Type: REGULATION (PER)

By: MINISTER OF COMMUNICATION AND INFORMATICS OF THE REPUBLIC OF INDONESIA

Number: 20 YEAR 2016

Date: NOVEMBER 7, 2016 (JAKARTA)

Title: PROTECTION OF PERSONAL DATA IN AN ELECTRONIC SYSTEM

BY THE GRACE OF THE ALMIGHTY GOD

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

Considering:

whereas to implement the provisions of Article 15 paragraph (3) of Government Regulation Number 82 Year 2012 regarding the Operation of Electronic System and Transaction, it is necessary to stipulate a Regulation of the Minister of Communication and Informatics regarding the Protection of Personal Data in an Electronic System;

In view of:

1. Law Number 11 Year 2008 regarding Electronic Information and Transactions (State Gazette of the Republic of Indonesia Year 2008 Number 58, Supplement to the State Gazette of the Republic of Indonesia Number 4843);

2. Law Number 39 Year 2008 regarding State Ministries (State Gazette of the Republic of Indonesia Year 2008 Number 166, Supplement to the State Gazette of the Republic of Indonesia Number 4916);

3. Government Regulation Number 82 Year 2012 regarding the Implementation of Electronic System and Transaction (State Gazette of the Republic of Indonesia Year 2012 Number 189, Supplement to the State Gazette of the Republic of Indonesia Number 5348);

4. Presidential Regulation Number 7 Year 2015 regarding the Organization of State Ministries (State Gazette of the Republic of Indonesia Year 2015 Number 8);

5. Presidential Regulation Number 54 Year 2015 regarding the Ministry of Communication and Informatics (State Gazette of the Republic of Indonesia Year 2015 Number 96);

6. Regulation of the Minister of Communication and Informatics Number 1 Year 2016 regarding the Organization and Working Procedures of the Ministry of Communication and Informatics (Official Gazette of the Republic of Indonesia Year 2016 Number 103);

HAS DECIDED:

To stipulate: REGULATION OF THE MINISTER OF COMMUNICATION AND INFORMATICS REGARDING THE PROTECTION OF PERSONAL DATA IN AN ELECTRONIC SYSTEM.

CHAPTER I
GENERAL PROVISIONS

Article 1

Referred to herein:

1. Personal Data shall be data on certain individuals retained, treated, and the accuracy of which is maintained as well as the confidentiality of which is protected.

2. Data on Certain Individuals shall be every accurate and actual information which is attached and may be identified, either directly or indirectly, to each individual the utilization of which is in accordance with the provisions of laws and regulations.

3. Personal Data Owners shall be individuals to which Data on Certain Individuals is attached.

4. Approval of Personal Data Owners hereinafter referred to as Approval shall be written statement either manual and/or electronic given by Personal Data Owners after obtaining complete explanation of the actions of Personal Data acquisition, collection, processing, analysis, retention, display, publication, transmission, and dissemination as well as confidentiality or non-confidentiality.

5. Electronic System shall be a set of electronic devices and procedures which function to prepare, collect, process, analyze, retain, display, publish, transmit, and/or disseminate electronic information.

6. Electronic System Operator shall be every Person, state administrator, Business Entity, and community providing, managing, and/or operating an Electronic System either individually or jointly to Electronic System Users for its personal purpose and/or another party's purpose.

7. Electronic System User hereinafter referred to as User shall be every Person, state administrator, Business Entity, and community utilizing goods, services, facilities, or information provided by Electronic System Operators.

8. Business Entity shall be an individual company or partnership company, either incorporated or unincorporated.

9. Minister shall be a minister organizing governmental affairs in the communication and informatic sector.

10. Director General shall be a director general in charge of the informatic application sector.

Article 2

(1) The Protection of Personal Data in an Electronic System shall include protection of the acquisition, collection, processing, analysis, retention, display, publication, transmission, dissemination, and destruction of Personal Data.

(2) The implementation of provisions as referred to in paragraph (1) must be based on the principle of good protection of Personal Data, including the following:

a. respect for Personal Data as privacy;

b. Personal Data shall be private in accordance with the Agreement and/or based on the provisions of laws and regulations;

c. based on Approval;

d. relevance to the purpose of acquisition, collection, processing, analysis, retention, display, publication, transmission, and dissemination;

e. feasibility of the Electronic System used;

f. good faith to immediately notify Personal Data Owners in writing of each failure in the protection of Personal Data;

g. availability of an internal rule of the management of Personal Data protection;

h. responsibility for Personal Data in Users' control;

i. ease of access and correction to Personal Data by Personal Data Owners; and

j. integrity, accuracy, and validity as well as update of Personal Data.

