PERATURAN PEMERINTAH REPUBLIK INDONESIA

NOMOR 71 TAHUN 2019

TENTANG

PENYELENGGARAAN SISTEM DAN TRANSAKSI ELEKTRONIK

REGULATION OF THE GOVERNMENT OF THE REPUBLIC OF INDONESIA

NUMBER 71 OF 2019

ON

ELECTRONIC SYSTEM AND TRANSACTION OPERATIONS

MINISTRY OF COMMUNICATIONS AND INFORMATICS
DIRECTORATE GENERAL OF INFORMATICS APPLICATIONS
Towards The Indonesian Information Society

FOREWORD

Praise and gratitude be to the One Almighty God for His Mercy and Grace, the process of translating Government Regulation Number 71 of 2019 (GR Number 71 of 2019) on Electronic System and Transaction Operations has been completed.

Along with the development of information and communication technology, countries in the world are increasingly connected and interdependent. The laws and regulations of a country are not only part of the interests of that country but also the interest of other relevant countries because they can affect, among others, trade, investment, cooperation between countries, and the position of the said country in many international fora.

GR Number 71 of 2019 was promulgated on 10 October 2019 and revoked Government Regulation Number 82 of 2012 because the latter is no longer relevant with the development of legal needs in society. In addition, GR Number 71 of 2019 was established to encourage digital economic growth and enforce Indonesia's sovereignty over electronic information in Indonesian territory. The regulation is in line with the government's vision to build a productive, independent, and competitive economic structure. GR Number 71 of 2019 contains various important provisions in electronic system and transaction operations which include electronic system registration, electronic data processing inside or outside the territory of Indonesia, protection of personal data, and electronic signatures. These provisions have become an interest of stakeholders of both Indonesia and its partner countries.

Language is a means of communication. The translation of GR Number 71 of 2019 from Indonesian Language into English is intended to provide far-reaching information about the provisions to the international stakeholders. Although this translation is not an official translation of the Indonesian government, it is expected

that business actors, governments, academics, and practitioners of partner countries can better understand GR Number 71 of 2019 comprehensively by reading its translation.

The translation process of GR Number 71 of 2019 was carried out by the Translation Team of the Ministry of Communication and Informatics, which includes Filmon Leonard Warouw, Penni Patmawati Rusman, Siti Chodijah, Erik Limantara, and Josua Sitompul and was supported by the active roles of Astrid Wirajuda, Sakurayuki, Michelle Virgiani, and Vik Tang of Hiswara Bunjamin & Tandjung Law Firm as well as colleagues from the Legal and Cooperation Division of the Secretariat of the Directorate General of Informatics Applications. The Directorate General of Informatics Applications hereby extends its gratitude to the translators and deeply appreciates the translation result.

Users of this translation are welcome to send constructive input, suggestions, or criticism via email to *hkaptika@kominfo.go.id.* to make it more accurate, legible and reasonable.

Jakarta, 27 October 2020
Director General of Informatics Applications


Ditandatangani secara elektronik oleh
Direktur Jenderal Aplikasi Informatika

Semuel Abrijani Pangerapan

REGULATION OF THE GOVERNMENT OF THE REPUBLIC OF INDONESIA

NUMBER 71 OF 2019

ON

ELECTRONIC SYSTEM AND TRANSACTION OPERATIONS

BY THE BLESSINGS OF THE ALMIGHTY GOD

PRESIDENT OF THE REPUBLIC OF INDONESIA,

Considering :

a. that with the highly rapid development of information technology for purposes of promoting growth of the digital economy and upholding state sovereignty over electronic information within the territory of the Unitary State of the Republic of Indonesia, it is necessary to regulate the utilization of information technology and electronic transactions in a comprehensive manner;

b. that Government Regulation Number 82 of 2012 on Electronic System and Transaction Operations is no longer relevant with the development of legal needs of the public and therefore, it needs to be superseded;

c. that based on the consideration as referred to in letter a and letter b, it is necessary to issue a Government Regulation on Electronic System and Transaction Operations;

Observing :

1. Article 5 section (2) of the 1945 Constitution of the Republic of Indonesia; and
2. Law Number 11 of 2008 on 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 of 2016 on Amendment to Law Number 11 of 2008 on 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 establish : GOVERNMENT REGULATION ON ELECTRONIC SYSTEM AND TRANSACTION OPERATIONS.

CHAPTER I
GENERAL PROVISIONS

Article 1

In this Government Regulation:

1. Electronic System means a set of electronic equipment and procedures which have the function to prepare, collect, process, analyze, store, display, announce, deliver and/or disseminate Electronic Information.
2. Electronic Transaction means any legal acts carried out through the use of computers, computer networks and/or other electronic media.
3. Electronic Agent means equipment in an Electronic System made to initiate an automated act on certain Electronic Information, as operated by a Person.
4. Electronic System Operators mean any Persons, state administrators, Business Entities and the public that provide, manage and/or operate an Electronic System individually or jointly to Electronic System Users for its own interests and/or the interests of another party.
5. Public Electronic System Operator means an Electronic System operation by a State Administrator Agency or institutions appointed by a State Administrator Agency.
6. Private Electronic System Operator means an Electronic System Operation by a Person, Business Entity and the public.
7. Ministry or Agency means the State Administrator Agency which has the duties of supervising and issuing regulations in its sector.

