20

If Data Subject requests erasure of its own Certain Individual Data, such erasure request is performed in accordance with provisions under laws and regulations.

Fifth Division

Display, Publication, Transfer, Dissemination, and/or Open of Access to Personal Data

Article 21

(1) Display of, publish of, transfer of, disseminate of, and/or open access to Personal Data within Electronic System may only be performed:

a. based on Consent, unless deemed otherwise by provisions under laws and regulations; and

b. after its accuracy and conformity with the purpose of acquisition and collection of such Personal Data have been verified.

(2) Display of, publish of, transfer of, disseminate of, and/or open access to Personal Data within Electronic System as referred to in paragraph (1) include those which are performed among Electronic System Providers, between Electronic System Provider with User, or among Users.

Article 22

(1) Transfer of Personal Data under the management of Electronic System Provider at governmental institution and regional government, as well as community or private party which is domiciled within the territories of the state of the Republic of Indonesia to outside territories of the state of the Republic of Indonesia should:
   a. coordinate with Minister or official/agency which is given the authority to do so; and
   b. enforce provisions under laws and regulations on cross-border exchange of Personal Data.

(2) Performance of coordination as referred to in paragraph (1) letter a takes form as:
   a. report plan for the performance of transfer of Personal Data, at least consists of full name of designated country, full name of receiving subject, performance date, and reasons/purposes of transfer;
   b. request advocacy, if necessary; and
   c. report the result of performance of activity.

Article 23

(1) For the purpose of law enforcement process, Electronic System Provider must handover Personal Data which exist within Electronic System or Personal Data which are produced by Electronic System upon formal request from law enforcers based on provisions under laws and regulations.

(2) Personal Data as referred to in paragraph (1) are Personal Data which are relevant and in accordance with law enforcement purposes.

Article 24

(1) Use and utilization of Personal Data which are displayed, published, received, and disseminated by Electronic System Provider should be based on Consent.

(2) Use and utilization of Personal Data as referred to in paragraph (1) should be in accordance with the purposes of acquisition, collection, processing, and/or analysis of Personal Data.

Sixth Division
Destruction of Personal Data

Article 25

(1) Destruction of Personal Data within Electronic System may only be performed if:
   a. they have passed the provisions on time period for storage of Personal Data within Electronic System based on this Regulation of the Minister or in accordance with provisions under other laws and regulations which specifically regulate within respective Supervising Institution and Sectoral Regulator for that matter; or
   b. based on request of Data Subject, unless deemed otherwise by provisions under laws and regulations.

(2) Destruction as referred to in paragraph (1) should eliminate a part or entirety of documents relating to Personal Data, including the electronic or non-electronic ones, as managed by Electronic System Provider and/or User, so that such personal Data cannot be redisplayed within Electronic System, unless Data Subject gives its new Personal Data.

(3) Partial or entire elimination of briefs as referred to in paragraph (2) is performed based on Consent or in accordance with provisions under other laws and regulations which specifically regulate within respective sectors for that matter.

CHAPTER III
RIGHTS OF DATA SUBJECT

Article 26

Data Subject has the right:

a. over confidentiality of its Personal Data;
b. to file complaint in the event of dispute settlement of Personal Data on the failure of protection of confidentiality of its Personal Data by Electronic System Provider to Minister;

c. to obtain access or opportunity to modify or update its Personal Data without interrupting the management system of Personal Data, unless deemed otherwise by provisions under laws and regulations;
d. to obtain access or opportunity to obtain the history of its Personal Data which have been handed over to Electronic System Provider, provided that it is still in accordance with provisions under laws and regulations; and
e. to request destruction of its Certain Individual Data within Electronic System as managed by Electronic System Provider, unless deemed otherwise by provisions under laws and regulations.

CHAPTER IV
OBLIGATIONS OF USER

Article 27

User is obliged:
a. to maintain the confidentiality of Personal Data as acquired, collected, processed, and analyzed by it;
b. to use Personal Data in accordance only with the needs of the User;
c. to protect Personal Data, as well as documents containing such Personal Data from misuse activities; and
d. be held liable over Personal Data existing under its possession, either possession based on organization which is under its authority or individual, if there is any misuse activity.

