Revokes 82 Year 2012

Type:	GOVERNMENT REGULATION (PP)
By:	PRESIDENT OF REPUBLIC OF INDONESIA
Number:	71 YEAR 2019 (71/2019)
Date:	OCTOBER 4, 2019 (JAKARTA)
Source:	LN 2019/185 TLN 6400
Title:	ADMINISTRATION OF ELECTRONIC SYSTEMS AND TRANSACTIONS

BY THE GRACE OF THE ALMIGHTY GOD

THE PRESIDENT OF THE REPUBLIC OF INDONESIA,

Considering:

a. whereas with extremely fast development of information technology in order to encourage digital economic growth and state sovereignty enforcement on electronic information in the territory of the Unitary State of the Republic of Indonesia, comprehensive regulation of information technology utilization and electronic transactions is required;

b. whereas Government Regulation Number 82 Year 2012 regarding Administration of Electronic Systems and Transactions is no longer in accordance with the development of legal needs of the community, thus it needs to be replaced;

c. whereas based on the considerations as referred to in point a and point b, it is necessary to stipulate a Government Regulation on Administration of Electronic Systems and Transactions.

In view of:

1. Article 5 paragraph (2) of the 1945 Constitution of the Republic of Indonesia;

2. 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) as amended by Law Number 19 Year 2016 regarding the Amendment to Law Number 11 Year 2008 regarding Electronic Information and Transactions (State Gazette of the Republic of Indonesia Year 2016 Number 251, Supplement to the State Gazette of the Republic of Indonesia Number 5952).

HAS DECIDED:

To stipulate: GOVERNMENT REGULATION REGARDING ADMINISTRATION OF ELECTRONIC SYSTEMS AND TRANSACTIONS

CHAPTER I

GENERAL PROVISIONS

Article 1

Referred to herein as:

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

2. Electronic Transaction shall a legal action taken by using computers, computer networks, and/or other electronic media.

3. Electronic Agent shall be a device of an Electronic System made to take an automatic action on certain Electronic Information which is administered by a Person.

4. Electronic System Administrator shall be every Person, state administrator, Business Entity, and community which provide, manage, and/or operate an Electronic System individually or jointly for Electronic System Users for its personal purpose and/or the purpose of another party.

5. Public Scope Electronic System Administrator shall be the administration of Electronic Systems by a State Administrative Agency or an institution appointed by a State Administrative Agency.

6. Private Scope Electronic System Administrator shall be the administration of Electronic Systems by a Person, Business Entity, and the community.

7. Ministry or Institution shall be a State Administrative Agency tasked to supervise and issue regulations for its sector.

8. Electronic Information shall be a single or a set of Electronic Data, including but not limited to processed writing, audio, drawing, map, design, photograph, electronic data interchange (EDI), electronic mail, telegram, telex, telecopy or the like, alphabet, sign, figure, Access code, symbol, or perforation which has a meaning or can be understood by a person capable of understanding it.

9. Electronic Document shall be every Electronic Information made, forwarded, sent, received, or stored in an analog, digital, electromagnetic, optical form, or the like, which may be seen, displayed, and/or heard through a computer or Electronic System, including but not limited to writing, audio, drawing, map, design, photograph or the like, alphabet, sign, figure, Access code, symbol or perforation which has a meaning or can be understood by a person capable of understanding it.

10. Information Technology shall be a technique to collect, prepare, store, process, announce, analyze, and/or disseminate information.

11. Electronic System User shall be every Person, state administrator, Business Entity, and community which utilize goods, services, facilities, or information provided by an Electronic System Administrator.

12. Hardware shall be a single or a set of tools connected to an Electronic System.

13. Software shall be a single or a set of related computer programs, procedures, and/or documentation in the operations of Electronic Systems.

14. Electronic System Worthiness Test shall be a set of objective assessment processes on every component of Electronic Systems, both conducted independently and/or conducted by an authorized and competent institution.

15. Access shall be an activity to make an interaction with an independent or online Electronic System.

16. Administration of Electronic Transactions shall be a set of Electronic Transaction activities conducted by Senders and Receivers by using an Electronic System.

17. Electronic Contract shall be an agreement of the parties entered into through an Electronic System.

18. Sender shall be a legal subject which sends Electronic Information and/or Electronic Documents.

19. Receiver shall be a legal subject which receives Electronic Information and/or Electronic Documents from a Sender.

20. Electronic Certificate shall be an electronic certificate containing an Electronic Signature and identity indicating the legal subject status of the parties in an Electronic Transaction which is issued by an Electronic Certification Administrator.

21. Electronic Certification Administrator shall be a legal entity serving as a trustworthy party which gives and audits an Electronic Certificate.

22. Electronic Signature shall be a signature consisting of Electronic Information embedded, associated or related to other Electronic Information used as a means of verification and authentication.

23. Signatory shall be legal subject associated or related to an Electronic Signature.

24. Electronic Signature Maker shall be a Software or Hardware which is configured and used to make an Electronic Signature.

25. Electronic Signature Making Data shall be personal code, biometric code, cryptographic code, and/or code resulting from the transformation of manual signature into an Electronic Signature, including other codes resulting from the development of Information Technology.

26. Reliability Certification Body shall be an independent body established by professionals which is acknowledged, approved, and supervised by the Government with the authority to audit and issue a Reliability Certificate in Electronic Transactions.

27. Reliability Certificate shall be a document stating that the Business Player administering an Electronic Transaction has passed the audit or conformity test of Reliability Certification Body.

28. Business Player shall be every individual or Business Entity, both incorporated and unincorporated, established and domiciled or conducting activities in the jurisdiction of the Republic of Indonesia, individually and jointly, through a business activity implementation agreement in various economic sectors.

29. Personal Data shall be every data on a person either identified and/or identifiable separately or in combination with other information both directly and indirectly through an Electronic System and/or non-electronically.

30. Electronic Data shall be electronic data not limited to writing, audio, drawing, map, design, photograph, electronic data interchange (EDI), electronic mail, telegram, telex, telecopy or the like, alphabet, sign, figure, Access code, symbol, or perforation.

31. Domain Name shall be the internet address of state administrator, Person, Business Entity, and/or the community, which can be used in communicating through the internet, in the form of unique code or composition of characters to indicate a certain location in the internet.

32. Domain Name Registry shall be an administrator responsible for conducting the management, operations, and maintenance of Domain Name Electronic System administration.

33. Domain Name Registrar shall be a Person, Business Entity, or the community providing a Domain Name registration service.

34. Domain Name User shall be a Person, State Administrative Agency, Business Entity, or the community applying for registration for the use of Domain Name to Domain Name Registrars.

35. State Administrative Agency hereinafter referred to as an Agency shall be legislative, executive, and judicial institutions at the central and regional levels and other agencies formed by laws and regulations.

36. Person shall be an individual, either an Indonesian citizen, foreign citizen, or legal entity.

37. Business Entity shall be an individual company or partnership company, both incorporated and unincorporated.

38. Government shall be the Minister or another official appointed by the President.

39. Minister shall be the minister organizing government affairs in the area of communication and informatics.

CHAPTER II
ADMINISTRATION OF ELECTRONIC SYSTEMS

Part One
General

Article 2

(1) The administration of Electronic Systems shall be implemented by Electronic System Administrators.

(2) The Electronic System Administrators as referred to in paragraph (1) shall include:

a. Public Scope Electronic System Administrators; and

b. Private Scope Electronic System Administrators.

(3) Public Scope Electronic System Administrators shall include:

a. Agency; and

b. an institution appointed by an Agency.

(4) The Public Scope Electronic System Administrators as referred to in paragraph (2) sub-paragraph a shall not include Public Scope Electronic System Administrators constituting the regulatory and supervisory authorities of the financial sector.

(5) The Private Scope Electronic System Administrators as referred to in paragraph (2) sub-paragraph b shall include:

a. Electronic System Administrators regulated or supervised by a Ministry or Institution based on the provisions of laws and regulations; and

b. Electronic System Administrators having an online portal, site, or application through the internet which is used for:

1. providing, managing, and/or operating the offering and/or trading of goods and/or services;

2. providing, managing, and/or operating financial transaction services;

3. delivery of paid digital materials or contents through a data network either by way of downloads through a portal or site, delivery through an electronic mail, or through other applications to user devices;

4. providing, managing, and/or operating communication services including but not limited to short message, audio call, video call, electronic mail, and online conversation in the form of digital platform, network service and social media;

5. search engine service, service for the provision of Electronic Information in the form of writing, audio, drawing, animation, music, video, film, and game or a combination of part and/or all of them; and/or

6. Personal Data processing for operational activities of public services related to Electronic Transaction activities.

Article 3

(1) Every Electronic System Administrator must administer an Electronic System reliably and securely as well as responsibly for the proper operations of Electronic Systems.

(2) Electronic System Administrators shall be responsible for the administration of their Electronic System.

(3) The provisions as referred to in paragraph (2) shall not apply in the event that the occurrence of force majeure, mistake, and/or negligence of Electronic System Users can be proven.

Article 4

Insofar as not otherwise determined by a separate law, every Electronic System Administrator shall be obligated to operate an Electronic System which meet the following minimum requirements:

a. being able to redisplay Electronic Information and/or Electronic Documents completely according to the retention period stipulated by laws and regulations;

b. being able to protect the availability, integrity, authenticity, confidentiality, and accessibility of Electronic Information in the administration of Electronic Systems;

c. being able to operate in accordance with procedures or instructions in the administration of Electronic Systems;

d. equipped with procedures or instructions announced by a language, information, or symbol which can be understood the party concerned with the administration of Electronic Systems; and

e. having a sustainable mechanism to maintain the novelty, clarity, and responsibility of procedures or instructions.

Article 5

(1) Electronic System Administrators shall be obligated to ensure that their Electronic System does not contain prohibited Electronic Information and/or Electronic Documents in accordance with the provisions of laws and regulations.

(2) Electronic System Administrators shall be obligated to ensure that their Electronic System does not facilitate the dissemination of prohibited Electronic Information and/or Electronic Documents in accordance with the provisions of laws and regulations.

(3) The provisions on obligations of Electronic System Administrators as referred to in paragraph (1) and paragraph (2) shall be regulated by a Ministerial Regulation.

Part Two
Registration of Electronic Systems

Article 6

(1) Every Electronic System Administrator as referred to in Article 2 paragraph (2) shall be obligated to make registration.

(2) The obligation to make registration for Electronic System Administrators shall be performed before an Electronic System starts to be used by Electronic System Users.

(3) The registration of Electronic System Administrators as referred to in paragraph (1) shall be applied to the Minister through the online single submission service in accordance with the provisions of laws and regulations.

(4) Further provisions on the registration of Electronic System Administrators as referred to in paragraph (3) shall refer to norms, standards, procedures, and criteria regulated by a Ministerial Regulation.

Part Three
Hardware

Article 7

(1) The Hardware used by Electronic System Administrators must:

a. comply with the aspects of security, interconnectivity and compatibility with the system used;

b. have technical support, maintenance, and/or after-sales services from the seller or provider; and

c. have a service sustainability guarantee.

(2) The fulfillment of requirements as referred to in paragraph (1) must be made through certification or other similar evidence.

Part Four
Software

Article 8

The Software used by Electronic System Administrators must:

a. ensure the security and reliability of proper operations; and

b. ensure service sustainability.

Article 9

(1) A developer which provides Software specifically developed for Public Scope Electronic System Administrators shall be obligated to hand over the source code and documentation of Software to the Agency or institution concerned.

(2) The Agency or institution concerned as referred to in paragraph (1) shall be obligated to store the intended source code and documentation of Software in an appropriate means in accordance with the provisions of laws and regulations.

(3) In the event that the means as referred to in paragraph (2) has not been available, an Agency or institution may store the source code and documentation of Software at a source code escrow.

(4) A developer shall be obligated to ensure the acquisition and/or Access to the source code and documentation of Software for the trustworthy third party as referred to in paragraph (3).

(5) Public Scope Electronic System Administrators shall be obligated to ensure the confidentiality of the source code of Software used and only use it for the interests of the Public Scope Electronic System Administrators.