8. Electronic Information means one or a collection of Electronic Data, including but not limited to texts, sounds, images, maps, designs, photographs, electronic data interchange (EDI), electronic mails, telegrams, telexes, telecopies or the like, letters, signs, numbers, Access codes, symbols or perforations which have been processed that carry meaning or may be understood by persons qualified to understand them.

9. Electronic Document means any Electronic Information created, forwarded, delivered, received, or stored in analog, digital, electromagnetic, optical forms, or the like, which may be seen, displayed, and/or heard through a computer or an Electronic System, including but not limited to texts, sounds, images, maps, designs, photographs or the like, letters, signs, numbers, Access codes, symbols or perforations that have purport or meaning or may be understood by persons qualified to understand them.

10. Information Technology means any techniques for the collecting, preparing, storing, processing, announcing, analyzing, and/or disseminating information.

11. Electronic System User means any Persons, state administrators, Business Entities and the public which utilize goods, services, facilities, or information provided by Electronic System Operators.

12. Hardware means one or a series of devices connected in an Electronic System.

13. Software means one or a set of computer programs, procedures, and/or related documentation in the operation of an Electronic System.

14. Electronic System Propriety Test means a series of objective assessment processes for each component of an Electronic System, carried out either independently and/or by an authorized and competent institution.

15. Access means any activities of interacting with an Electronic System that is a standalone or forms part of a network.

16. Electronic Transaction Operation means a set of Electronic Transaction activities carried out by Senders and Receivers using an Electronic System.

17. Electronic Contract means an agreement entered into by parties through an Electronic System.

18. Sender means a legal subject which deliver Electronic Information and/or Electronic Documents.

19. Receiver means a legal subject which receive Electronic Information and/or Electronic Documents from a Sender.

20. Electronic Certificates mean certificates which are electronic in nature and contain Electronic Signatures and identities indicating the legal subject statuses of parties to Electronic Transactions, as issued by Certification Authorities.

21. Certification Authory means a legal entity that function as a trustworthy party, which issue and audit Electronic Certificates.

22. Electronic Signature means a signatures comprising Electronic Information attached to, associated with, or related to other Electronic Information, which is used as a verification and authentication tool.

23. Signatory means a legal subject associated with or related to an Electronic Signature.

24. Electronic Signature Creation Equipment means Software or Hardware that is configured and used to generate Electronic Signatures.

25. Electronic Signature Creation Data means personal codes, biometric codes, cryptographic codes, and/or codes generated from the conversion of manual signatures into Electronic

Signatures, including another code generated from developments in Information Technology.

26. Trustmark Certification Provider means an independent agency established by professionals which is recognized, authorized, and supervised by the Government and has the authority to audit and issue Trustmarks in Electronic Transactions.

27. Trustmark means a document attesting that a Business Actor operating Electronic Transactions have passed audits or conformity tests held by a Trustmark Certification Provider.

28. Business Actor means any persons or Business Entities, whether in legal entity or non-legal entity form, which are established and domiciled or engage in activities within the jurisdiction of the Republic of Indonesia, whether individually or collectively, through an agreement on the operation of business activities in various sectors of the economy.

29. Personal Data means any data about a person which is identified and/or is identifiable either separately or when combined with other information, either directly or indirectly through an Electronic System and/or non-electronic system.

30. Electronic Data means data in electronic form that is not limited to texts, sounds, images, maps, designs, photographs, electronic data interchange (EDI), electronic mails, telegrams, telexes, telecopies or the like, letters, signs, numbers, Access codes, symbols, or perforations.

31. Domain Name means an internet address of any state administrator, Person, Business Entity, and/or the public, which may be used in communicating through the internet and is in the form of codes or unique character arrangements to indicate certain locations on the internet.

32. Domain Name Registry means an operator responsible for managing, operating, and maintaining a Domain Name Electronic System.

33. Domain Name Registrar means a Person, Business Entity, or the public that provide Domain Name registration services.

34. Domain Name User means a Person, State Administrator Agency, Business Entity, or the public which has applied for registration to use Domain Names to Domain Name Registrars.

35. State Administrator Agency, hereinafter referred to as Agency, is a legislative, executive, and judicial institution at the central and regional levels and such other agencies established under laws and regulations.

36. Person means a person, whether an Indonesian citizen, foreign citizen, or legal entity.

37. Business Entity means a sole proprietorship or partnership company, whether in legal entity or non-legal entity form.

38. Government means the Minister or other officials appointed by the President.

39. Minister means the minister overseeing government affairs in the field of communications and informatics.

CHAPTER II
ELECTRONIC SYSTEM OPERATIONS

Part One
General

Article 2

(1) An Electronic System Operation is carried out by an Electronic System Operator.