(3) The privacy as referred to in paragraph (2) sub-paragraph a shall be the freedom of Personal Data Owners to state whether or not Personal Data is confidential, unless otherwise determined in accordance with the provisions of laws and regulations.

(4) The approval as referred to in paragraph (2) sub-paragraph b shall be given after Personal Data Owners give confirmation of the accuracy, confidentiality status and purpose of Personal Data management.

(5) The validity as referred to in paragraph (2) sub-paragraph j shall be legality in the acquisition, collection, processing, analysis, retention, display, publication, transmission, dissemination, and destruction of Personal Data.

CHAPTER II
PROTECTION

Part One
General

Article 3

The Protection of Personal Data in an Electronic System shall be conducted in the following processes:

a. acquisition and collection;

b. processing and analysis;

c. retention;

d. display, publication, transmission, dissemination, and/or access opening; and

e. destruction.

Article 4

(1) The Electronic System used for the processes as referred to in Article 3 must be certified.

(2) The implementation of certification as referred to in paragraph (1) shall be in accordance with the provisions of laws and regulations.

Article 5

(1) Every Electronic System Operator must have an internal rule of the protection of Personal Data to implement the processes as referred to in Article 3.

(2) Every Electronic System Operator must make an internal rule of the protection of Personal Data as a preventive measure to prevent the occurrence of failure in the protection of Personal Data managed.

(3) The making of an internal rule as referred to in paragraph (1) and paragraph (2) must consider the aspects of technology application, human resources, method and cost as well as refer to the provisions of this Ministerial Regulation and other relevant laws and regulations.

(4) Other preventive measures to prevent the occurrence of failure in the protection of Personal Data managed must be taken by every Electronic System Operator, at least in the form of the following activities:

a. raising the awareness of human resources within its purview to provide the protection of Personal Data in an Electronic System managed; and

b. providing training on the prevention of failure in the protection of Personal Data in an Electronic System managed for human resources within its purview.

Article 6

Electronic System Operators implementing the processes as referred to in Article 3 shall be obligated to provide an approval form in Indonesian language to request Approval of the intended Personal Data Owners.

Part Two
Acquisition and Collection of Personal Data

Article 7

(1) The acquisition and collection of Personal Data by Electronic System Operators must be limited to information which is relevant and in accordance with its purpose as well as must be conducted accurately.

(2) Supervisory Agency and Sector Supervisor may determine the information which is relevant and in accordance with its purpose as referred to in paragraph (1).

Article 8

(1) In acquiring and collecting Personal Data, Electronic System Operators must respect private Personal Data of Personal Data Owners.

(2) Respect for private Personal Data of Personal Data Owners as referred to in paragraph (1) shall be given through the provision of choice in an Electronic System for Personal Data Owners on the following:

a. confidentiality or non-confidentiality of Personal Data; and
b. change, addition or update of Personal Data.

(3) The choice for Personal Data Owners on the confidentiality or non-confidentiality of Personal Data as referred to in paragraph (2) sub-paragraph a shall not be applicable if laws and regulations have expressly stated that Personal Data for several elements are specifically declared confidential.

(4) The choice for Personal Data Owners on the change, addition or update of Personal Data as referred to in paragraph (2) sub-paragraph b shall be to provide opportunity for Personal Data Owners if they intend to change their Data on Certain Individuals.

Article 9

(1) The acquisition and collection of Personal Data by Electronic System Operators must be based on Approval or based on the provisions of laws and regulations.

(2) Personal Data Owners giving Approval as referred to in paragraph (1) may state that their Data on Certain Individuals is confidential.

(3) In the event that the Approval as referred to in paragraph (2) does not include Approval to the disclosure of Personal Data confidentiality:

a. every Person conducting the acquisition and collection of Personal Data; and

b. Electronic System Operator;

must maintain the confidentiality of Personal Data.

(4) Provisions on the maintenance of confidentiality of Personal Data for every Person and Electronic System Operator as referred to in paragraph (3) shall be also applicable to Personal Data declared confidential in accordance with the provisions of laws and regulations.

Article 10

(1) Personal Data directly acquired and collected must be verified with Personal Data Owners.