(6) Further provisions on the obligation to deliver the source code and documentation of Software to the Agency or institution as referred to in paragraph (1) and to store the source code and documentation of Software to a trustworthy third party as referred to in paragraph (3) shall be regulated by a Ministerial Regulation.

Part Five
Experts

Article 10

(1) The experts engaged by Electronic System Administrators must have competency in the Electronic System and Information Technology areas.

(2) The experts as referred to in paragraph (1) shall be obligated to comply with the provisions of laws and regulations.

Part Six
Governance of Electronic Systems

Article 11

(1) Electronic System Administrators must ensure:

a. the availability of service level agreement;

b. the availability of information security agreement regarding the Information Technology service used; and

c. security of the administered information and internal means of communication.

(2) The Electronic System Administrators as referred to in paragraph (1) must ensure the proper operations of every component and integrity of the entire Electronic System.

Article 12

Electronic System Administrators must apply risk management against the occurring damages or losses.

Article 13

Electronic System Administrators must have a governance policy, work operating procedure, and mechanism for audit conducted periodically on an Electronic System.

Article 14

(1) Electronic System Administrators shall be obligated to implement the principle of Personal Data protection in conducting Personal Data processing including:

a. the collection of Personal Data shall be conducted in a limited and specific manner, lawfully, fairly, with the acknowledgement and approval from Personal Data owners;

b. Personal Data processing shall be conducted according to its purposes;

c. Personal Data processing shall be conducted by ensuring the rights of Personal Data owners;

d. Personal Data processing shall be conducted in an accurate, complete, non-misleading, up-to-date, accountable manner, and by taking into account the purposes of Personal Data processing;

e. Personal Data processing shall be conducted by protecting the security of Personal Data from loss, misuse, unauthorized Access and disclosure, as well as change or damage to Personal Data;

f. Personal Data processing shall be conducted by informing the purposes of collection, processing activity, and failure in the protection of Personal Data; and

g. Personal Data processing shall be destroyed and/or deleted unless remaining in a retention period in accordance with the needs based on the provisions of laws and regulations.

(2) The Personal Data processing as referred to in paragraph (1) shall include:

a. acquisition and collection,

b. processing and analysis;

c. retention;

d. correction and update;

e. display, announcement, transfer, dissemination, or disclosure; and/or
f. deletion or destruction.

(3) Personal Data processing must comply with the provision on valid approval from Personal Data owners for 1 (one) or several certain purposes which have been notified to Personal Data owners.

(4) In addition to the approval as referred to in paragraph (3), Personal Data processing must comply with the provisions required for:

a. the fulfillment of agreement obligations in the event that a Personal Data owner is one of the parties or to comply with the request of Personal Data owners when an agreement will be entered into;

b. fulfillment of legal obligations of Personal Data controllers in accordance with the provisions of laws and regulations;

c. fulfillment of the protection of vital interest of Personal Data owners;

d. performance of authority of Personal Data controllers based on the provisions of laws and regulations;

e. fulfillment of the obligations of Personal Data controllers in public services for public interests; and/or

f. fulfillment of other valid interests of Personal Data controllers and/or Personal Data owners.

(5) In the event of failure in protection of Personal Data managed by them, Electronic System Administrators shall be obligated to notify the owners of the Personal Data in writing.

(6) Provisions on Personal Data processing techniques shall be regulated in accordance with the provisions of laws and regulations.

Article 15

(1) Every Electronic System Administrator shall be obligated to delete irrelevant Electronic Information and/or Electronic Documents under its control upon a request of the person concerned.

(2) The obligation to delete irrelevant Electronic Information and/or Electronic Documents as referred to in paragraph (1) shall consist of:

a. deletion (right to erasure); and

b. delisting from the search engine (right to delisting).

(3) Electronic System Administrators which are obligated to delete Electronic Information and/or Electronic Documents as referred to in paragraph (1) shall be Electronic System Administrators which acquire and/or process Personal Data under their control.

Article 16

(1) The irrelevant Electronic Information and/or Electronic Documents subject to deletion (right to erasure) as referred to in Article 15 paragraph (2) sub-paragraph a shall consist of Personal Data:

a. acquired and processed without the approval from Personal Data owners;

b. the approval of which has been withdrawn by Personal Data owners;

c. acquired and processed unlawfully;

d. no longer in accordance with the purposes of acquisition based on the agreement and/or provisions of laws and regulations;

e. the use of which has exceeded the period in accordance with the agreement and/or provisions of laws and regulations; and/or

f. displayed by Electronic System Administrators resulting in losses to Personal Data owners.

(2) The obligation to delete Electronic Information and/or Electronic Documents as referred to in paragraph (1) shall not apply in the event that the Electronic Information and/or Electronic Documents must be retained or are prohibited from being deleted by Electronic System Administrators in accordance with the provisions of laws and regulations.

Article 17

(1) The deletion of irrelevant Electronic Information and/or Electronic Documents delisted from the search engine (right to delisting) as referred to in Article 15 paragraph (2) sub-paragraph b shall be made based on a judicial stipulation.

(2) An application for the stipulation of deletion of Electronic Information and/or Electronic Documents to the local district court shall be made by the person concerned as a Personal Data owner in accordance with the provisions of laws and regulations.

(3) The application for deletion stipulation as referred to in paragraph (2) must contain:

a. identity of the applicant;

b. identity of the Electronic System Administrator and/or address of the Electronic System;

c. irrelevant Personal Data under the control of an Electronic System Administrator; and

d. reason for deletion request.

(4) In the event that the court grants an application for the deletion stipulation as referred to in paragraph (2), Electronic System Administrators shall be obligated to make the deletion of irrelevant Electronic Information and/or Electronic Documents.

(5) The judicial stipulation as referred to in paragraph (4) shall be a basis for the request for deletion of irrelevant Electronic Information and/or Electronic Documents by the person concerned to an Electronic System Administrator.

Article 18

(1) Every Electronic System Administrator shall be obligated to provide a mechanism for the deletion of irrelevant Electronic Information and/or Electronic Documents in accordance with the provisions of laws and regulations.

(2) The deletion mechanism as referred to in paragraph (1) shall at least contain the provisions on:

a. provision of a communication channel between Electronic System Administrators and Personal Data owners;

b. feature for the deletion of irrelevant Electronic Information and/or Electronic Documents which allows Personal Data owners to make the deletion of their Personal Data; and

c. collection of data on requests for the deletion of irrelevant Electronic Information and/or Electronic Documents.

(3) Further provisions on the deletion mechanism as referred to in paragraph (1) and paragraph (2) shall be regulated by a Ministerial Regulation.

(4) Provisions on the deletion mechanism in a certain sector may be made by the relevant Ministry or Institution after coordination with the Minister.

Article 19

(1) Electronic System Administrators must apply good and accountable Electronic System governance.

(2) The governance as referred to in paragraph (1) shall at least fulfill the following requirements:

a. availability of procedures or instructions in the administration of Electronic Systems documented and/or announced in a language, information, or symbol understood by the parties related to the administration of Electronic Systems;

b. existence of sustainable mechanism to maintain the novelty and clarity of implementation guideline procedure;

c. existence of supporting personnel institution and completeness for the proper operations of Electronic Systems;

d. existence of performance management application in the administered Electronic System to ensure the proper operations of Electronic Systems; and

e. existence of plan to maintain administration sustainability of the managed Electronic System.

(3) In addition to the requirements as referred to in paragraph (2), the relevant Ministry or Institution may determine other requirements stipulated in laws and regulations.

Article 20

(1) Public Scope Electronic System Administrators shall be obligated to have a business continuity plan to mitigate disturbances or disasters in accordance with the risks of the incurred impacts.

(2) Public Scope Electronic System Administrators shall be obligated to conduct the management, processing, and/or retention of Electronic Systems and Electronic Data in the territory of Indonesia.

(3) Public Scope Electronic System Administrators may conduct the management, processing, and/or retention of Electronic Systems and Electronic Data outside the territory of Indonesia in the event that the retention technology is not domestically available.

(4) The criteria of domestically unavailable retention technology as referred to in paragraph (3) shall be determined by a committee consisting of the ministry organizing government affairs in the area of communication and informatics, institution in charge of technology review and application affairs, institution in charge of cyber security affairs, and the relevant Ministry or Institution.

(5) The formation of committee as referred to in paragraph (4) shall be stipulated by the Minister.

(6) In the event that Public Scope Electronic System Administrators use a third party service, the Public Scope Electronic System Administrators shall be obligated to make data classification according to the risks incurred.

(7) Further provisions on the data classification according to risks as referred to in paragraph (6) shall be regulated by a Ministerial Regulation.

Article 21

(1) Private Scope Electronic System Administrators may conduct the management, processing, and/or retention of Electronic Systems and Electronic Data in the territory of Indonesia and/or outside the territory of Indonesia.

(2) In the event that the management, processing, and/or retention of Electronic Systems and Electronic Data outside the territory of Indonesia, Private Scope Electronic System Administrators shall be obligated to ensure the effectiveness of supervision by a Ministry or Institution and law enforcer.

(3) Private Scope Electronic System Administrators shall be obligated to give Access to Electronic System and Electronic Data in the context of supervision and law enforcement in accordance with the provisions of laws and regulations.

(4) Provisions on the management, processing, and retention of Electronic Systems and Electronic Data for Private Scope Electronic System Administrators in the financial sector shall be further regulated by the regulatory and supervisory authorities of the financial sector.

Part Seven
Safeguard of the Administration of Electronic Systems

Article 22

(1) Electronic System Administrators shall be obligated to provide the trail of audit of all administrative activities of Electronic Systems.

(2) The audit trail as referred to in paragraph (1) shall be used for the purpose of supervision, law enforcement, dispute resolution, verification, testing, and other examination.

Article 23

Electronic System Administrators shall be obligated to conduct the safeguard of Electronic System components.

Article 24

(1) Electronic System Administrators shall be obligated to have and implement the procedure and means for Electronic System safeguard in avoiding disturbances, failures, and losses.

(2) Electronic System Administrators shall be obligated to provide a safeguard system covering the procedure and system of prevention and mitigation of threats and attacks which cause disturbances, failures, and losses.

(3) In the event of system failure or disturbance having serious impacts as a result of action of another party on an Electronic System, Electronic System Administrators shall be obligated to safeguard Electronic Information and/or Electronic Documents and immediately report it at the first opportunity to the law enforcement apparatus and relevant Ministry or Institution.

(4) Further provisions on the safeguard system as referred to in paragraph (2) shall be regulated in a regulation of the head of institution organizing government affairs in the area of cyber security.

Article 25

Electronic System Administrators shall be obligated to redisplay Electronic Information and/or Electronic Documents completely in accordance with the stipulated format and retention period based on the provisions of laws and regulations.

Article 26

(1) Electronic System Administrators shall be obligated to maintain the confidentiality, integrity, authentication, accessibility, availability, and traceability of Electronic Information and/or Electronic Documents in accordance with the provisions of laws and regulations.

(2) In the administration of Electronic Systems allocated for transferable Electronic Information and/or Electronic Documents, the Electronic Information and/or Electronic Documents must be unique as well as explain their possession and ownership.

Article 27

Electronic System Administrators must ensure the functions of Electronic Systems in accordance with its allocation, by still taking into account interoperability and compatibility with the previous Electronic System and/or relevant Electronic System.

Article 28

(1) Electronic System Administrators shall be obligated to provide education to Electronic System Users.

(2) The education as referred to in paragraph (1) shall be at least regarding rights, obligations, and responsibilities of all relevant parties, as well as complaint filing procedure.

Article 29

Electronic System Administrators shall be obligated to deliver information to Electronic System Users at least on:

a. identity of the Electronic System Administrators;

b. transacted objects;

c. worthiness or security of the Electronic System;

d. device usage procedure;

e. contractual conditions;

f. procedure for achieving an agreement;

g. Personal Data privacy and/or protection guarantee; and

h. call center telephone number.

Article 30

(1) Electronic System Administrators shall be obligated to provide features in accordance with the characteristics of the Electronic System used by them.