(2) The Electronic System Operator as referred to in section (1) includes:
   a. Public Electronic System Operators; and
   b. Private Electronic System Operators.

(3) Public Electronic System Operators include:
   a. Agencies; and
   b. institutions appointed by Agencies.

(4) The Public Electronic System Operators as referred to in section (2) letter a do not include Public Electronic System Operators that are authorities regulating and supervising the financial sector.

(5) Private Electronic System Operators as referred to in section (2) letter b include:
   a. An Electronic System Operator regulated or supervised by Ministries or Agencies in accordance with the provisions of laws and regulations; and
   b. An Electronic System Operator which has an online portal, site, or online application through the internet, which is used to:
      1. provide, manage, and/or operate offers of and/or trade in goods and/or services;
      2. provide, manage, and/or operate financial transaction services;
      3. deliver paid digital materials or contents through a data network, either by way of downloading through a portal or site, delivery through electronic mail, or through another application tot he user's device;
      4. provide, manage, and/or operate communication services, including but not limited to short messages, voice calls, video calls, electronic mails, and online chats in the forms of digital platforms, networking and social media services;
      5. manage search engine services, provide Electronic Information in the forms of text, sound, image,

animation, music, video, film, and games or a combination of any and/or all of the foregoing; and/or

6. process Personal Data for the operational activities of providing services to the public relating to Electronic Transaction activities.

Article 3

(1) Any Electronic System Operator shall operate the Electronic System in a reliable and secure manner and be responsible for the due operations of the Electronic System.

(2) An Electronic System Operator is responsible for the operation of its Electronic System.

(3) The provision as referred to in section (2) does not apply in the event that a force majeure, fault, and/or negligence of Electronic System Users may be proven.

Article 4

To the extent not stipulated otherwise by a separate law, any Electronic System Operators must operate Electronic System that fulfil the following minimum requirements:

a. be able to re-display Electronic Information and/or Electronic Documents in full in accordance with the retention period determined under the laws and regulations;

b. be able to protect the availability, integrity, authenticity, confidentiality, and accessibility of the Electronic Information in the Electronic System operation;

c. be able to operate in accordance with procedures for or instructions on an Electronic System operation;

d. be equipped with procedures or instructions which are announced in languages, information, or symbols

understandable to the relevant parties to the Electronic System operation; and

e. provide a continuous mechanism to maintain the currency, clarity, and accountability of the procedures or instructions.

Article 5

(1) An Electronic System Operator must ensure its Electronic Systems do not contain any Electronic Information and/or Electronic Documents that are prohibited in accordance with the provisions of laws and regulations.

(2) An Electronic System Operator must ensure that its Electronic Systems do not facilitate the distribution of any Electronic Information and/or Electronic Documents that are prohibited in accordance with the provisions of laws and regulations.

(3) Provisions regarding the obligations of Electronic System Operators as referred to in section (1) and section (2) are regulated by a Ministerial Regulation.

Part Two
Electronic System Registration

Article 6

(1) Any Electronic System Operators as referred to in Article 2 section (2) must apply for registration.

(2) The obligation of an Electronic System Operator to apply for registration is satisfied prior to the commencement of use of the said Electronic System by Electronic System Users.

(3) The registration of Electronic System Operators as referred to in section (1) is submitted to the Minister through an electronically integrated business licensing service in accordance with the provisions of laws and regulations.

(4) Further provisions regarding the registration of Electronic System Operators as referred to in section (3) refer to norms, standards, procedures, and criteria which are regulated by a Ministerial Regulation.

Part Three
Hardware

Article 7

(1) Hardware used by an Electronic System Operator shall:
   a. fulfil the aspects of security, interconnectivity, and compatibility with the systems used;
   b. have technical support, maintenance, and/or after sales services from sellers or providers; and
   c. have service continuity guarantee.

(2) Fulfillment of the requirements as referred to in section (1) shall be demonstrated by certifications or other similar evidence.

Part Four
Software

Article 8

Software used by an Electronic System Operator shall:
a. have its operational security and reliability duly guaranteed; and
b. have its service continuity guaranteed.

Article 9

(1) A developer who provides Software specifically developed for a Public Electronic System Operator must deliver the source codes of and documentation on the Software to the relevant Agencies or institutions.

(2) The relevant Agencies or institutions as referred to in section (1) must store the source codes and documentation of the Software in facilities in accordance with the provisions of laws and regulations.

(3) In the event the facilities as referred to in section (2) are not yet available, the Agencies or institutions may store the source codes of and documentation on the Software with a trusted source code escrow.

(4) A developer must guarantee the procurement of and/or Access to the source codes of and documentation on the Software to the trusted third party as referred to in section (3).

(5) A Public Electronic System Operator must guarantee the confidentiality of Software source code used and to use it only for the interest of a Public Electronic System Operator.

(6) Further provisions regarding the obligation to deliver the source codes of and documentation on Software to the Agencies or institutions as referred to in section (1) and the storage of the said source code and documentation with a trusted third party as referred to in section (3) are regulated by a Ministerial Regulation.