(2) Personal Data indirectly acquired and collected must be verified based on the results of processing of various sources of data.

(3) The sources of data in the acquisition and collection of Personal Data as referred to in paragraph (2) must have a valid legal basis.

Article 11

(1) The Electronic System used for accommodating the acquisition and collection of Personal Data must:

a. have interoperability and compatibility capabilities; and
b. use a legal software.

(2) The interoperability and compatibility capabilities as referred to in paragraph (1) sub-paragraph a shall be in accordance with the provisions of laws and regulations.

(3) The interoperability as referred to in paragraph (2) shall be the capability of different Electronic Systems to operate integratedly.

(4) The compatibility as referred to in paragraph (2) shall be the compatibility of an Electronic System with another Electronic System

Part Three
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 Operators which have been expressly stated when acquiring and collecting it.

(2) The processing and analysis of Personal Data as referred to in paragraph (1) shall be conducted based on Approval.

Article 13

The provisions as referred to in Article 12 paragraph (2) shall not be applicable if the processed and analyzed Personal Data originates from Personal Data which has been displayed or published openly by an Electronic System for public services.

Article 14

The processed and analyzed Personal Data must be Personal Data the accuracy of which has been verified.

Part Four
Retention of Personal Data

Article 15

(1) Personal Data retained in an Electronic System must be Personal Data the accuracy of which has been verified.

(2) Personal Data retained in an Electronic System must be in the form of encrypted data.

(3) The Personal Data as referred to in paragraph (1) must be retained in an Electronic System:

a. in accordance with the provisions of laws and regulations providing for the obligation of retention period of Personal Data at each Sector Supervisory and Regulatory Agency; or

b. for not less than 5 (five) years, if there is no provision of laws and regulations which specifically provides for it.

Article 16

In the event that Personal Data Owners no longer become Users, Electronic System Operators shall be obligated to retain Personal Data in accordance with the deadline as referred to in Article 15 paragraph (2) as from the last date on which Personal Data Owners become Users.

Article 17

(1) The data center and disaster recovery center of Electronic System Operators for public services used for the process of Personal Data protection as referred to in Article 3 must be located in the territory of the state of the Republic of Indonesia.

(2) The data center as referred to in paragraph (1) shall be a facility used for placing an Electronic System and its relevant components for the purpose of data placement, retention and processing.

(3) The disaster recovery center as (1) shall be a facility used for recovering data or informasi as well as important functions of a disturbed or damaged Electronic System due to a disaster caused by the nature and/or human.

(4) Further provisions on the obligation of placement of data center and disaster recovery center in the territory of Indonesia as referred to in paragraph (1) shall be provided for by the relevant Sector Supervisory and Regulatory Agency in accordance with the provisions of laws and regulations following coordination with the Minister.

Article 18

(1) Retention of Personal Data in an Electronic System must be conducted in accordance with the provisions on procedure and facility of Electronic System safeguarding.

(2) The procedure and facility of Electronic System safeguarding as referred to in paragraph (1) shall be in accordance with the provisions of laws and regulations.

Article 19

In the event that the retention period of Personal Data has exceeded the deadline as referred to in Article 15 paragraph (2), Personal Data in an Electronic System may be deleted unless the Personal Data will continue to be used or utilized in accordance with the initial purpose of its acquisition and collection.

Article 20

In the event that Personal Data Owners request the deletion of their Data on Certain Individuals, the request for deletion shall be conducted in accordance with the provisions of laws and regulations.

Part Five
Display, Publication, Transmission,
Dissemination and/or Access Opening of Personal Data

Article 21

(1) The display, publication, transmission, dissemination and/or access opening of Personal Data in an Electronic System may only be conducted:

a. upon Approval unless otherwise determined by the provisions of laws and regulations; and

b. after the accuracy and suitability for the purpose of acquisition and collection of the Personal Data are verified.

(2) The display, publication, transmission, dissemination and/or access opening of Personal Data in an Electronic System Operator as referred to in paragraph (1) shall include the ones conducted among Electronic System Operators, between Electronic System Operators and Users, or among Users.

Article 22

(1) The transmission of Personal Data managed by Electronic System Operators at government agencies and regional governments as well as community or private parties domiciled in the territory of the state of the Republic of Indonesia to outside the territory of the state of the Republic of Indonesia must:

a. be coordinated with the Minister or official/institution authorized for it; and

b. apply the provisions of laws and regulations on the cross-border country exchange of Personal Data.