CHAPTER V
OBLIGATIONS OF ELECTRONIC SYSTEM PROVIDER

Article 28

Any Electronic System Provider is obliged:
a. to perform certification of Electronic System under its management in accordance with provisions under laws and regulations;

b. to maintain veracity, validity, confidentiality, accuracy and relevance, as well as conformity with the purposes of acquisition, collection, processing, analysis, storage, display, publication, transfer, dissemination, and destruction of Personal Data;

c. to notify in writing to Data Subject if failure of protection of Personal Data within Electronic System under its management occurs, with the following notification provisions:

   1. should be accompanied with reason or cause on the occurrence of failure of protection of confidentiality of Personal Data;
   2. may be performed electronically if Data Subject has given Consent for that, which was declared when acquisition and collection of its Personal Data was performed;
   3. should be ascertained that it has been received by Data Subject if such failure involves loss potential for the party in question; and
   4. written notification is delivered to Data Subject within 14 (fourteen) days at maximum since such failure has been noticed.

d. to have internal rules in relation to Personal Data protection which are in accordance with provisions under laws and regulations;

e. to provide audit trail of all activities on the organization of Electronic System under its management;

f. to give options for Data Subject on Personal Data under its management may/or may not be used and/or displayed by/to third party based on Consent, provided that it is still in relation to the purposes of acquisition and collection of Personal Data;

g. to give access or opportunity for Data Subject to modify or update its Personal Data without interrupting the management system of Personal Data, unless deemed otherwise by provisions under laws and regulations;

h. to destruct Personal Data in accordance with provisions under this Regulation of the Minister or provisions under other laws and regulations which specifically regulate within respective Supervising Institution and Sectoral Regulator for that matter; and

i. to provide contact person (*narahubung*) which is contactable by Data Subject in relation to management of its Personal Data.

CHAPTER VI
DISPUTE SETTLEMENT

Article 29

(1) Any Data Subject and Electronic System Provider may file complaint to Minister on failure of protection of confidentiality of Personal Data.

(2) Complaint as referred to in paragraph (1) is intended as the dispute-settlement effort in amicable manner or through other alternative settlement efforts.

(3) Complaint as referred to in paragraph (1) is performed based on the reasons of:

a. non-performance of written notification on failure of protection of confidentiality of Personal Data by Electronic System Provider toward Data Subject or other Electronic System Provider in relation to such Personal Data, either having or not having potential of incurring losses; or

b. the incurring losses for Data Subject or other Electronic System Provider in relation to failure of protection of confidentiality of such Personal Data, although written notification on failure of protection of confidentiality of Personal Data has been performed, but the notification's timing is late.

(4) Minister may enter into coordination with heads of Supervising Institution and Sectoral Regulator to follow-up complaint as referred to in paragraph (1).

Article 30

(1) Minister delegates authority for dispute settlement of Personal Data as referred to under Article 29 to Director General.

(2) Director General may constitute Personal Data dispute settlement panel.

Article 31

Complaint and handling of complaint are performed based on procedures, as follows:

a. complaint is made no later than 30 (thirty) business days since the complainant realizes the information as referred to under Article 29 paragraph (3) letter a or letter b;

b. complaint is filed in writing, containing:

1. name and address of complainant;
2. reason or ground for complaint;
3. request for the settlement of complained problem; and
4. location of complaint, time when filing the complaint, and signature of the complainant.

c. complaint should be accompanied with supporting evidences;

d. official/team for Personal Data dispute settlement of failure of protection of confidentiality of Personal Data must respond the complaint within 14 (fourteen) business days at maximum since the complaint was received, which at least addresses complete or incomplete complaint;

e. incomplete complaint should be completed by complainant within 30 (thirty) business days since the complainant receives response as referred to in letter d and if exceeds such timeframe, complaint is deemed to be canceled;

f. official/team for Personal Data dispute settlement of failure of protection of confidentiality of Personal Data must handle settlement of complaint starting from 14 (fourteen) business days after the complaint was completely received;

g. dispute settlement based on such complete complaint is performed in amicable manner or through other alternative settlement efforts in accordance with provisions under laws and regulations; and

h. official/team for Personal Data dispute settlement of failure of protection of confidentiality of Personal Data which handles complaint may issue recommendation to Minister for imposition of administrative sanctions toward Electronic System Provider, although the complaint may or may not be settled in amicable manner or through other alternative settlement efforts.

Article 32

(1) In the course that dispute settlement effort through amicable manner or through other alternative settlement efforts are yet to settle the dispute on failure of protection of confidentiality of Personal Data, any Data Subject and Electronic System Provider may file a claim against the occurrence of failure of protection of confidentiality of Personal Data.

(2) Claim as referred to in paragraph (1) only takes form as civil lawsuit and be filed in accordance with provisions under laws and regulations.