Part Five
Experts

Article 10

(1) An expert consulted by Electronic System Operators shall have competence in the field of Electronic System or Information Technology.

(2) The expert as referred to in section (1) must comply with the provisions of laws and regulations.

Part Six
Electronic System Governance

Article 11

(1) An Electronic System Operator shall guarantee:
   a. the availability of service level agreements;
   b. the availability of information security agreements for the Information Technology services used; and
   c. the security of information and internal communication facilities being operated.

(2) The Electronic System Operator as referred to in section (1) shall guarantee that each component and integration of the entire Electronic System is duly operated.

Article 12

An Electronic System Operator shall apply risk management to any damages or losses incurred.

Article 13

An Electronic System Operator shall have governance policies, operational work procedures, and audit mechanisms implemented periodically on its Electronic Systems.

Article 14

(1) An Electronic System Operator must implement the principles of Personal Data protection in processing Personal Data, which include that:
   a. Personal Data collection is carried out in a limited and specific, legally valid and fair manner, with the acknowledgement and consent of the Personal Data subject;

b. Personal Data processing is carried out in accordance with its purpose;
c. Personal Data processing is carried out by guaranteeing the rights of the Personal Data subject;
d. Personal Data processing is carried out in an accurate, complete, not misleading, up to date and accountable manner and by observing the purpose of Personal Data processing;
e. Personal Data processing is carried out by protecting Personal Data security from any losses, misuses, unauthorized Accesses and disclosures, as well as any alterations of or destructions of Personal Data;
f. Personal Data processing is carried out by notifying collection purpose, processing activities and failure of protection of Personal Data; and
g. Processed Personal Data is destructed and/or erased, unless it is within the retention period in accordance with needs based on the provisions of laws and regulations.

(2) The Personal Data processing as referred to in section (1) includes:
a. procurement and collection;
b. processing and analysis;
c. storage;
d. correction and updating;
e. display, announcement, transfer, dissemination, or disclosure; and / or
f. erasure or destruction.

(3) Personal Data processing shall fulfill the requirement of obtaining valid consent from a Personal Data subject for 1 (one) or several certain purposes that have been informed to the said Personal Data subject.

(4) In addition to the consent as referred to in section (3), Personal Data processing shall meet the requirements needed to:

a. fulfil obligations under an agreement to which a Personal Data subject is a party or to fulfil a request of the Personal Data subject upon entering into an agreement;
b. fulfil legal obligations of Personal Data controllers in accordance with the provisions of laws and regulations;
c. protect the vital interest of the Personal Data subject;
d. exercise of the authorities of Personal Data controllers based on the provisions of laws and regulations;
e. fulfil obligations of Personal Data controllers in public services for public interest; and/or
f. fulfil other legitimate interests of Personal Data controllers and/or Personal Data subjects.

(5) In the event of failure in the protection of Personal Data being managed, an Electronic System Operator must notify the said Personal Data subject in writing.

(6) Provisions regarding the processing techniques of Personal Data are regulated in accordance with the provisions of laws and regulations.

Article 15

(1) Any Electronic System Operators must erase irrelevant Electronic Information and/or Electronic Documents under its control at the request of the person concerned.

(2) The obligation to erase the irrelevant Electronic Information and/or Electronic Documents as referred to in section (1) comprises:
a. erasure (right to erasure); and
b. removal from search engine listing (right to delisting).

(3) The Electronic System Operator that must erase the Electronic Information and/or Electronic Documents as referred to in section (1) is an Electronic System Operator that has obtained and/or processed Personal Data under its control.

Article 16

(1) The irrelevant Electronic Information and/or Electronic Documents which are erased (in accordance with the right to erasure) as referred to in Article 15 section (2) letter a comprise Personal Data:
   a. obtained and processed without the consent of a Personal Data subject;
   b. in respect of which consent has been withdrawn by the Personal Data subject;
   c. obtained and processed in an unlawful manner;
   d. which is no longer relevant to the purpose for which it was procured based on agreements and/or provisions of the laws and regulations;
   e. which use has exceeded the period in accordance with agreements and/or provisions of the laws and regulations; and/or
   f. displayed by the Electronic System Operator resulting in losses to a Personal Data subject.

(2) The obligation to erase Electronic Information and/or Electronic Documents as referred to in section (1) does not apply in the event the said Electronic Information and/or Electronic Documents are required to be stored or are prohibited from being erased by the Electronic System Operator in accordance with the provisions of laws and regulations.

Article 17

(1) The erasure of irrelevant Electronic Information and/or Electronic Documents by way of removal from search engine listing (in accordance with the right to delisting) as referred to in Article 15 section (2) letter b is carried out based on a court order.

(2) An application for order on the erasure of Electronic Information and/or Electronic Documents to a local district court is made by the person concerned as a Personal Data subject in accordance with the provisions of laws and regulations.