(2) The features as referred to in paragraph (1) shall be at least facilities to:

a. make corrections;

b. cancel orders;

c. give confirmations or recommendations;

d. choose between proceeding with or stopping the next activity;

e. see the delivered information in the form of Electronic Contract offers or advertisements;

f. check the success or failure status of Electronic Transactions; and

g. read the agreement before making Electronic Transactions.

Article 31

Electronic System Administrators shall be obligated to protect their users and the community at large from losses incurred by the Electronic System administered by them.

Article 32

(1) Every person working in the administration of Electronic Systems shall be obligated to safeguard and protect Electronic System facilities and infrastructures or information channeled through an Electronic System.

(2) Electronic System Administrators shall be obligated to provide, educate, and train personnel tasked and being responsible for the safeguard and protection of Electronic System facilities and infrastructures.

Article 33

For the purpose of criminal justice process, Electronic System Administrators shall be obligated to give Electronic Information and/or Electronic Data contained in an Electronic System or Electronic Information and/or Electronic Data generated by an Electronic System upon a valid request from an investigator for certain criminal acts in accordance with the authority regulated in laws.

Part Eight
Electronic System Worthiness Test

Article 34

(1) Electronic System Administrators shall be obligated to conduct an Electronic System Worthiness Test.

(2) The obligation as referred to in paragraph (1) may be performed on all components or part of components in an Electronic System in accordance with the protection requirement characteristics and strategic nature of the administration of Electronic Systems.

Part Nine
Supervision

Article 35

(1) The Minister shall be authorized to conduct supervision of the administration of Electronic Systems.

(2) The supervision as referred to in paragraph (1) shall cover monitoring, control, examination, tracking, and safeguard.

(3) Provisions on supervision of the administration of Electronic Systems in a certain sector shall be made by the relevant Ministry or Institution after coordination with the Minister.

CHAPTER III
ELECTRONIC AGENT ADMINISTRATORS

Part One
Electronic Agent

Article 36

(1) Electronic System Administrators may administer their Electronic System by themselves or through an Electronic Agent.

(2) The Electronic Agent as referred to in paragraph (1) shall be part of an Electronic System.

(3) The obligations of Electronic System Administrators shall apply //mutatis mutandis// to Electronic Agent administrators.

(4) An Electronic Agent may be in the form of:

a. visual;

b. audio;

c. Electronic Data; and

d. other forms.

Article 37

(1) Electronic Agent administrators shall be obligated to contain or provide information to protect user rights in the Electronic Agent administered by them, including at least information on:

a. identity of the Electronic Agent administrators;

b. transacted objects;

c. worthiness or security of the Electronic Agent;

d. device usage procedure;

e. contractual conditions;

f. procedure for achieving an agreement;

g. Personal Data privacy and/or protection guarantee; and

h. call center telephone number.

(2) Electronic Agent administrators shall be obligated to contain or provide features in order to protect user rights in the Electronic Agent administered by them in accordance with the characteristics of the Electronic Agent used by them.

(3) The features as referred to in paragraph (2) shall be facilities to:

a. make corrections;

b. cancel orders;

c. give confirmations, or recommendations;

d. choose between proceeding with or stopping the next activity;

e. see the delivered information in the form of Electronic Contract offers or advertisements;

f. check the success or failure status of transactions; and/or

g. read the agreement before making transactions.

(4) Electronic Agent administrators must provide features in the Electronic Agent operated by them which allow its users to make a change of information which is still in a transaction process.

Article 38

(1) An Electronic Agent may be administered for more than 1 (one) interest of Electronic System Administrators based on an agreement between the parties.

(2) The agreement as referred to in paragraph (1) must at least contain:

a. rights and obligations;

b. responsibilities;

c. mechanism for complaints and dispute resolution;

d. period;

e. fees;

f. scope of services; and

g. choice of law.

(3) In the event that an Electronic Agent is administered for more than 1 (one) interest of Electronic System Administrators, Electronic Agent administrators shall be obligated to give the same treatment to the Electronic System Administrators using the Electronic Agent.

(4) In the event that an Electronic Agent is administered for the interests of more than 1 (one) Electronic System Administrators, administrators of the Electronic Agent shall be considered as a separate Electronic System Administrator.

Part Two
Obligations

Article 39

(1) In the administration of Electronic Agent, Electronic Agent administrators must take into account the following principles:

a. prudence;

b. safeguard and integration of Information Technology system;

c. safeguard control over Electronic Transaction activities,

d. cost effectiveness and efficiency; and

e. consumer protection in accordance with the provisions of laws and regulations.

(2) Electronic Agent administrators shall be obligated to have and implement standard operating procedures fulfilling the principles of safeguard control over user data and Electronic Transactions.

(3) The principles of safeguard control over user data and Electronic Transactions as referred to in paragraph (2) shall include:

a. confidentiality;

b. integrity;

c. availability;

d. authentication;

e. authorization; and

f. non-repudiation.

Article 40

(1) Electronic Agent administrators shall be obligated to:

a. conduct an identity authentication testing and examine the authorization of Electronic System Users making Electronic Transactions;

b. have and implement policies and procedures to take actions in the event of indication of data theft;

c. ensure control over the authorization and right of Access to Electronic Transaction system, database, and application;

d. prepare and implement methods and procedures to protect and/or keep confidential data integrity, records, and information related to Electronic Transactions;

e. have and implement standards and control over the use and protection of data if service providers have Access to the data;

f. have a business sustainability plan including an effective contingency plan to ensure the sustainable availability of Electronic Transaction systems and services; and

g. have procedures for fast and appropriate handling of unforeseeable events to reduce the impacts of an incident, fraud, and Electronic System failure.

(2) Electronic Agent administrators shall be obligated to prepare and stipulate procedures for guaranteeing Electronic Transactions thus they cannot be denied by consumers.

CHAPTER IV
ADMINISTRATION OF ELECTRONIC TRANSACTIONS

Part One
Scope of the Administration of Electronic Transactions

Article 41

(1) The Administration of Electronic Transactions may be conducted in a public or private scope.

(2) The Administration of Electronic Transactions in a public scope shall include the Administration of Electronic Transactions by:

a. an Agency;

b. an institution appointed by an Agency;

c. inter-Agency;

d. inter-appointed institution;

e. between an Agency and appointed institution; and

f. between an Agency or institution and Business Player in accordance with the provisions of laws and regulations.

(3) The Administration of Electronic Transactions in a private scope shall include the following Electronic Transactions:

a. inter-Business Player;

b. between a Business Player and consumer; and

c. interpersonal.

Part Two
Requirements for the Administration of Electronic Transactions

Article 42

(1) The Administration of Electronic Transactions must use an Electronic Certificate issued by an Indonesian Electronic Certification Administrator.

(2) The Administration of Electronic Transactions may use a Reliability Certificate.

(3) In the event that a Reliability Certificate is used as referred to in paragraph (2), the Administration of Electronic Transactions must use a Reliability Certificate issued by a registered Reliability Certification Body.

Article 43

The Administration of Electronic Transactions conducted by Public Scope Electronic System Administrators must take into account the aspects of security, reliability, and efficiency.

Article 44

(1) Senders shall be obligated to ensure that the sent Electronic Information is correct and is not disturbing.

(2) Further provisions on the sending of Electronic Information shall be regulated in a Ministerial Regulation.

Part Three
Requirements of Electronic Transactions

Article 45

(1) Electronic Transactions made by the parties shall have legal consequences to the parties.

(2) The Administration of Electronic Transactions made by the parties must take into account:

a. good faith;

b. prudential principle;

c. transparency;

d. accountability; and

e. reasonableness.

Article 46

(1) Electronic Transactions may be made based on an Electronic Contract or other contractual forms as a form of agreement entered into by the parties.

(2) An Electronic Contract shall be considered valid if:

a. there is an agreement of the parties;

b. made by a legal subject which is capable or which is authorized to represent in accordance with the provisions of laws and regulations;

c. there are certain matters; and

d. transaction objects may not contradict laws and regulations, morality, and public order.

Article 47

(1) The Electronic Contract and other contractual forms as referred to in Article 46 paragraph (1) addressed to Indonesian population must be made in the Indonesian Language.

(2) An Electronic Contract made by standard clauses must be in accordance with the provisions on standard clauses as regulated in laws and regulations.

(3) An Electronic Contract shall at least contain:

a. identity data of the parties;

b. objects and specifications;

c. requirements of Electronic Transactions;

d. prices and fees;

e. procedures in the event of cancellation by the parties;

f. provisions which grant a right to the prejudiced party to be able to recover goods and/or request for product replacement in case of a hidden defect; and

g. choice of law for the settlement of Electronic Transactions.

Article 48

(1) Business Players offering products through an Electronic System must provide complete and correct information related to contract conditions, producers, and the offered products.

(2) Business Players shall be obligated to give information clarity regarding contract offers or advertisements.

(3) Business Players shall be obligated to give a deadline to consumers and/or contract receivers to return the delivered goods and/or the provided services if they are not in accordance with the contract or there is a hidden defect.

(4) Business Players shall be obligated to provide information on the delivered goods and/or the provided services.

(5) Business Players may not charge consumers regarding the obligation to pay the delivered goods and/or the provided services without any contract basis.

Article 49

(1) Electronic Transactions shall take place when an agreement of the parties is achieved.

(2) Unless otherwise determined by the parties, the agreement as referred to in paragraph (1) shall take place when a transaction offer sent by a Sender has been received and approved by a Receiver.

(3) The agreement as referred to in paragraph (2) may be entered into by way of:

a. acceptance action stating an agreement; or

b. acceptance and/or object usage actions by Electronic System Users.

Article 50

(1) In the Administration of Electronic Transactions, parties must ensure:

a. provision of correct data and information; and

b. availability of facilities and services as well as complaint resolution.

(2) In the Administration of Electronic Transactions, parties must determine the choice of law equally for the implementation of Electronic Transactions.

CHAPTER V
ADMINISTRATION OF ELECTRONIC CERTIFICATION

Part One
Electronic Certificate

Article 51

(1) The Electronic System Administrator as referred to in Article 2 paragraph (2) shall be obligated to have an Electronic Certificate.

(2) Electronic System Users may use an Electronic Certificate in Electronic Transactions.

(3) to have an Electronic Certificate, Electronic System Administrators and Electronic System Users must submit an application to an Indonesian Electronic Certification Administrator.

(4) If necessary, a Ministry or Institution may obligate Electronic System Users to use an Electronic Certificate in Electronic Transactions.

(5) Further provisions on the use of Electronic Certificate as referred to in paragraph (4) shall be regulated by a Ministry or Institution.

(6) Further provisions on the procedure for having an Electronic Certificate shall be regulated in a Ministerial Regulation.

Part Two
Electronic Certification Administrators

Article 52

Electronic Certification Administrators shall be authorized to conduct:

a. the examination of Electronic Certificate owner and/or holder candidates, issuance of Electronic Certificate, extension of the validity period of Electronic Certificate, blocking and revocation of Electronic Certificate, validation of Electronic Certificate; and preparation of the list of active and revoked Electronic Certificates; and

b. the making, verification, and validation of Electronic Signature and/or other services using an Electronic Certificate.

Article 53

(1) Electronic Certification Administrators shall consist of:

a. Indonesian Electronic Certification Administrators; and

b. foreign Electronic Certification Administrators.

(2) The administration of Indonesian electronic certification shall stick to the one parent principle.

(3) Indonesian Electronic Certification Administrators shall be obligated to have an acknowledgement from the Minister by referring to the parent Electronic Certification Administrator organized by the Minister.

(4) Indonesian Electronic Certification Administrators must have an assessment from an accredited Electronic Certification Administrator certification body.

(5) Foreign Electronic Certification Administrators operating in Indonesia must be registered in Indonesia.

(6) Further provisions on the registration of foreign Electronic Certification Administrators as referred to in paragraph (5) shall be regulated in a Ministerial Regulation.

Article 54

(1) The acknowledgement of Indonesian Electronic Certification Administrators as referred to in Article 53 paragraph (3) shall be given by the Minister after the Indonesian Electronic Certification Administrators fulfill the acknowledgement process requirements regulated in a Ministerial Regulation.

(2) The list of acknowledged Indonesian Electronic Certification Administrators including the services provided by them shall be made, maintained, and published by the Minister.