(2) The implementation of coordination as referred to in paragraph (1) subparagraph a shall be in the following form:

a. reporting the plan for implementation of Personal Data transmission, which shall at least contain clear name of the destination country, clear name of the receiving subject, date of implementation, and reason/purpose of transmission;

b. requesting advocacy, if necessary; and

c. reporting the results of activity implementation.

Article 23

(1) For the purpose of law enforcement process, Electronic System Operators shall be obligated to provide Personal Data contained in an Electronic System or Personal Data generated by an Electronic System upon valid request from law enforcement apparatus based on the provisions of laws and regulations.

(2) Personal Data as referred to in paragraph (1) shall be the Personal Data which is relevant and in accordance with the need of law enforcement.

Article 24

(1) The use and utilization of Personal Data displayed, published, received, and disseminated by Electronic System Operators must be based on Approval.

(2) The use and utilization of Personal Data as referred to in paragraph (1) must be in accordance with the purpose of acquisition, collection, processing, and/or analysis of Personal Data.

Part Six
Destruction of Personal Data

Article 25

(1) The destruction of Personal Data in an Electronic System may only be conducted if:

a. the retention period of Personal Data in an Electronic System based on this Ministerial Regulation or in accordance with the other provisions of laws and regulations which specifically provide for it at each Sector Supervisory and Regulatory Agency has been exceeded; or

b. upon request of Personal Data Owners, unless otherwise determined by the provisions of laws and regulations.

(2) The destruction as referred to in paragraph (1) must partially or entirely remove the documents related to Personal Data, including electronic or non-electronic documents managed by Electronic System Operators and/or Users thus the Personal Data cannot be re-displayed in an Electronic System unless Personal Data Owners provide their new Personal Data.

(3) Partial or entire removal of files as referred to in paragraph (2) shall be conducted based on Approval or in accordance with the other provisions of laws and regulations which specifically provide for it in each sector.

CHAPTER III
RIGHTS OF THE PERSONAL DATA OWNERS

Article 26

Personal Data Owners shall be entitled to the following:

a. confidentiality of their Personal Data;

b. filing complaints in the context of Personal Data dispute resolution with respect to failure in the protection of their Personal Data confidentiality by Electronic System Operators to the Minister;

c. having access or opportunity to change or update their Personal Data without disturbing the Personal Data management system, unless otherwise determined by the provisions of laws and regulations;

d. having access or opportunity to obtain the history of their Personal Data which has been given to Electronic System Operators insofar as it is still in accordance with the provisions of laws and regulations; and

e. requesting the destruction of their Data on Certain Individuals in an Electronic System managed by Electronic System Operators, unless otherwise determined by the provisions of laws and regulations.

CHAPTER IV
OBLIGATIONS OF THE USERS

Article 27

Users shall be obligated to the following:

a. maintaining the confidentiality of Personal Data acquired, collected, processed, and analyzed by them;

b. using Personal Data only in accordance with the need of the Users;

c. protecting Personal Data along with documents containing the Personal Data from the act of misuse; and

d. being responsible for Personal Data in their control, either organizational control constituting their authority or individual control, in the event of the act of misuse.

CHAPTER V
OBLIGATIONS OF THE ELECTRONIC SYSTEM OPERATORS

Article 28

Every Electronic System Operator shall be obligated to the following:

a. conducting the certification of Electronic System managed by them in accordance with the provisions of laws and regulations;

b. maintaining the correctness, validity, confidentiality, accuracy and relevance as well as compatibility with the purpose of acquisition, collection, processing, analysis, retention, display, publication, transmission, dissemination and destruction of Personal Data;

c. notifying Personal Data Owners in writing in the event of failure in the protection of confidentiality of Personal Data in an Electronic System managed by them, with the following provisions on notification:

1. must be completed with the reason or cause of occurrence of failure in protection of Personal Data confidentiality;

2. may be conducted electronically if Personal Data Owners have given Approval to it stated when the acquisition and collection of their Personal Data are conducted;

3. must be ensured that it has been received by Personal Data Owners if such failure has the potential for loss to the person concerned; and