(3) The application for order on the erasure as referred to in section (2) shall contain:
   a. identity of the applicant;
   b. identity of the Electronic System Operator and/or address of the Electronic System;
   c. irrelevant Personal Data under the control of the Electronic System Operators; and
   d. the reason for the request for erasure.

(4) In the event the court approves the application for order on the erasure as referred to in section (2), the Electronic System Operator must erase the irrelevant Electronic Information and/or Electronic Documents.

(5) The court order as referred to in section (4) serves as the basis for the request for erasure of irrelevant Electronic Information and/or Electronic Documents by the person concerned to the Electronic System Operator.

Article 18

(1) Any Electronic System Operators must provide a mechanism for the erasure of Electronic Information and/or Electronic Documents which are no longer relevant in accordance with the provisions of laws and regulations.

(2) The mechanism for erasure as referred to in section (1) at least contains provisions on:
   a. The providing of communication channels between Electronic System Operator and Personal Data subject;

b. feature for erasure of irrelevant Electronic Information and/or Electronic Documents that allows a Personal Data subject to erase their Personal Data; and
c. recording of requests for erasure of irrelevant Electronic Information and/or Electronic Documents.

(3) Further provisions regarding the erasure mechanism as referred to in section (1) and section (2) are regulated by a Ministerial Regulation.

(4) Provisions concerning the erasure mechanism in certain sectors may be established by relevant Ministries or Agencies upon coordinating with the Minister.

Article 19

(1) An Electronic System Operator shall implement good and accountable Electronic System governance.

(2) The governance as referred to in section (1) at least fulfils the following requirements:
a. availability of procedures for or instructions on Electronic System operations that are documented and/or announced using languages, information, or symbols which are understood by parties relevant to the said Electronic System operation;
b. a sustainable mechanism being in place to maintain currency and clarity of implementation procedural guidelines;
c. agencies and complete supporting personnel being in place for due operation of the Electronic Systems;
d. performance management being applied in relation to the operated Electronic System to ensure due operation of the Electronic System; and
e. plans being in place to maintain the continuity of operations of the Electronic System under their management.

(3) In addition to the requirements as referred to in section (2), relevant Ministries or Agencies may determine other requirements as stipulated under the laws and regulations.

Article 20

(1) A Public Electronic System Operator must have business continuity plan to cope with disruptions or disasters in accordance with risks arising from consequences thereof.

(2) A Public Electronic System Operator must carry out management, processing, and/or storage of an Electronic System and Electronic Data within the territory of Indonesia.

(3) A Public Electronic System Operator may carry out the management, processing, and/or storage of an Electronic System and Electronic Data outside the territory of Indonesia in the event the relevant storage technology is not available in Indonesia.

(4) The criterion of storage technology which are not available in Indonesia as referred to in section (3) is determined by a committee comprising the ministry undertaking government affairs in the field of communications and informatics, the institution in charge of technology assessment and application affairs, the agency in charge of cyber security and related Ministries or Agencies.

(5) Formation of the committee as referred to in section (4) is determined by the Minister.

(6) In the event a Public Electronic System Operator uses third party services, it must classify data according to risks incurred.

(7) Further provisions regarding the data classification according to risks as referred to in section (6) are regulated by a Ministerial Regulation.

Article 21

(1) A Private Electronic System Operator may carry out management, processing, and/or storage of an Electronic System and Electronic Data within the territory of Indonesia and/or outside the territory of Indonesia.

(2) In the event the management, processing, and/or storage of the Electronic System and Electronic Data are carried out outside the territory of Indonesia, the Private Electronic System Operator must ensure the effectiveness of supervision by the Ministry or Agencies and of law enforcement.

(3) A Private Electronic System Operator must provide Access to the Electronic System and Electronic Data for supervision and law enforcement purposes in accordance with the provisions of laws and regulations.

(4) Provisions regarding the management, processing, and storage of an Electronic System and Electronic Data for a Private Electronic System Operator in the financial sector are further regulated by financial sector regulating and supervising authorities.

Part Seven
Securing of Electronic System Operations

Article 22

(1) An Electronic System Operator must provide an audit trail of all Electronic System operation activities.

(2) The audit trail as referred to in section (1) is used for the purposes of supervision, law enforcement, dispute resolution, verification, testing, and other examinations.

Article 23

An Electronic System Operator must secure components of its Electronic System.

Article 24

(1) An Electronic System Operator must have and run procedures and facilities for securing its Electronic Systems in order to avoid any disruptions, failures and losses.

(2) An Electronic System Operators must provide a security system that covers procedures and systems for the prevention and overcoming of threats and attacks that result in any disruptions, failures, and losses.

(3) In the occurrence of a system failure or disruption that has brought about serious impact on an Electronic System as a result of actions of another party, the Electronic System Operators must secure Electronic Information and/or Electronic Documents and immediately report at the first opportunity to law enforcement officials and related Ministries or Agencies.

(4) Further provisions regarding the security system as referred to in section (2) are regulated by a regulation of the head of the agency undertaking government affairs in the field of cyber security.