(3) Further provisions on the procedure for acknowledgement of Indonesian Electronic Certification Administrators shall be regulated in a Ministerial Regulation.

Article 55

(1) Indonesia Electronic Certification Administrators shall be entitled to receive a revenue fee by charging a service fee from Electronic Certificate users.

(2) Indonesian Electronic Certification Administrators shall be obligated to pay every revenue from service fee for the use of Electronic Certificate calculated from a revenue percentage to the state.

(3) The revenue as referred to in paragraph (1) and paragraph (2) shall constitute non-tax state revenue.

Part Three
Supervision

Article 56

(1) The Minister shall conduct the supervision of:

a. administration of Indonesian electronic certification; and

b. foreign Electronic Certification Administrators.

(2) Supervision for the administration of Indonesian electronic certification as referred to in paragraph (1) sub-paragraph a shall include:

a. acknowledgement; and

b. operations of parent Electronic Certification Administrator facilities for Indonesian Electronic Certification Administrators.

(3) Further provisions on the supervision of administration of Indonesian electronic certification and foreign Electronic Certification Administrators shall be regulated in a Ministerial Regulation.

Part Four
Services of Electronic Certification Administrators

Paragraph 1
General

Article 57

(1) Indonesian Electronic Certification Administrators shall provide certified services.

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

a. Electronic Signature; and/or

b. other services using an Electronic Certificate.

(3) The other services as referred to in paragraph (2) sub-paragraph b shall include:

a. electronic seal;

b. electronic time stamp;

c. electronic registered delivery service;

d. website authentication; and/or

e. preservation of Electronic Signature and/or electronic seal.

Article 58

(1) Indonesian Electronic Certification Administrators shall bear losses caused by deliberateness or negligence to Persons, Business Entities or Agencies due to their failure in fulfilling their obligations as regulated in this Government Regulation.

(2) Indonesian Electronic Certification Administrators shall be considered deliberate or negligent unless the Indonesian Electronic Certification Administrators can prove that losses arise not due to their deliberateness or negligence.

(3) The responsibility for substantiation of deliberateness or negligence committed by a party which is not an Indonesian Electronic Certification Administrator shall be the responsibility of Persons, Business Entities or Agencies suffering the losses.

Paragraph 2
Electronic Signature

Article 59

(1) An Electronic Signature used in Electronic Transactions may be generated through various signing procedures.

(2) In the event of use of Electronic Signature to represent Business Entities, the Electronic Signature shall be referred to as an electronic seal.

(3) The Electronic Signature as referred to in paragraph (1) and paragraph (2) shall have valid legal force and legal consequences insofar as fulfilling the following requirements:

a. Electronic Signature Making Data shall be related only to a Signatory;

b. Electronic Signature Making Data at the time of electronic signing process shall be only in the possession of Signatory;

c. all changes in Electronic Signatures taking place after the time of signing can be identified;

d. all changes in Electronic Information related to the Electronic Signature after the time of signing can be identified;

e. there is a certain method used to identify its Signatory; and

f. there is a certain method to indicate that the Signatory has given an approval of the relevant Electronic Information.

Article 60

(1) An Electronic Signature shall serve as a means of authentication and verification of:

a. identity of Signatory; and

b. integrity and authentication of Electronic Information.

(2) An Electronic Signature shall include:

a. certified Electronic Signature; and

b. uncertified Electronic Signature.

(3) The certified Electronic Signature as referred to in paragraph (2) sub-paragraph a must:

a. fulfill the validity of legal force and legal consequences of Electronic Signature as referred to in Article 59 paragraph (3);

b. use an Electronic Certificate made by the services of Indonesian Electronic Certification Administrators; and

c. be made by using a certified Electronic Signature Maker.

(4) The uncertified Electronic Signature as referred to in paragraph (2) sub-paragraph b shall be made without using the services of Indonesian Electronic Certification Administrators.

Paragraph 3
Electronic Signature Making Data

Article 61

(1) Electronic Signature Making Data must uniquely refer only to the Signatory and may be used to identify the Signatory.

(2) The Electronic Signature Making Data as referred to in paragraph (1) may be made by Electronic Certification Administrators.

(3) The Electronic Signature Making Data as referred to in paragraph (1) and paragraph (2) must fulfill the following provisions:

a. if using a cryptographic code, Electronic Signature Making Data must not be easily identifiable from Electronic Signature verification data through a certain calculation, in a certain time period, and by a reasonable means;

b. Electronic Signature Making Data shall be stored in an electronic media located in the possession of the Signatory; and

c. data related to the Signatory must be stored in a place or means for data storage, using a trustworthy system of Electronic Certification Administrators which can detect any changes and fulfills the following requirements:

1. only an authorized person can input new data, change, exchange, or replace data;

2. the authentication of information on the identity of Signatory can be examined; and

3. other technical changes violating the security requirement can be detected or identified by administrators.

d. if Electronic Signature Making Data is made by Electronic Certification Administrators, the security and confidentiality of all making processes of Electronic Signature Making Data shall be guaranteed by Electronic Certification Administrators.

(4) A Signatory must maintain the confidentiality and be responsible for Electronic Signature Making Data.

Article 62

(1) In a signing process, a mechanism must be implemented to ensure that the Electronic Signature verification data related to Electronic Signature Making Data remains applicable or is not revoked.

(2) In a signing process, a mechanism must be implemented to ensure that Electronic Signature Making Data:

a. is not reported lost;

b. is not reported transferred to an unauthorized person; and

c. is in the possession of the Signatory.

(3) Before signing, the Electronic Information to be signed must be known and understood by the Signatory.

(4) The approval of Signatory to the Electronic Information to be signed by an Electronic Signature must use an affirmation mechanism and/or other mechanisms indicating the purpose and objective of the Signatory to be bound in an Electronic Transaction.

(5) An Electronic Signature in Electronic Information shall at least:

a. be made using Electronic Signature Making Data; and

b. set out the time of signing.

(6) A change of Electronic Signature and/or Electronic Information signed after the time of signing must be identified, detected, or recognized by a certain method or by a certain way.

Article 63

(1) A Signatory may entrust its Electronic Signature Making Data to an Electronic Certification Administrator.

(2) The Electronic Signature Making Data as referred to in paragraph (1) may be entrusted only to Indonesian Electronic Certification Administrators.

(3) In the event that Electronic Certification Administrators store Electronic Signature Making Data, the Electronic Certification Administrators shall be obligated to:

a. ensure that the use of Electronic Signature Making Data is only in the possession of the Signatory;

b. use a certified Electronic Signature Maker in the storage process of Electronic Signature Making Data; and

c. ensure that the mechanism used for the use of Electronic Signature Making Data for an Electronic Signature applies a combination of not less than 2 (two)-factor authentication.

(4) Provisions on the certified Electronic Signature Maker as referred to in paragraph (3) sub-paragraph b shall be stipulated in a Ministerial Regulation.

Article 64

(1) Before an Electronic Signature is used, Electronic Certification Administrators shall be obligated to ensure the preliminary identification of Signatory by way of:

a. the Signatory shall submit identity to Electronic Certification Administrators;

b. the Signatory shall make registration with Electronic Certification Administrators; and

c. if necessary, Electronic Certification Administrators may confidentially transfer data on Signatory identity to another Electronic Certification Administrator with the approval of Signatory.

(2) The mechanism used for the use of Electronic Signature Making Data for an Electronic Signature applies a combination of not less than 2 (two)-factor authentication.

(3) The verification process of signed Electronic Information may be conducted by examining Electronic Signature verification data to track every change in the signed data.

Paragraph 4
Electronic Seal

Article 65

The regulation on Electronic Signature shall apply //mutatis mutandis// to the regulation on electronic seal.

Paragraph 5
Electronic Time Stamp

Article 66

Electronic time stamp services shall consist of:

a. certified electronic time stamp services; and

b. uncertified electronic time stamp services.

Article 67

(1) The requirements of certified electronic time stamp must fulfill the following requirements:

  a. binding date and time with Electronic Information and/or Electronic Documents to prevent the possibility of undetected change in Electronic Information and/or Electronic Documents;

  b. referring to an accurate time source related to coordinated universal time;

  c. use an Electronic Certificate made by the services of Indonesian Electronic Certification Administrators; and

  d. signed using an Electronic Signature or electronic seal administered by an Indonesia Electronic Certification Administrator or using an equivalent method.

(2) A certified electronic time stamp must provide:

  a. accurate date and time; and

  b. integrity of Electronic Information and/or Electronic Documents related to the date and time.

(3) Uncertified electronic time stamp services shall be provided without using the services of Indonesian Electronic Certification Administrators.

(4) Further provisions on certified electronic time stamp shall be regulated by a Ministerial Regulation.

Paragraph 6
Electronic Registered Delivery Service

Article 68

An electronic registered delivery service shall consist of:

a. certified electronic registered delivery service; and

b. uncertified electronic registered delivery service.

Article 69

(1) Certified Electronic Certification Administrators providing a certified electronic registered delivery service shall be obligated to guarantee:

a. integrity of the transmitted data;

b. identifiable data Senders;

c. identifiable data Receivers; and

d. accuracy of data delivery and receipt date and time.

(2) The certified electronic registered delivery service as referred to in paragraph (1) must fulfill at least the following requirements:

a. provided by 1 (one) Indonesian Electronic Certification Administrator or more;

b. being able to identify the Sender accurately;

c. being able to identify the Receiver address before data delivery;

d. data delivery and receipt are safeguarded by an Electronic Signature and electronic seal from Indonesian Electronic Certification Administrators;

e. the change of data in the process of data delivery or receipt can be identified by the Sender and Receiver; and

f. time and date of delivery, receipt, and change of data can be displayed by a certified electronic time stamp.

(3) In the event that data delivery involves 2 (two) Indonesia Electronic Certification Administrators or more, all requirements as referred to in paragraph (2) shall apply to all of the involved Indonesian Electronic Certification Administrators.

(4) Uncertified electronic registered delivery service shall be provided without using the services of Indonesian Electronic Certification Administrators.

(5) Further provisions on electronic registered delivery service shall be regulated by a Ministerial Regulation.

Paragraph 7
Website Authentication

Article 70

Website authentication shall consist of:

a. certified website authentication; and

b. uncertified website authentication.

Article 71

(1) Electronic Certification Administrators providing a website authentication service must have a reliable method which is able to identify a Person or Business Entity responsible for the administration of website using the website authentication service.

(2) Website authentication shall be aimed at ensuring trust in making electronic transactions through a website.

(3) Certified website authentication must use an Electronic Certificate made by the services of Indonesian Electronic Certification Administrators.

(4) Information which must be contained in an Electronic Certificate used for website authentication shall include but not limited to:

a. name of Person, Business Entity, or Agency administering the website;

b. address of Person, Business Entity, or Agency at least explaining the city of domicile in which the Person, Business Entity, or Agency is operating;

c. Name of Domain operated by the website administrator;

d. validity period of Electronic Certificate;

e. identity of the Electronic Certification Administrator issuing the Electronic Certificate; and

f. Electronic Certificate number.

(5) Uncertified website authentication shall be provided without using the services of Indonesian Electronic Certification Administrators.

(6) Further provisions on the certified website authentication as referred to in paragraph (3) shall be regulated by a Ministerial Regulation.

Paragraph 8
Preservation of Electronic Signature and/or Electronic Seal

Article 72

(1) Preservation of Electronic Signature and/or electronic seal shall consist of:

a. certified preservation of Electronic Signature and/or electronic seal; and

b. uncertified preservation of Electronic Signature and/or electronic seal.

(2) Certified preservation of Electronic Signature and/or electronic seal must fulfill the following requirements:

a. use an Electronic Certificate made by the services of Indonesian Electronic Certification Administrators; and

b. the Certified Electronic Signature and/or electronic seal contained in Electronic Information and/or Electronic Documents can still be validated although the validity period of their Electronic Certificate expires.

(3) Uncertified preservation of Electronic Signature and/or electronic seal shall be made without using the services of Indonesian Electronic Certification Administrators.