4. written notification shall be sent to Personal Data Owners by no later than 14 (fourteen) days as from the identification of such failure;

d. having an internal regulation related to the protection of Personal Data which is in accordance with the provisions of laws and regulations;

e. providing audit track record on all activities of the operation of Electronic System managed by them;

f. giving options to Personal Data Owners on the Personal Data managed by them which may/or may not be used and/or displayed by/to third parties on Approval insofar as it is still related to the purpose of acquisition and collection of Personal Data;

g. giving access or opportunity to Personal Data Owners to change or update their Personal Data without disturbing the Personal Data management system, unless otherwise determined by the provisions of laws and regulations;

h. destroying Personal Data in accordance with the provisions of this Ministerial Regulation or other provisions of laws and regulations which specifically provide for it at each Sector Supervisory and Regulatory Agency; and

i. providing a contact person who is easily contacted by Personal Data Owners related to the management of their Personal Data.

CHAPTER VI
DISPUTE RESOLUTION

Article 29

(1) Every Personal Data Owner and Electronic System Operator may file a complaint to the Minister about failure in the protection of confidentiality of Personal Data.

(2) The complaint as referred to in paragraph (1) shall be intended as an effort to resolve a dispute by deliberation or through other alternative resolution efforts.

(3) The complaint as referred to in paragraph (1) shall be made based on the following reasons:

a. non-delivery of written notice of failure in the protection of confidentiality of Personal Data by Electronic System Operators to Personal Data Owners or other Electronic System Operators related to the Personal Data, either potentially or not potentially resulting in a loss; or

b. occurrence of a loss to Personal Data Owners or other Electronic System Operators related to failure in the protection of confidentiality of the Personal Data, despite the delivery of written notice of failure in the protection of confidentiality of Personal Data the time for notice of which is late.

(4) The Minister may coordinate with the leadership of the Sector Supervisory and Regulatory Agency to follow up the complaint as referred to in paragraph (1).

Article 30

(1) The Minister shall delegate the authority to resolve a Personal Data dispute as referred to in Article 29 to the Director General.

(2) The Director General may establish a panel for Personal Data dispute resolution.

Article 31

The complaint and handling of complaint shall be conducted based on the following procedures:

a. a complaint shall be made by no later than 30 (thirty) business days since the party filing the complaint is aware of the information as referred to in Article 29 paragraph (3) sub-paragraph a or sub-paragraph b;

b. a complaint shall be filed in writing which contains the following:

1. name and address of the party filing the complaint;
2. reason or basis for the complaint;
3. request for the resolution of the complained issue; and
4. place for the complaint, time for filing the complaint, and signature of the party filing the complaint.

c. the complaint must be completed with supporting evidence;

d. The Personal Data dispute resolution official/team with respect to failure in the protection of confidentiality of Personal Data shall be obligated to respond to the complaint by no later than 14 (fourteen) business days as from the receipt of complaint which shall at least state that the complaint is complete or incomplete;

e. incomplete complaint must be completed by the party filing the complaint by no later than 30 (thirty) business days as from the receipt of response by the party filing the complaint as referred to in sub-article d and if the deadline is exceeded, the complaint shall be considered cancelled;

f. The Personal Data dispute resolution official/institution with respect to failure in the protection of confidentiality of Personal Data shall be obligated to handle the resolution of complaint starting 14 (fourteen) business days as from the complete receipt of complaint;

g. dispute resolution based on complete complaint shall be conducted by deliberation or through other alternative resolution efforts in accordance with the provisions of laws and regulations; and

h. The Personal Data dispute resolution official/institution with respect to failure in the protection of confidentiality of Personal Data which handle a complaint may give recommendation to the Minister for the imposition of administrative sanctions to Electronic System Operators although the complaint is or is not resolved by deliberation or through other alternative resolution efforts.

Article 32

(1) In the event that the effort to resolve a dispute by deliberation or through other alternative resolution efforts has not been able to resolve the dispute about failure in the protection of confidentiality of Personal Data, every Personal Data Owner and Electronic System Operator may submit a claim for the occurrence of failure in the protection of confidentiality of Personal Data.

(2) The claim as referred to in paragraph (1) may only be in the form of civil claim and be submitted in accordance with the provisions of laws and regulations.

Article 33

(1) In the event that in the law enforcement process by law enforcement apparatus in accordance with the provisions of laws and regulations, the authorities must make confiscation, only Personal Data related to the legal case may be confiscated without the obligation to confiscate the entire Electronic System.