Article 25

An Electronic System Operator must re-display Electronic Information and/or Electronic Documents in full in accordance with the format and retention period stipulated under laws and regulations.

Article 26

(1) An Electronic System Operator must maintain the confidentiality, integrity, authenticity, accessibility, availability, and traceability of Electronic Information and/or Electronic Documents in accordance with the provisions of laws and regulations.

(2) In the operation of an Electronic System intended for transferable Electronic Information and/or Electronic Documents, Electronic Information and/or Electronic Documents shall be unique and explain their control and ownership.

Article 27

An Electronic System Operator shall guarantee the functionality of the Electronic System in accordance with their purposes, with due observance of their interoperability and compatibility with previous and/or related Electronic System.

Article 28

(1) An Electronic System Operator must provide Electronic Systems Users with education.

(2) The education as referred to in section (1) at least covers the rights, obligations, and responsibilities of all related parties as well as procedures for the filing of complaints.

Article 29

An Electronic System Operator must deliver information to Electronic System Users on at least the following:
a. identity of Electronic System Operators;
b. object being transacted;

c. Electronic Systems propriety or security;
d. equipment use procedures;
e. contract conditions;
f. procedures for the reaching of agreement;
g. guarantee of privacy and/or Personal Data protection; and
h. telephone number of complaint center.

Article 30

(1) An Electronic System Operator must provide features compatible with characteristics of the Electronic Systems used.

(2) The features as referred to in section (1) are at least in the form of facilities to:
   a. make corrections;
   b. cancel instructions;
   c. provide confirmations or re-confirmations;
   d. choose whether to continue or discontinue subsequent activities;
   e. view information provided in the form of Electronic Contracts or advertisement offers;
   f. check the successful or failed status of Electronic Transactions; and
   g. read agreements prior to carrying out Electronic Transactions.

Article 31

An Electronic System Operator must protect users and the public from losses incurred by the Electronic System which it operates.

Article 32

(1) Any persons working in an environment where an Electronic System is operated must secure and protect Electronic System facilities and infrastructure or information channeled through the Electronic System.

(2) An Electronic System Operator must provide, educate, and train personnel who are in charge of and responsible for the security and protection of Electronic System facilities and infrastructure.

Article 33

For criminal justice process purposes, an Electronic System Operator must provide Electronic Information and/or Electronic Data contained in its Electronic System or Electronic Information and/or Electronic Data produced by its Electronic System upon a valid request from investigators for certain criminal offences in accordance with the authorities regulated by the provisions of laws and regulations.

Part Eight
Electronic System Propriety Test

Article 34

(1) An Electronic System Operator must perform an Electronic System Propriety Test.

(2) The obligation as referred to in section (1) may be implemented on all or parts of components of the Electronic System in accordance with characteristics of protection required and strategic nature of the Electronic System operation.

Part Nine
Supervision

Article 35

(1) The Minister has the authority to exercise supervision over an Electronic System operation.

(2) The supervision as referred to in section (1) covers monitoring, control, inspection, tracking, and securing.

(3) Provisions on supervision over an Electronic System operation in certain sectors must be made by the relevant Ministries or Agencies upon coordinating with the Minister.

CHAPTER III
ELECTRONIC AGENT OPERATORS

Part One
Electronic Agent

Article 36

(1) An Electronic System Operator may operate Electronic System on its own or through an Electronic Agent.

(2) The Electronic Agent as referred to in section (1) forms a part of the Electronic System.

(3) Obligations of an Electronic System Operator apply mutatis mutandis to an Electronic Agent operator.

(4) An Electronic Agent may be in:
a. visual;
b. audio;
c. Electronic Data; and
d. other forms.

Article 37

(1) An Electronic Agent Operator must provide or convey information to protect rights of users of the Electronic Agent it operates, which at least includes:
   a. identity of the Electronic Agent operator;
   b. object being transacted;
   c. propriety or security of the Electronic Agent;
   d. equipment use procedures;
   e. contract conditions;
   f. procedures for the reaching of agreement;
   g. guarantee of privacy and/or Personal Data protection; and
   h. telephone number of complaint center.

(2) The Electronic Agent Operator must accommodate or provide features to protect rights of users on the Electronic Agent it operates in accordance with characteristics of the Electronic Agent used.

(3) The features as referred to in section (2) are in the form of facilities to:
   a. make corrections;
   b. cancel instructions;
   c. provide confirmations or re-confirmations;
   d. choose whether to continue or discontinue subsequent activities;
   e. view information provided in the form of Electronic Contracts or advertisement offers;
   f. check successful or failed status of transactions; and/or
   g. read the agreement prior to carrying out transactions.

(4) An Electronic Agent Operator shall provide features on the Electronic Agent it operates allowing its users to edit information that is still in the the process of being transacted.

Article 38

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

(2) The agreement as referred to in section (1) shall contain at least:
   a. rights and obligations;
   b. responsibilities;
   c. complaint and dispute resolution mechanisms;
   d. time period;
   e. costs;
   f. scope of service; and
   g. choice of law.