(4) Further provisions on the certified preservation Electronic Signature and/or electronic seal shall be regulated by a Ministerial Regulation.

CHAPTER VI
RELIABILITY CERTIFICATION BODY

Article 73

(1) Business Players administering Electronic Transactions may be certified by a Reliability Certification Body.

(2) A Reliability Certification Body must be domiciled in Indonesia.

(3) A Reliability Certification Body shall be established by professionals.

(4) The professionals establishing a Reliability Certification Body as referred to in paragraph (3) shall at least include the following professions:

a. Information Technology consultant;

b. Information Technology auditor; and

c. legal consultant in the area of Information Technology.

(5) A Reliability Certification Body must be registered in the list of Reliability Certification Bodies issued by the Minister.

(6) Further provisions on requirements for the establishment of Reliability Certification Body shall be regulated in a Ministerial Regulation.

Article 74

(1) A Reliability Certificate shall be aimed at protecting consumers in Electronic Transactions.

(2) The Reliability Certificate as referred to in paragraph (1) shall be a guarantee that a Business Player has fulfilled the criteria determined by a Reliability Certification Body.

(3) The Business Player which has fulfilled the criteria as referred to in paragraph (2) shall be entitled to use a Reliability Certificate in pages and/or other Electronic Systems.

Article 75

(1) A Reliability Certification Body may issue a Reliability Certificate through a Reliability Certification process.

(2) The Reliability Certification process as referred to in paragraph (1) shall include the examination of complete and correct information of Business Players along with their Electronic Systems.

(3) The complete and correct information as referred to in paragraph (2) shall include but not limited to information which:

a. contains the identity of Business Players;

b. contains privacy protection policies and procedures;

c. contains system safeguard policies and procedures; and

d. contains a statement on the guarantee for the offered goods and/or services.

Article 76

(1) A Reliability Certificate issued by a Reliability Certification Body shall include the following category:

a. identity registration;

b. Electronic System security; and

c. privacy policy.

(2) The fulfillment of categorization as referred to in paragraph (1) shall determine a Reliability Certificate level.

(3) Further provisions on the regulation of Reliability Certificate level as referred to in paragraph (2) shall be regulated by a Ministerial Regulation.

Article 77

The supervision of Reliability Certification Bodies shall be conducted by the Minister.

Article 78

(1) To have an acknowledgement, Reliability Certification Bodies shall be subject to an administrative fee.

(2) Every revenue from the administrative fee as referred to in paragraph (1) shall constitute non-tax state revenue.

CHAPTER VII
MANAGEMENT OF DOMAIN NAMES

Article 79

(1) The management of Domain Names shall be administered by Domain Name managers.

(2) Domain Names shall consist of:

a. generic top-level Domain Names;

b. Indonesian top-level Domain Names;

c. Indonesian second-level Domain Names; and

d. Indonesian derivative-level Domain Names.

(3) The Domain Name managers as referred to in paragraph (1) shall consist of:

a. Domain Name Registries; and

b. Domain Name Registrars.

Article 80

(1) The Domain Name managers as referred to in Article 79 paragraph (3) may be administered by the Government and/or the community.

(2) The community as referred to in paragraph (1) must be incorporated in Indonesia.

(3) Domain Name managers shall be designated by the Minister.

Article 81

(1) The Domain Name Registries as referred to in Article 79 paragraph (3) sub-paragraph a shall implement the management of generic top-level Domain Names and Indonesian top-level Domain Names.

(2) Domain Name Registries may grant the authority to register generic top-level Domain Names and Indonesian top-level Domain Names to Domain Name Registrars.

(3) Domain Name Registries shall serve to:

a. give inputs to a Domain Name regulation plan to the Minister;

b. conduct supervision of Domain Name Registrars; and

c. settle Domain Name disputes.

(4) Further provisions on the settlement of Domain Name disputes as referred to in paragraph (3) sub-paragraph c shall be regulated by a Ministerial Regulation.

Article 82

(1) The Domain Name Registrars as referred to in Article 79 paragraph (3) sub-paragraph b shall implement the management of Indonesian second-level Domain Names and Indonesian derivative-level Domain Names.

(2) Domain Name Registrars shall consist of:

a. Agency Domain Name Registrars; and

b. Non-Agency Domain Name Registrars.

(3) Agency Domain Name Registrars shall implement the registration of Indonesian second-level Domain Names and Indonesian derivative-level Domain Names for the needs of Agency.

(4) The Agency Domain Name Registrars as referred to in paragraph (3) shall be implemented by the Minister.

(5) For military purposes, the Agency Domain Name Registrars as referred to in paragraph (3) shall be implemented by the minister organizing government affairs in the area of defense and security.

(6) Non-Agency Domain Name Registrars shall conduct the registration of Indonesian second-level Domain Names for commercial and non-commercial users.

(7) Non-Agency Domain Name Registrars shall be obligated to registered with the Minister.

Article 83

(1) The registration of Domain Names shall be implemented based on the first registrar principle.

(2) The registered Domain Names as referred to in paragraph (1) must fulfill the following requirements:

a. in accordance with the provisions of laws and regulations;

b. appropriateness applicable in the community; and

c. good faith.

(3) Domain Name Registries and Domain Name Registrars shall be authorized to:

a. reject the registration of Domain Names in the event that the Domain Names do not fulfill the requirements as referred to in paragraph (2);

b. temporarily deactivate the use of Domain Names; or

c. delete Domain Names in the event that Domain Name users violate the provisions of this Government Regulation.

Article 84

(1) Domain Name Registries and Domain Name Registrars shall be obligated to administer the management of Domain Names accountably.

(2) In the event that Domain Name Registries or Domain Name Registrars intend to terminate their management, the Domain Name Registries or Domain Name Registrars shall be obligated to delegate the entire management of Domain Names to the Minister by no later than 3 (three) months in advance.

Article 85

(1) Domain Names indicating an Agency may only be registered and/or used by the Agency concerned.

(2) An Agency must use Domain Names in accordance with the name of the Agency concerned.

Article 86

(1) Domain Name Registries and Domain Name Registrars shall receive the registration of Domain Names upon request of Domain Name Users.

(2) The Domain Name Users as referred to in paragraph (1) shall be responsible for the Domain Names registered by them.

Article 87

(1) Domain Name Registries and/or Domain Name Registrars shall be entitled to receive revenue by collecting fees for the registration and/or use of Domain Names from Domain Name Users.

(2) In the event that Domain Name Registries and Domain Name Registrars as referred to in paragraph (1) constitute Non-Agency Domain Name managers, the Domain Name Registries and Domain Name Registrars shall be obligated to pay part of revenue from the registration and use of Domain Names calculated from a revenue percentage to the state.

(3) The revenue as referred to in paragraph (1) and state revenue as referred to in paragraph (2) shall be non-tax state revenue.

Article 88

The supervision of Domain Name management shall be conducted by the Minister.

Article 89

Further provisions on the requirements and procedures for designation of Domain Name managers shall be regulated in a Ministerial Regulation.

CHAPTER VIII
ROLE OF THE GOVERNMENT

Article 90

The role of the Government in the administration of Electronic systems and Transactions shall include:

a. facilitating the utilization of Information Technology and Electronic Transactions in accordance with the provisions of laws and regulations;

b. protecting public interests from all types of disturbance as a result of misuse of Electronic Information and Electronic Transactions disturbing public order, in accordance with the provisions of laws and regulations;

c. conducting the prevention of dissemination and use of Electronic Information and/or Electronic Documents having prohibited contents in accordance with the provisions of laws and regulations; and

d. designating Agencies or institutions having strategic Electronic Data which must be protected.

Article 91

The role of the Government to facilitate the utilization of Information Technology and Electronic Transactions as referred to in Article 90 sub-article a shall include:

a. policy stipulation;

b. policy implementation;

c. infrastructure facilitation;

d. promotion and education; and

e. supervision.

Article 92

The infrastructure facilitation as referred to in Article 91 sub-article c shall include:

a. development and administration of national Electronic System portal;

b. development and administration of the forensic facilities of Information Technology;

c. parent electronic certification administration;

d. integrated administration of data center and national disaster recovery center in the context of electronic government affairs administration;

e. safeguard facilities of Electronic Systems for the prevention of attacks on vital information infrastructures in strategic sectors;

f. deposit or storage facilities of the source code and documentation of software for Agencies; and

g. other facilities required to facilitate the utilization of Information Technology and Electronic Transactions based on the provisions of laws and regulations.

Article 93

(1) The promotion and education as referred to in Article 91 sub-article d shall be implemented by an Agency in accordance with its authority based on the provisions of laws and regulations to realize safe, ethical, smart, creative, productive, and innovative utilization of Information Technology and Electronic Transactions.

(2) The implementation of promotion and education may involve stakeholders including the community and/or Information Technology and/or Electronic Transaction activists.

Article 94

(1) The role of the Government to protect public interests from all types of disturbance as a result of misuse of Electronic Information and Electronic Transactions disturbing public order as referred to in Article 90 sub-article b shall include:

a. stipulation of national cyber security strategy constituting part of the national security strategy, including the development of cyber security culture;

b. regulation of information security standard;

c. regulation of the administration of vital information infrastructure protection;

d. regulation of the risk management of Electronic System administration;

e. regulation of human resources in the administration of Electronic System protection;

f. development and supervision of the administration of vital information infrastructure protection;

g. development and supervision of the risk management of Electronic System administration;

h. development and supervision of human resources in the administration of Electronic System protection;

i. administration of Electronic Information safeguard;

j. administration of information security incident handling;

k. administration of emergency response handling; and

l. other functions required to protect public interests from all types of disturbance.

(2) The authority as referred to in paragraph (1) may be implemented in cooperation with other parties.

Article 95

The role of the Government to conduct the prevention of dissemination and use of Electronic Information and/or Electronic Documents having prohibited contents in accordance with the provisions of laws and regulations as referred to in Article 90 sub-article c shall be in the form of:

a. termination of Access; and/or

b. ordering Electronic System Administrators to conduct the termination of Access to the Electronic Information and/or Electronic Documents.

Article 96

The termination of Access shall be conducted on Electronic Information and/or Electronic Documents as referred to in Article 95 with the following classification:

a. violating the provisions of laws and regulations;

b. troubling the community and disturbing public order; and

c. informing the method or providing Access to Electronic Information and/or Electronic Documents having prohibited contents in accordance with the provisions of laws and regulations.

Article 97

(1) The community may submit an application for the termination of Access to Electronic Information and/or Electronic Documents as referred to in Article 96 to the Minister.

(2) The relevant Ministry or Institution shall coordinate with the Minister for the termination of Access to Electronic Information and/or Electronic Documents as referred to in Article 96.

(3) Law enforcement apparatuses may request the termination of Access to Electronic Information and/or Electronic Documents as referred to in Article 96 to the Minister.

(4) Judicial institutions may order the termination of Access to Electronic Information and/or Electronic Documents as referred to in Article 96 to the Minister.

(5) Provisions on the procedure for application for termination of Access as referred to in paragraph (1) up to paragraph (4) shall be regulated by a Ministerial Regulation.

Article 98

(1) Electronic System Administrators shall be obligated to make the termination of Access to Electronic Information and/or Electronic Documents as referred to in Article 96.

(2) The Electronic System Administrators as referred to in paragraph (1) shall include internet Access service providers, telecommunication network and service providers, content administrators, and link administrators providing the traffic network of Electronic Information and/or Electronic Documents.

(3) Electronic System Administrators which do not make the termination of Access may be subject to legal liabilities based on the provisions of laws and regulations.

(4) Further provisions on the implementation of obligation to terminate Access as referred to in paragraph (1) shall be regulated by a Ministerial Regulation.

Article 99

(1) The Government shall designate Agencies or institutions having strategic Electronic Data which must be protected.

(2) The Agencies or institutions having strategic Electronic Data which must be protected as referred to in paragraph (1), shall include:

a. government administration sector;

b. energy and mineral resources sector;

c. transportation sector;

d. financial sector;

e. health sector;

f. information and communication technology sector;

g. food sector;

h. defense sector; and

i. other sectors designated by the President.