Article 33

(1) If in the course of law enforcement process by law enforcers in accordance with provisions under laws and regulations, the authorized parties should conduct seizure, then only Personal Data in relation to the legal case which may be seized without having to seize the entire Electronic System.

(2) Electronic System Provider which provides, stores, and/or manages Personal Data as seized in accordance with paragraph (1) is prohibited from performing any conduct which may cause the alteration or missing of such Personal Data and must still maintain security or provide protection of confidentiality of Personal Data within Electronic System under its management.

CHAPTER VII
ROLES OF GOVERNMENT AND COMMUNITY

Article 34

(1) In order to ease the organization of Personal Data protection within Electronic System and in order to empower participation of community, Director General performs education toward the community on:

a. definition of Personal Data;
b. essence of Personal Data which are private in nature;
c. definition of Consent and its consequence;
d. definition of Electronic System and its mechanism;
e. rights of Data Subject, obligations of User, and obligations of Electronic System Provider;
f. provisions on dispute settlement if failure of protection of confidentiality of Personal Data by Electronic System Provider occurs; and
g. provisions under other laws and regulation in relation to Personal Data protection within Electronic System

(2) Community may participate in the course of performance of education as referred to in paragraph (1).

(3) Implementation of provisions as referred to in paragraph (1) may be performed through education and/or training, advocacy, technical counseling, and socialization by using various media.

CHAPTER VIII
SUPERVISION

Article 35

(1) Supervision of implementation of this Regulation of the Minister is performed by Minister and/or heads of Supervising Institution and Sectoral Regulator.

(2) Supervision as performed by Minister as referred to in paragraph (1) encompasses direct or indirect supervision.

(3) Minister has the authority to request data and information from Electronic System Provider in the event of Personal Data protection.

(4) Request of data and information as referred to in paragraph (3) may be performed periodically or incidentally if necessary.

(5) Minister delegates the supervisory authority to Director General.

CHAPTER IX
ADMINISTRATIVE SANCTIONS

Article 36

(1) Any Person who acquires, collects, processes, analyzes, stores, displays, publishes, transfers, and/or disseminates Personal Data unlawfully or not in accordance with provisions under this Regulation of the Minister or other laws and regulations, is imposed with administrative sanctions in accordance with provisions under laws and regulations in the forms of:

a. verbal warning;

b. reprimand;

c. temporary suspension of activities; and/or

d. announcement on online website (*situs dalam jaringan*).

(2) Provisions on procedures for the implementation of administrative sanctions as referred to in paragraph (1) are addressed under Regulation of the Minister.

(3) Administrative sanctions are handed down by minister or relevant heads of supervising institution and sectoral regulator in accordance with provisions under laws and regulations.

(4) Imposition of sanctions by relevant heads of supervising institution and sectoral regulator as referred to in paragraph (3) is performed after entering into coordination with Minister.

CHAPTER X
MISCELLANEOUS PROVISIONS

Article 37

(1) If Data Subject is person who is classified in the category of child in accordance with provisions under laws and regulations, the giving of Consent as referred to under this Regulation of the Minister is performed by the parents or guardian of child in question.

(2) Parents as referred to in paragraph (1) are biological father or mother of child in question in accordance with provisions under laws and regulation.

(3) Guardian as referred to in paragraph (1) is person who assumes the obligation to foster child in question before such child becomes [*sic*] an adult in accordance with provisions under laws and regulations.

CHAPTER XI
TRANSITIONAL PROVISIONS

Article 38

Electronic System Provider which has provided, stored, and managed Personal Data prior to the entry into force of this Regulation of the Minister should continue to maintain the

confidentiality of Personal Data under its management and adjusts with this Regulation of the Minister within 2 (two) years at maximum.

CHAPTER XII
FINAL PROVISIONS

Article 39

This Regulation of the Minister enters into force on the date of its promulgation.

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

Established in Jakarta
on 7 November 2016
MINISTER OF COMMUNICATION AND INFORMATICS OF THE REPUBLIC OF INDONESIA,
signed.
RUDIANTARA

Promulgated in Jakarta
on 1 December 2016
DIRECTOR-GENERAL OF LAWS AND REGULATIONS
MINISTRY OF LAW AND HUMAN RIGHTS OF THE REPUBLIC OF INDONESIA,
signed.
WIDODO EKATJAHJANA

OFFICIAL GAZETTE OF THE REPUBLIC OF INDONESIA OF 2016 NUMBER 1829