(3) In the event an Electronic Agent is operated for more than 1 (one) interest of an Electronic System Operator, the Electronic Agent operator must provide equal treatment to Electronic System Operator using the said Electronic Agent.

(4) In the event an Electronic Agent is operated for the interest of more than 1 (one) Electronic System Operator, the Electronic Agent operator is deemed to be a separate Electronic System Operator.

Part Two
Obligations

Article 39

(1) In operating an Electronic Agent, an Electronic Agent operator shall consider the principles of:
   a. prudence;
   b. security and integration of Information Technology system;
   c. security control over Electronic Transaction activities;
   d. cost effectiveness and efficiency; and

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

(2) An Electronic Agent Operator must establish and run standard operating procedures that fulfil the principles of security control of user and Electronic Transaction data.

(3) The principles of security control of user and Electronic Transaction data as referred to in section (2) include:
a. confidentiality;
b. integrity;
c. availability;
d. authenticity;
e. authorization; and
f. non-repudiation.

Article 40

(1) An Electronic Agent Operator must:
a. authenticate identities and validate authorizations of Electronic System Users entering into Electronic Transactions;
b. establish and implement policies and procedures for taking action if any indication of data theft is found;
c. ensure control over authorization and Access rights to Electronic Transaction system, databases, and applications;
d. formulate and implement methods and procedures for protecting and/or keeping confidential data integrity, records, and information related to Electronic Transactions;
e. establish and implement standards and controls over data use and protection in the event service providers have Access to the said data;
f. have business sustainability plans, including effective contingency plans to ensure the continued availability of Electronic Transaction system and services; and

g. have procedures for the quick and accurate handling of unexpected occurrences to mitigate the impact of an Electronic System incident, fraud, and failure.

(2) An Electronic Agent Operator must formulate and stipulate procedures for ensuring that Electronic Transactions may not be disclaimed by consumers.

CHAPTER IV
ELECTRONIC TRANSACTION OPERATIONS

Part One
Scope of Electronic Transaction Operations

Article 41

(1) An Electronic Transaction Operation may be carried out within both public and private scopes.

(2) Public Electronic Transaction Operations include Electronic Transaction Operations by:
a. Agencies;
b. institutions appointed by Agencies;
c. inter-Agencies;
d. inter-institutions appointed;
e. between Agencies and institutions appointed; and
f. between Agencies or institutions and Business Actors in accordance with the provisions of laws and regulations.

(3) Private Electronic Transaction Operations include Electronic Transactions:
a. between Business Actors;
b. between Business Actors and consumers; and
c. between individuals.

Part Two
Requirements for Electronic Transaction Operations

Article 42

(1) An Electronic Transaction Operation must use Electronic Certificate issued by an Indonesian Certification Authority.

(2) An Electronic Transaction Operation may use Trustmark.

(3) In the event that a Trustmark as referred to in section (2) is used, an Electronic Transaction Operation must use a Trustmark issued by a registered Trustmark Certification Provider.

Article 43

An Electronic Transaction Operation carried out by a Public Electronic System Operator shall observe security, reliability and efficiency aspects.

Article 44

(1) A sender must ensure that the delivered Electronic Information is correct and unsolicited in nature.

(2) Further provisions regarding the delivery of Electronic Information are regulated by a Ministerial Regulation.

Part Three
Requirements of Electronic Transactions

Article 45

(1) An Electronic Transaction entered into by parties has legal effect on the said parties.

(2) An Electronic Transaction Operation undertaken by the parties shall consider:
   a. good faith;
   b. prudence;
   c. transparency;
   d. accountability; and
   e. reasonableness.

Article 46

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

(2) An Electronic Contract is deemed valid if:
   a. an agreement is reached between the parties;
   b. it is entered into by a competent legal subject or their authorised representatives in accordance with the provisions of laws and regulations;
   c. there is a specific matter; and
   d. object of the transaction does not contravene the laws and regulations, good morals, and public order.

Article 47

(1) An Electronic Contract and other contractual forms as referred to in Article 46 section (1) which are aimed at Indonesian residents shall be made in the Indonesian language.

(2) An Electronic Contract entered into with standard clauses shall comply with the provisions on standard clauses as stipulated under the laws and regulations.

(3) An Electronic Contract contains at least:
   a. data on identities of the parties;
   b. objects and specifications;

c. Electronic Transaction requirements;
d. prices and costs;
e. procedures in the event of cancellation by the parties;
f. provisions granting rights to an injured party allowing it to return the goods and/or to request for a product replacement if any hidden defects are found; and
g. choice of law for the completion of Electronic Transactions.

Article 48

(1) A Business Actor offering products through an Electronic System shall provide complete and correct information in relation to contract conditions, manufacturers, and the products offered.

(2) A Business Actor must provide clear information on contract or advertisement offers.

(3) A Business Actor must provide consumers and/or contract recipients with the deadline to return goods delivered and/or services provided in the event they are not in accordance with the contract or any hidden defects are found.

(4) A Business Actor must deliver information on the goods delivered and/or services provided.