(3) The Agencies or institutions having strategic Electronic Data as referred to in paragraph (1) must prepare Electronic Documents and their electronic backups as well as connect them to a certain data center for the purpose of data safeguard.

(4) Further provisions on the obligation to prepare Electronic Documents and their electronic backups as well as to connect them to a certain data center as referred to in paragraph (3) shall be regulated in a regulation of the head of institution in charge of cyber security affairs.

CHAPTER IX
ADMINISTRATIVE SANCTIONS

Article 100

(1) A violation of the provisions of Article 4, Article 5 paragraph (1) and paragraph (2), Article 6 paragraph (1), Article 9 paragraph (1) and paragraph (4), Article 14 paragraph (1) and paragraph (5), Article 15 paragraph (1), Article 17 paragraph (4), Article 18 paragraph (1), Article 21 paragraph (2) and paragraph (3), Article 22 paragraph (1), Article 23, Article 24 paragraph (1), paragraph (2), and paragraph (3), Article 25, Article 26 paragraph (1), Article 28 paragraph (1), Article 29, Article 30 paragraph (1), Article 31, Article 32 paragraph (1) and paragraph (2), Article 33, Article 34 paragraph (1), Article 37 paragraph (1) and paragraph (2), Article 38 paragraph (3), Article 39 paragraph (2), Article 40 paragraph (1) and paragraph (2), Article 42 paragraph (1) and paragraph (3), Article 51 paragraph (1), Article 53 paragraph (3), Article 55 paragraph (2), Article 63 paragraph (3), Article 64 paragraph (1), Article 69 paragraph (1), Article 82 paragraph (7), Article 84 paragraph (1) and paragraph (2), Article 87 paragraph (2), and Article 98 paragraph (1), shall be subject to administrative sanctions.

(2) The administrative sanctions as referred to in paragraph (1) may be in the form of:

a. written warning;

b. administrative fine;

c. temporary suspension;

d. termination of Access; and/or

e. delisting.

(3) Administrative sanctions shall be imposed by the Minister in accordance with the provisions of laws and regulations.

(4) The imposition of administrative sanctions as referred to in paragraph (2) sub-paragraph c and sub-paragraph d shall be made in coordination with the leader of the relevant Ministry or Institution.

(5) The imposition of administrative sanctions as referred to in paragraph (2) and paragraph (3) shall not nullify any criminal and civil responsibilities.

Article 101

Further provisions on the procedure for imposition of administrative sanctions and submission of objection to the imposition of administrative sanctions shall be regulated in a Ministerial Regulation.

CHAPTER X
TRANSITIONAL PROVISIONS

Article 102

(1) At the time this Government Regulation comes into effect, Electronic System Administrators which have been in operations prior to the promulgation of this Government Regulation, shall be obligated to adjust themselves with the provisions of Article 6 paragraph (1) within 1 (one) year.

(2) At the time this Government Regulation comes into effect, Public Scope Electronic System Administrators which have been in operations prior to the promulgation of this Government Regulation, shall be obligated to adjust themselves with the provisions of Article 20 paragraph (2) within 2 (two) years.

CHAPTER XI
CLOSING PROVISIONS

Article 103

(1) At the time this Government Regulation comes into effect, the implementing regulations of Government Regulation Number 82 Year 2012 regarding Administration of Electronic Systems and Transactions shall be declared remaining valid insofar as they do not contradict or have not been replaced by a new one based on this Government Regulation.

(2) At the time this Government Regulation comes into effect, Government Regulation Number 82 Year 2012 regarding the Operation 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) shall be revoked and declared null and void.

Article 104

This Government Regulation shall come into effect on the date of its promulgation.

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

Stipulated in Jakarta
On 4 October 2019
PRESIDENT OF THE REPUBLIC OF INDONESIA,
Signed
JOKO WIDODO

Promulgated in Jakarta,
On 10 October 2019
MINISTER OF LAW AND HUMAN RIGHTS
OF THE REPUBLIC OF INDONESIA,

Signed
TJAHJO KUMOLO

STATE GAZETTE OF THE REPUBLIC OF INDONESIA YEAR 2019 NUMBER 185
Issued as a true copy
MINISTRY OF STATE SECRETARIAT
OF THE REPUBLIC OF INDONESIA
Deputy of Legal Affairs and
Legislation,

Signed and stamped

Lydia Silvanna Djaman

ELUCIDATION
OF
GOVERNMENT REGULATION OF THE REPUBLIC OF INDONESIA
NUMBER 71 YEAR 2019
REGARDING
ADMINISTRATION OF ELECTRONIC SYSTEMS AND TRANSACTIONS

I. GENERAL

Some provisions of Law Number 11 Year 2008 regarding Electronic Information and Transactions mandate further regulation in a Government Regulation, namely regulation on Reliability Certification Body, Electronic Signature, Electronic Certification Administrator, Electronic System Administrator, Administration of Electronic Transactions, Electronic Agent administrator, and management of Domain Names have been regulated in Government Regulation Number 82 Year 2012 regarding Administration of Electronic Systems and Transactions. However, Government Regulation Number 82 Year 2012 regarding Administration of Electronic Systems and Transactions needs to be adjusted with the development of technology and public needs.

The stipulation of this Government Regulation is also intended to further regulate some provisions of Law Number 19 Year 2016 regarding the Amendment to Law Number 11 Year 2008 regarding Electronic Information and Transactions established to ensure the acknowledgement as well as respect for the rights and freedom of other persons and to fulfill fair demands in accordance with security and public order considerations in a democratic community. some provisions which require further regulation are, namely:

a. obligation for every Electronic System Administrator to delete irrelevant Electronic Information and/or Electronic Documents under its control upon a request of the Person concerned based on a judicial stipulation; and

b. the role of the Government in facilitating the utilization of Information Technology and Electronic Transactions, protecting public interests from all types of disturbance as a result of misuse of Electronic Information and Electronic Transactions disturbing public order, and prevent the dissemination and use of Electronic Information and/or Electronic Documents having prohibited contents in accordance with the provisions of laws and regulations.

The content materials of this Government Regulation include:

a. category of Electronic System Administrators;

b. obligations of Electronic System Administrators;

c. deletion and/or termination of Access to irrelevant Electronic Information and/or Electronic Documents;

d. placement of Electronic System and Electronic Data;

e. supervision of Electronic System administration;

f. administration of Electronic Agent;

g. Administration of Electronic Transactions;

h. administration of Electronic Certification;

i. management of Domain Names;

j. the role of the Government in the administration of Electronic Systems and Transactions; and

k. administrative sanctions.

II. ARTICLE BY ARTICLE

Article 1
Self-explanatory.

Article 2
Paragraph (1)
Self-explanatory.
Paragraph (2)
Self-explanatory.
Paragraph (3)
Sub-paragraph a
Self-explanatory.
Sub-paragraph b
"An institution appointed by an Agency" shall be an institution which implement the administration of public scope Electronic System in the name of the appointing Agency.
Paragraph (4)
"The regulatory and supervisory authorities of the financial sector" shall be among other things authorities in the monetary, payment system, macroprudential, banking, capital market, as well as insurance, pension fund, finance institution, and other financial service institution areas.
Paragraph (5)
Sub-paragraph a
Self-explanatory.
Sub-paragraph b

"Electronic System Administrators having an online portal, site, or application through the internet" shall be Electronic System Administrators the Electronic System of which is used in the territory of Indonesia, and/or is offered in the territory of Indonesia.

Sub-sub-paragraph 1

Self-explanatory.

Sub-sub-paragraph 2

Self-explanatory.

Sub-sub-paragraph 3

Self-explanatory.

Sub-sub-paragraph 4

Self-explanatory.

Sub-sub-paragraph 5

Self-explanatory.

Sub-sub-paragraph 6

Personal Data processing shall include the acquisition and collection, processing and analysis, correction and update, display, announcement, transfer, dissemination, or disclosure, and/or deletion or destruction of Personal Data.

Article 3

Paragraph (1)

"Reliable" shall be an Electronic System having capability in accordance with the needs of its use.

"Safe" shall be an Electronic System protected physically and non-physically.

"Proper operations of Electronic Systems" shall be an Electronic System having capability in accordance with its specifications.

Paragraph (2)

"Responsible" shall be Electronic System Administrators legally responsible for the administration of Electronic System.

Paragraph (3)

Self-explanatory.

Article 4

Self-explanatory.

Article 5

Self-explanatory.

Article 6

Self-explanatory.

Article 7

Paragraph (1)

Sub-paragraph a

"Interconnectivity" shall be capability to be interconnected thus being able to work properly. Interconnectivity shall include the capability of interoperability.

"Compatibility" shall be the compatibility of an Electronic System with another Electronic System.

Sub-paragraph b

Self-explanatory.

Sub-paragraph c

Self-explanatory.

Paragraph (2)

Certification evidence may be obtained through an accredited third party in Indonesia or other supporting evidence stating the fulfillment of requirements from a certification body outside Indonesia.

Article 8

Sub-paragraph a

"Ensure the security and reliability of proper operations" shall be Electronic System Administrators ensuring Software does not contain any other instructions than it should or unlawful hidden instructions (malicious code), such as time bomb instruction, virus program, trojan, worm, and backdoor. This safeguard may be conducted by examining the source code.

Sub-paragraph b

Self-explanatory.

Article 9

Paragraph (1)

"Source code" shall be a set of orders, statements, and/or declarations written in a computer programming language which can be read and understood by persons.

Paragraph (2)

Self-explanatory.

Paragraph (3)

"Source code escrow" shall be a profession or independent party which is competent in providing a computer program or Software source code escrow service for the purpose of source code access, acquisition, or handover by a provider to a user.

Paragraph (4)

Self-explanatory.

Paragraph (5)

Self-explanatory.

Paragraph (6)

Self-explanatory.

Article 10

Paragraph (1)

"Experts" shall be staff having special knowledge and skills in the area of Electronic System which can be academically and practically accounted for.

Paragraph (2)

Self-explanatory.

Article 11

Paragraph (1)

Sub-paragraph a

"Service level agreement" shall be a statement on the service quality level of an Electronic System.

Sub-paragraph b

Self-explanatory.

Sub-paragraph c

Self-explanatory.

Paragraph (2)

Self-explanatory.

Article 12

"Apply risk management" shall be conducting a risk analysis and formulating mitigation and management measures to overcome threats, disturbances, and obstacles to an Electronic System managed by them.

Article 13

"Governance policy" shall include among other things, policy on activities to develop an organization structure, business process, and performance management, as well as to provide personnel supporting the operations of Electronic System to ensure the Electronic System can operate properly.

Article 14

Paragraph (1)

Self-explanatory.

Paragraph (2)

Self-explanatory.

Paragraph (3)

"Valid approval" shall be an approval which is given explicitly, may not be implicit or based on mistake, negligence, or duress.

Paragraph (4)

Sub-paragraph a

Self-explanatory.

Sub-paragraph b

Self-explanatory.

Sub-paragraph c

"Vital interest" shall be the need/requirement to protect crucial matters regarding the existence of a person.

Sub-paragraph d

Self-explanatory.

Sub-paragraph e

Self-explanatory.

Sub-paragraph f

Self-explanatory.

Paragraph (5)

Self-explanatory.

Paragraph (6)

Self-explanatory.

Article 15

Paragraph (1)

Self-explanatory.

Paragraph (2)

Sub-paragraph a

Self-explanatory.

Sub-paragraph b

The obligation to delist from the search engine (right to delisting) shall include Electronic System Administrators running a search engine to remove the display and/or terminate Access to the irrelevant Electronic Information and/or Electronic Documents based on a judicial stipulation.

Paragraph (3)

Self-explanatory.

Article 16

Self-explanatory.

Article 17

Self-explanatory.

Article 18

Self-explanatory.

Article 19

Paragraph (1)

Good Electronic System governance (IT Governance) shall include the process of planning, implementation, operations, maintenance, and documentation.

Paragraph (2)

Self-explanatory.

Paragraph (3)

Self-explanatory.

Article 20

Paragraph (1)

"Business continuity plan" shall be a set of processes conducted to ensure continued activities in a condition of having a disturbance or disaster.

Paragraph (2)

Self-explanatory.

Paragraph (3)

Self-explanatory.