(2) Electronic System Operators providing, retaining, and/or managing Personal Data confiscated as referred to in paragraph (1) shall be prohibited from taking any action which may lead to the change or loss of the Personal Data and still be obligated to maintain the confidentiality or provide the protection of confidentiality of Personal Data in an Electronic System managed by them.

CHAPTER VII
ROLE OF THE GOVERNMENT AND COMMUNITY

Article 34

(1) In order to facilitate the implementation of protection of Personal Data in an Electronic System and to empower community participation, the Director General shall provide education to the community on the following:

a. definition of Personal Data;

b. nature of private Personal Data;

c. definition of Approval and the consequences thereof;

d. definition of Electronic System and the mechanism thereof;

e. rights of the Personal Data Owners, obligations of the Users, and obligations of the Electronic System Operators;

f. provisions on dispute resolution in the event of failure in the protection of confidentiality of Personal Data by Electronic System Operators; and

g. other provisions of laws and regulations related to the protection of Personal Data in an Electronic System.

(2) The community may participate in the provision of education as referred to in paragraph (1).

(3) The implementation of provisions as referred to in paragraph (1) may be conducted through education and/or training, advocacy, technical coaching, and dissemination by using various media.

CHAPTER VIII
SUPERVISION

Article 35

(1) The supervision of implementation of this Ministerial Regulation shall be conducted by the Minister and/or leadership of the Sector Supervisory and Regulatory Agency.

(2) The supervision conducted by the Minister as referred to in paragraph (1) shall include direct and indirect supervision.

(3) The Minister shall be authorized to request data and information from Electronic System Operators in the context of protection of Personal Data.

(4) The request for data and information as referred to in paragraph (3) may be conducted periodically or at any time if necessary.

(5) The Minister shall delegate the supervisory authority to the Director General.

CHAPTER IX
ADMINISTRATIVE SANCTIONS

Article 36

(1) Every Person acquiring, collecting, processing, analyzing, retaining, displaying, publishing, transmitting, and/or disseminating Personal Data not rightfully or not in accordance with the provisions of this Ministerial Regulation or other laws and regulations shall be subject to administrative sanctions in accordance with the provisions of laws and regulations in the following forms:

a. verbal warning;
b. written warning;
c. suspension of activities; and/or
d. announcement in an online website.

(2) The provisions on procedure for the implementation of administrative sanctions as referred to in paragraph (1) shall be provided for by a Ministerial Regulation.

(3) The administrative sanctions shall be imposed by the minister or leadership of the relevant sector supervisory and regulatory agency in accordance with the provisions of laws and regulations.

(4) The imposition of sanctions by the leadership of the relevant sector supervisory and regulatory agency as referred to in paragraph (3) shall be conducted following coordination with the Minister.

CHAPTER X
MISCELLANEOUS PROVISIONS

Article 37

(1) In the event that Personal Data Owners are persons included in the category of children in accordance with the provisions of laws and regulations, the grant of Approval referred to in this Ministerial Regulation shall be made by the parents or guardian of the children concerned.

(2) The parents as referred to in paragraph (1) shall be the biological father and mother of the children concerned in accordance with the provisions of laws and regulations.

(3) The guardian as referred to in paragraph (1) shall be a person having the obligation to take care of the children concerned before the children become adults in accordance with the provisions of laws and regulations.

CHAPTER XI
TRANSITIONAL PROVISIONS

Article 38

Electronic System Operators which have provided, retained, and managed Personal Data prior to the entry into force of this Ministerial Regulation must still maintain the confidentiality of Personal Data managed by them and adjust to this Ministerial Regulation by no later than 2 (two) years.

CHAPTER XII
CLOSING PROVISIONS

Article 39

This Ministerial Regulation shall enter into force on the date of its promulgation.

For public cognizance, hereby ordering the promulgation of this Ministerial Regulation by placing it in the Official Gazette of the Republic of Indonesia.

Stipulated in Jakarta
on November 7, 2016

MINISTER OF COMMUNICATION AND INFORMATICS OF THE
REPUBLIC OF INDONESIA,

signed
RUDIANTARA

Promulgated in Jakarta
on December 1, 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 YEAR 2016 NUMBER 1829

Issued as a true copy
Ministry of Communication and Informatics
Head of the Legal Affairs Bureau,

signed and stamp
Bertiana Sari

NOTE

Source: LOOSE LEAF REGULATION OF THE MINISTER OF COMMUNICATION AND INFORMATICS YEAR 2016