Paragraph (4)

Self-explanatory.

Paragraph (5)

Self-explanatory.

Paragraph (6)

Self-explanatory.

Paragraph (7)

Self-explanatory.

Article 21

Self-explanatory.

Article 22

Paragraph (1)

The audit trail mechanism shall include:

a. maintaining a transaction log in accordance with the data retention policy of the administrator, in accordance with the provisions of laws and regulations;

b. giving notification to consumers if a transaction has been successfully made;

c. ensuring the availability of audit trail function to be able to detect an attempt and/or occurrence of infiltration which must be reviewed or evaluated periodically; and

d. in the event that the processing and audit trail system is the responsibility of a third party, the audit trail process must be in accordance with the standard stipulated by Electronic System Administrators.

Paragraph (2)

"Other examination" shall be among other things examination for the purpose of emergency response (incident response) mitigation or management.

Article 23

Components of an Electronic System shall consist of:

a. Software;

b. Hardware;

c. experts;

d. Electronic System security system; and

e. governance of Electronic Systems.

Article 24

Paragraph (1)

"Disturbance" shall be every action which is destructive or having a serious impact on an Electronic System thus the Electronic System cannot work properly.

"Failure" shall be the stoppage of part or the entire essential function of Electronic System thus the Electronic System does not work properly.

"Loss" shall be an impact of damage to an Electronic System having a legal consequence for users, administrators, and other third parties both material and immaterial.

Paragraph (2)

"System of prevention and mitigation" shall be among other things anti-virus, anti spamming, firewall, intrusion detection, prevention system, and/or management of information security management system.

Paragraph (3)

Self-explanatory.

Paragraph (4)

Self-explanatory.

Article 25

Self-explanatory.

Article 26

Paragraph (1)

Self-explanatory.

Paragraph (2)

"Transferable Electronic Information and/or Electronic Documents" shall be commercial papers or electronic commercial papers.

"Electronic Information and/or Electronic Documents must be unique" shall be that the Electronic Information and/or Electronic Documents and/or recording of the Electronic Information and/or Electronic Documents constitute the only one representing a certain value.

"Electronic Information and/or Electronic Documents must explain possession" shall be that the Electronic Information and/or Electronic Documents must explain the characteristics of possession represented in a control system or recording system of the Electronic Information and/or Electronic Documents concerned.

"Electronic Information and/or Electronic Documents must explain their ownership" shall be that the Electronic Information and/or Electronic Documents must explain the characteristics of ownership represented by the existence of technology control facility which ensures that there is only a single authoritative copy and it does not change.

Article 27

"Interoperability" shall be the capability of different Electronic Systems to work in an integrated manner.

"Compatibility" shall be the compatibility of an Electronic System with another Electronic System.

Article 28

Paragraph (1)

Self-explanatory.

Paragraph (2)

Education which may be provided to Electronic System Users shall be among other things:

a. informing Electronic System Users the importance to maintain the security of Personal Identification Number (PIN)/password, for example:

   1. keeping confidential and not telling the PIN/password to anyone including to the officers of administrators;

   2. making periodic PIN/password changes;

   3. using a PIN/password which is not easily guessed such as the use of personal identity in the form of date of birth;

   4. not taking note of the PIN/password; and

   5. the PIN/password for one product should be different from the PIN/password of another product.

b. informing Electronic System Users various criminal methods of Electronic Transactions; and

c. informing Electronic System Users the procedures for filing claims.

Article 29

The obligation to inform Electronic System Users is intended to protect the interests of Electronic System Users.

Article 30

Paragraph (1)

The provision of features is intended to protect the rights and interests of Electronic System Users.

Paragraph (2)

Self-explanatory.

Article 31

Self-explanatory.

Article 32

Self-explanatory.

Article 33

Self-explanatory.

Article 34

Self-explanatory.

Article 35

Self-explanatory.

Article 36

Paragraph (1)

Self-explanatory.

Paragraph (2)

Self-explanatory.

Paragraph (3)

Self-explanatory.

Paragraph (4)

Sub-paragraph a

"Visual form" shall be a display which can be seen or read, among other things graphical display of a website.

Sub-paragraph b

"Audio form" shall be all things which can be heard, among other things telemarketing service.

Sub-paragraph c

"Electronic Data form" shall be such as electronic data capture (EDC), radio frequency identification (RFI), and barcode recognition.

Electronic data capture (EDC) shall be an Electronic Agent for and on behalf of an Electronic System Administrator cooperating with a network administrator. EDC may be used independently by a bank financial institution and/or jointly with other financial or non-financial institutions.

In the event that Electronic Transactions are made by using a card of Bank X on the EDC of Bank Y, Bank Y shall forward the transactions to Bank X, through the network administrator.

Sub-paragraph d

Self-explanatory.

Article 37

Paragraph (1)

Sub-paragraph a

Information on the identity of Electronic Agent administrators shall at least contain a logo or name indicating the identity.

Sub-paragraph b

Self-explanatory.

Sub-paragraph c

Self-explanatory.

Sub-paragraph d

Self-explanatory.

Sub-paragraph e

Self-explanatory.

Sub-paragraph f

Self-explanatory.

Sub-paragraph g

Self-explanatory.

Sub-paragraph h

Self-explanatory.

Paragraph (2)

Self-explanatory.

Paragraph (3)

Self-explanatory.

Paragraph (4)

Self-explanatory.

Article 38

Paragraph (1)

Self-explanatory.

Paragraph (2)

Self-explanatory.

Paragraph (3)

"Same treatment" shall be among other things the same rate, facility, requirement, and procedure treatment.

Paragraph (4)

Self-explanatory.

Article 39

Paragraph (1)

Self-explanatory.

Paragraph (2)

Self-explanatory.

Paragraph (3)

Sub-paragraph a

"Confidentiality" shall be in accordance with the legal concept of confidentiality of electronic information and communication.

Sub-paragraph b

"Integrity" shall be in accordance with the legal concept of integrity of Electronic Information.

Sub-paragraph c

"Availability" shall be in accordance with the legal concept of availability of Electronic Information.

Sub-paragraph d

"Authentication" shall be in accordance with the legal concept of authentication including originality of the content of Electronic Information.

Sub-paragraph e

"Authorization" shall be in accordance with the legal concept of authorization based on the scope of duty and function in an organization and management.

Sub-paragraph f

"Non-repudiation" shall be in accordance with the legal concept of non-repudiation.

Article 40

Paragraph (1)

Sub-paragraph a

In conducting an identity authentication testing and examining the authorization of Electronic

System Users, the following needs to be taken into account:

1. written policies and procedures to ensure the capability to test the authentication of identity and examine the authority of Electronic System Users;

2. method to test authentication; and

3. combination of not less than 2 (two)-factor authentication, namely "what you know" (PIN/password), "what you have" (magnetic card with a chip, token, digital signature), "what you are" or "biometric" (retina and fingerprint).

Sub-paragraph b

Self-explanatory.

Sub-paragraph c

Self-explanatory.

Sub-paragraph d

Protection of the confidentiality of Personal Data of Electronic System Users must also be fulfilled in the event that administrators use the service of other parties (outsourcing).

Sub-paragraph e

Self-explanatory.

Sub-paragraph f

Self-explanatory.

Sub-paragraph g

Procedure for handling unexpected incident must also be fulfilled in the event that administrators use the service of other parties (outsourcing).

Paragraph (2)

In preparing and stipulating the procedure to ensure Electronic Transactions thus they cannot be denied by consumers, the following must be taken into account:

a. the Electronic Transaction system has been designed to reduce the possibility of unintended transactions by authorized users;

b. the authentication or originality of all identities of the parties making transactions have been tested; and

c. financial transaction data is protected from the possibility of change and every change can be detected.

Article 41

Self-explanatory.

Article 42

Self-explanatory.

Article 43

Self-explanatory.

Article 44

Paragraph (1)

This provision shall be intended to protect Electronic System Users from the sending of disturbing Electronic Information (spam).

The forms of generally known spam shall be for example e-mail spam, instant message spam, usenet newsgroup spam, web search engine spam, blog spam, news spam on cellular phones, and Internet forum spam.

Paragraph (2)

Self-explanatory.

Article 45

Paragraph (1)

Self-explanatory.

Paragraph (2)

Sub-paragraph a

Self-explanatory.

Sub-paragraph b

Self-explanatory.

Sub-paragraph c

Self-explanatory.

Sub-paragraph d

Self-explanatory.

Sub-paragraph e

"Reasonableness" shall refer to the applicable element of appropriateness in accordance with the developing business custom or practice.

Article 46

Paragraph (1)

Electronic Transactions may include some forms or variants, among other things:

a. an agreement is not entered into electronically but the implementation of contractual relationship is settled electronically;

b. an agreement is entered into electronically and the implementation of contractual relationship is settled electronically; and

c. an agreement not entered into electronically and the implementation of contractual relationship is not settled electronically.

Paragraph (2)

Self-explanatory.

Article 47

Paragraph (1)

Self-explanatory.

Paragraph (2)

"Laws and regulations" shall be among other things the Law on Consumer Protection.

Paragraph (3)

Self-explanatory.

Article 48

Paragraph (1)

"Complete and correct information" shall include:

a. information containing the identity as well as status of legal subjects and their competence, either as producer, supplier, administrator or intermediary;

b. other information explaining certain matters which become conditions for the validity of agreement as well as explaining the offered goods and/or services, such as name, address, and description of goods/services.

"Contract" shall include an agreement or cooperation.

Paragraph (2)

Self-explanatory.

Paragraph (3)

Self-explanatory.

Paragraph (4)

Self-explanatory.

Paragraph (5)

Self-explanatory.

Article 49

Paragraph (1)

Self-explanatory.

Paragraph (2)

Electronic Transactions shall take place at the time of agreement between the parties which may be in the form of checking of data, identity, personal identification number/PIN or password.

Paragraph (3)

Sub-paragraph a

"Acceptance action stating an agreement" shall be among other things by clicking an electronic agreement by Electronic System Users.

Sub-paragraph b

Self-explanatory.

Article 50

Paragraph (1)

Self-explanatory.

Paragraph (2)

"Equally" shall be taking into account the interests of both parties fairly.

Article 51

Paragraph (1)

The obligation to use an Electronic Certificate shall apply to SSL Encryption.

Paragraph (2)

Self-explanatory.

Paragraph (3)

The ownership of Electronic Certificate shall be one of the endeavors to improve the security of administration of Electronic Systems in addition to other security endeavors.

The ownership of Electronic Certificate shall serve to support the security of administration of Electronic Systems including among other things confidentiality, authentication, integrity, and non-repudiation.

Paragraph (4)

Self-explanatory.

Paragraph (5)

Self-explanatory.

Paragraph (6)

The Ministerial Regulation shall contain among other things regulation on the procedure to submit an application for electronic certification delivered through Electronic Certification Administrators or registration authorities appointed by Electronic Certification Administrators.

Article 52

Sub-paragraph a

"Examination" shall be the examination of physical presence of certificate owner candidates, which can be conducted online electronically if the examination uses a biometric method.

Sub-paragraph b

An Electronic Signature shall be an approval to Electronic Information and/or Electronic Documents conducted by an individual person or individual person representing a Business Entity or Agency.

Article 53

Paragraph (1)

Sub-paragraph a

"Indonesia Electronic Certification Administrator" shall be an Electronic Certification Administrator which has certification so that supervision of its administration can be conducted as well as to become a differentiator that Indonesian Electronic Certification Administrator can be a trustworthy third party which becomes the guarantor of originality of electronic identity.

Sub-paragraph b

Self-explanatory.

Paragraph (2)

"One parent principle" shall be Indonesian Electronic Certification Administrators referring to a parent Electronic Certification Administrator administered by the Minister and the certificate of which is signed using the certificate of parent Electronic Certification Administrator.

Paragraph (3)

Self-explanatory.

Paragraph (4)

Self-explanatory.

Paragraph (5)

"Registered" shall not be registering as an Indonesian Business Entity but registering its company as a foreign Electronic Certification Administrator with the Minister.

Paragraph (6)

Self-explanatory.

Article 54

Self-explanatory.

Article 55

Self-explanatory.

Article 56

Self-explanatory.

Article 57

Paragraph (1)

Self-explanatory.

Paragraph (2)

Self-explanatory.

Paragraph (3)

Sub-paragraph a

An electronic seal shall be an Electronic Signature used by a Business Entity or Agency to ensure the originality and integrity of Electronic Information and/or Electronic Documents.

Sub-paragraph b

An electronic time stamp shall be a stamp which binds between time and date with Electronic Information and/or Electronic Documents by using a reliable method.

Sub-paragraph c

Electronic registered delivery service shall be a service which provides the delivery of Electronic Information and/or Electronic Documents and gives evidence related to the delivery of Electronic Information and/or Electronic Documents and protect the delivered Electronic Information and/or Electronic Documents from the risk of loss, theft, damage, or unauthorized change.

Sub-paragraph d

Website authentication shall be a service which identifies a website owner and relates the website to a Person or Business Entity which receives an Electronic Certificate of website by using a reliable method.

Sub-paragraph e

The preservation of Electronic Signature and/or electronic seal shall be a service which ensures that the legal force of Electronic Signature and electronic seal in Electronic Information and/or Electronic Documents can still be validated although the validity period of its Electronic Certificate has expired.

Article 58

Paragraph (1)

In the event that an Indonesian Electronic Certification Administrator cooperates with another Electronic Certification Administrator in the administration of part of its infrastructure or service, the occurring loss or negligence shall still be the responsibility of the Indonesian Electronic Certification Administrator.

Paragraph (2)

Self-explanatory.

Paragraph (3)

Self-explanatory.

Article 59

Self-explanatory.

Article 60

Paragraph (1)

Ab Electronic Signature shall serve as a manual signature in terms of representing the identity of Signatory.

The substantiation of originality (authentication) of manual signature can be conducted through verification or examination of Electronic Signature specimen of the Signatory.

In an Electronic Signature, Electronic Signature Making Data shall serve as an Electronic Signature specimen of the Signatory.

An Electronic Signature must be usable by competent experts to conduct examination and substantiation that the Electronic Information signed by the Electronic Signature does not undergone any changes after signing.

Paragraph (2)

Legal consequences of the use of certified or uncertified Electronic Signature shall influence the power of substantiation score.

Paragraph (3)

Self-explanatory.

Paragraph (4)

Self-explanatory.

Article 61

Paragraph (1)

"Unique" shall be that any code whatsoever used or utilized as Electronic Signature Making Data must refer only to one legal subject or one entity which represents one identity.

Paragraph (2)

Self-explanatory.

Paragraph (3)

Sub-paragraph a

Electronic Signature Making Data generated by a cryptographic technique generally has a probability-based mathematical correlation with Electronic Signature verification data. Therefore, the choice of cryptographic code to be used must consider the sufficiency of level of difficulty faced and resources which must be prepared by parties trying to forge Electronic Signature Making Data.

Sub-paragraph b

"Electronic media" shall be facilities, means, or devices used to collect, store, process, and/or disseminate Electronic Information used temporarily or permanently.

Sub-paragraph c

"Data related to the Signatory" shall be all data which is usable to identify the identity of the Signatory like name, address, place and date of birth, as well as manual signature specimen code.

"Trustworthy system" shall be a system which follows the Electronic Signature usage procedure which ensures the authenticity and integrity of Electronic Information. It can be seen by taking into account some factors, among other things:

1. finance and resources;

2. quality of Hardware and Software;

3. procedure for certificate and application as well as data retention;

4. availability of Electronic Signature Making Data; and

5. audit by an independent institution.

Sub-paragraph d

Self-explanatory.

Paragraph (4)

Self-explanatory.

Article 62

Paragraph (1)

Self-explanatory.

Paragraph (2)

Self-explanatory.

Paragraph (3)

Self-explanatory.

Paragraph (4)

Self-explanatory.

Paragraph (5)

Self-explanatory.

Paragraph (6)

The example of this provision shall be as follows:

a. A change of Electronic Signature after the time of signing must cause the Electronic Information to which it is embedded no longer works properly, damaged, or cannot be displayed if an Electronic Signature is embedded and/or is related to the signed Electronic Information. The technique for embedding and relating an Electronic Signature to the signed Electronic Information may cause the occurrence of the new Electronic Information or Electronic Document which:

1. seems like an inseparable unity; or

2. seems separated and the signed Electronic Information can be read by a layman while the Electronic Signature is in the form of code and/or drawing.

b. A change of Electronic Signature after the time of Signing must cause part or the entire Electronic Information invalid or inapplicable if the Electronic Signature is logically associated with the signed Electronic Information.
A change occurring to the signed Electronic Information must cause incompatibility between an Electronic Signature and the relevant Electronic Information which can be seen clearly through a verification mechanism.

Article 63

Self-explanatory.

Article 64

Paragraph (1)

Self-explanatory.

Paragraph (2)

The authentication factor which may be chosen to be combined can be differentiated in 3 (three) types, namely:

a. something owned individually (what you have), for example an ATM card or smart card;

b. something known individually (what you know), for example PIN/password or cryptographic key; and

c. something which constitutes the features/characteristics of an individual (what you are), for example voice pattern, handwriting dynamics, or fingerprint.

Paragraph (3)

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

Paragraph (1)

Self-explanatory.

Paragraph (2)

Self-explanatory.

Paragraph (3)

Self-explanatory.

Paragraph (4)

Sub-paragraph a

Self-explanatory.

Sub-paragraph b

"Address" shall at least explain a city of domicile in which a person or Business Entity is operating.

Sub-paragraph c

Self-explanatory.

Sub-paragraph d

Self-explanatory.

Sub-paragraph e

Self-explanatory.

Sub-paragraph f

Self-explanatory.

Paragraph (5)

Self-explanatory.

Paragraph (6)

Self-explanatory.

Article 72

Self-explanatory.

Article 73

Paragraph (1)

Self-explanatory.

Paragraph (2)

Self-explanatory.

Paragraph (3)

Self-explanatory.

Paragraph (4)

Sub-paragraph a

Information Technology consultant shall include the information security profession.

Sub-paragraph b

Self-explanatory.

Sub-paragraph c

Self-explanatory.

Paragraph (5)

Self-explanatory.

Paragraph (6)

Self-explanatory.

Article 74

Self-explanatory.

Article 75

Self-explanatory.

Article 76

Paragraph (1)

sub-paragraph a

Identity registration shall be a Reliability Certificate the reliability guarantee of which is limited to safeguard that the identity of Business Player is correct.

Validation conducted by a Reliability Certification Body shall be only to the identity of Business Player which at least contains the name of legal subject, status of legal subject, address or position, telephone number, email address, business permit, and Taxpayer Identification Number (TIN) if it is not yet registered in the Online Single Submission system.

A Reliability Certification Body which issues this Reliability Certificate shall give the certainty of tracking that the identity of Business Player is correct.

sub-paragraph b

The security of Electronic System shall be a Reliability Certificate the reliability guarantee of which gives a certainty that the security of data delivery or exchange process through the website of Business.

Player is protected by using a data exchange process safeguard technology such as SSL/secure socket layer protocol.
This Reliability Certificate shall ensure that there is a safeguard system in a tested data exchange process.

Safeguard of vulnerability (vulnerability seal) shall be a Reliability Certificate the reliability guarantee of which is to give certainty that there is an information security management system applied by a Business Player by referring to a certain Electronic System safeguard standard based on the provisions of laws and regulations.

sub-paragraph c

A privacy policy shall be a Reliability Certificate the reliability guarantee of which is to give a certainty that the confidentiality of consumer Personal Data is protected properly.

Paragraph (2)

Self-explanatory.

Paragraph (3)

Self-explanatory.

Article 77

Self-explanatory.

Article 78

Self-explanatory.

Article 79

Paragraph (1)

Self-explanatory.

Paragraph (2)

Sub-paragraph a

"Generic top-level Domain Name" shall be a top-level Domain Name consisting of three characters or more in the hierarchy of domain naming system in addition to country code Top-Level Domain. For example, ".nusantara" or ".java".

Sub-paragraph b

"Indonesian top-level Domain Name" shall be a top-level domain in the hierarchy of domain naming system indicating Indonesian code (.id) in accordance with the list of state codes in ISO 3166-1 used and acknowledged by the Internet Assigned Numbers Authority (IANA).

Sub-paragraph c

The examples of Indonesian secondary-level Domain Name shall be co.id, go.id, ac.id, or.id, or mil.id.

Sub-paragraph d

The example of Indonesian derivative-level Domain Name shall be kominfo.go.id.

Paragraph (3)

Sub-paragraph a

The function and role of ccTLD manager shall be included in the scope of definition of Domain Name Registry.

Sub-paragraph b

Self-explanatory.

Article 80

Self-explanatory.

Article 81

Self-explanatory.

Article 82

Self-explanatory.

Article 83

Self-explanatory.

Article 84

Self-explanatory.

Article 85

Self-explanatory.

Article 86

Self-explanatory.

Article 87

Self-explanatory.

Article 88

Self-explanatory.

Article 89

Self-explanatory.

Article 90

Self-explanatory.

Article 91

Self-explanatory.

Article 92

Sub-paragraph a

"National Electronic System portal" shall be among other things Indonesia National Single Window (INSW) and online single submission system.

Sub-paragraph b

Self-explanatory.

Sub-paragraph c

Self-explanatory.

Sub-paragraph d

The integrated administration of data center and national disaster recovery center shall be aimed at general application and strategic Electronic Data.

Sub-paragraph e

Self-explanatory.

Sub-paragraph f

Self-explanatory.

Sub-paragraph g

Self-explanatory.

Article 93

Self-explanatory.

Article 94

Self-explanatory.

Article 95

Self-explanatory.

Article 96

Sub-paragraph a

"Violating the provisions of laws and regulations" shall be among other things Electronic Information and/or Electronic Documents containing the elements of pornography, gambling, slander and/or defamation, fraud, hatred towards an ethnic, religion, race, and inter-group relation (SARA), violence and/or child violence, violence of intellectual property, violence of goods and services e-commerce, terrorism and/or radicalism, separatism and/or banned hazardous organization, violation of information security, violation of consumer protection, violation in the health sector, violation of drug and food control.

Sub-paragraph b

"troubling the community and disturbing public order" shall be among other things forged information and/or facts.

Sub-paragraph c

Self-explanatory.

Article 97

Self-explanatory.

Article 98

Paragraph (1)

"Termination of Access" shall be among other things blocking of Access, termination of account, and/or deletion of content.

Paragraph (2)

Self-explanatory.

Paragraph (3)

Self-explanatory.

Paragraph (4)

Self-explanatory.

Article 99

Paragraph (1)

"Agency or institution having strategic Electronic Data" shall be an Agency or institution having vital information infrastructure in the stipulated sector.

Paragraph (2)

Self-explanatory.

Paragraph (3)

Linkage to a certain data center for the purpose of data safeguard shall be implemented in the context of occurrence of incident which must be reported to an institution in charge of cyber security.

Paragraph (4)

Self-explanatory.

Article 100

Paragraph (1)

Imposition of sanctions in this provision shall be only aimed at parties committing an administrative violation, meanwhile a moral or civil violation shall not be subject to an administrative sanction.

Paragraph (2)

Sub-paragraph a

Self-explanatory.

Sub-paragraph b

Self-explanatory.

Sub-paragraph c

"Temporary suspension" shall be in the form of suspension of part or all of the components or services in the Electronic System concerned for a certain period.

Sub-paragraph d

"Termination of Access" shall be among other things blocking of Access, termination of account, and/or deletion of content.

Sub-paragraph e

Self-explanatory.

Paragraph (3)

Self-explanatory.

Paragraph (4)

Self-explanatory.

Paragraph (5)

Self-explanatory.

Article 101

Self-explanatory.

Article 102

Self-explanatory.

Article 103

Self-explanatory.

Article 104

Self-explanatory.

SUPPLEMENT TO THE STATE GAZETTE OF THE REPUBLIC OF INDONESIA NUMBER 6400

NOTE

Source: LOOSE LEAF OF THE STATE SECRETARIATE YEAR 2019