(5) A Business Actor is prohibited from imposing an obligation on consumers to pay for goods delivered and/or services provided without any contract as basis.

Article 49

(1) An Electronic Transaction occurs when an agreement between the parties is reached.

(2) Unless otherwise agreed by the parties, the agreement as referred to in section (1) occurs when a transaction offer sent by a Sender has been received and approved by a Recipient.

(3) The agreement as referred to in section (2) may be made through:
   a. an act of acceptance stating approval; or
   b. an act of acceptance and/or use of the object by an Electronic System User.

Article 50

(1) In an Electronic Transaction Operation, the parties shall guarantee:
   a. provision of correct data and information; and
   b. availability of facilities and services as well as complaint settlement.

(2) In an Electronic Transaction Operation, the parties shall determine a proportionate choice of law for the implementation of Electronic Transactions.

CHAPTER V
ELECTRONIC CERTIFICATION OPERATIONS

Part One
Electronic Certificates

Article 51

(1) The Electronic System Operator as referred to in Article 2 section (2) must have an Electronic Certificate.

(2) Electronic System Users may use Electronic Certificates in Electronic Transactions.

(3) In order to obtain Electronic Certificates, Electronic System Operators and Electronic System Users shall submit an application to an Indonesian Certification Authority.

(4) If required, Ministries or Agencies may oblige Electronic System Users to use Electronic Certificates in Electronic Transactions.

(5) Further provisions on the use of Electronic Certificates as referred to in section (4) are regulated by the Ministries or Agencies.

(6) Further provisions on procedures for obtaining Electronic Certificates are regulated by a Ministerial Regulation.

Part Two
Certification Authorities

Article 52

A Certification Authority is authorized to:

a. examine prospective owners and/or holders of Electronic Certificates, issue Electronic Certificates, extend validity period of Electronic Certificates, suspend and revoke Electronic Certificates, validate Electronic Certificates, and create lists of active and revoked Electronic Certificates; and

b. make, verify, and validate Electronic Signatures and/or other services using Electronic Certificates.

Article 53

(1) Certification Authorities comprise:
   a. Indonesian Certification Authorities; and
   b. foreign Certification Authorities.

(2) Indonesian electronic certification operations adhere to the one-root principle.

(3) An Indonesian Certification Authority must obtain a recognition from the Minister under the Root Certification Authority implemented by the Minister.

(4) An Indonesian Certification Authority shall obtain an assessment from an accredited Certification Authority.

(5) A Foreign Certification Authority operating in Indonesia shall be registered in Indonesia.

(6) Further provisions on the registration of foreign Certification Operators as referred to in section (5) are regulated by a Ministerial Regulation.

Article 54

(1) The recognition of an Indonesian Certification Authority as referred to in Article 53 section (3) is granted by the Minister upon the Indonesian Certification Authority fulfiling the requirements for the recognition process as regulated by a Ministerial Regulation.

(2) A list of recognized Indonesian Certification Authorities, including the services they provide, is made, maintained, and published by the Minister.

(3) Further provisions on procedures for recognizing Indonesian Certification Authorities are regulated by a Ministerial Regulation.

Article 55

(1) An Indonesian Certification Authority is entitled to receive fee revenues by collecting service fees from Electronic Certificate users.

(2) An Indonesian Certification Authority must deposit any revenues from service fees for the use of Electronic Certificates, to be calculated from a percentage of revenues, to the state.

(3) The revenues as referred to in section (1) and section (2) are non-tax state income.

Part Three
Supervision

Article 56

(1) The Minister conducts supervision on:
    a. Indonesian electronic certification operations; and
    b. foreign Certification Authorities.

(2) The supervision on Indonesian electronic certification operations as referred to in section (1) letter a includes:
    a. recognition; and
    b. operations of the facilities of the Root Certification Authority for Indonesian Certification Authorities.

(3) Further provisions on the supervision on Indonesian electronic certification operations and foreign Certification Authorities are regulated by a Ministerial Regulation.

Part Four
Services of Certification Authorites

Paragraph 1
General Provisions

Article 57

(1) An Indonesian Certification Authority provides certified services.

(2) The services as referred to in section (1) include:
    a. Electronic Signatures; and/or
    b. other services using Electronic Certificates.

(3) The other services as referred to in section (2) letter b include:
    a. electronic seals;
    b. electronic time stamps;

c. registered electronic delivery services;
d. website authentication; and/or
e. preservation of Electronic Signatures and/or electronic seals.

Article 58

(1) An Indonesian Certification Authority is liable for losses resulting from any willful misconduct or negligence towards any Person, Business Entity or Agency due to its failure to comply with its obligations as regulated by this Government Regulation.

(2) An Indonesian Certification Authority is deemed to be willful or negligent unless it is able to prove that losses have been incurred not due to its willful misconduct or negligence.

(3) The liability to provide evidence of the willful misconduct or negligence committed by a party other than an Indonesian Electronic Certification Authority rests with the Person, Business Entity or Agency who has suffered the losses.

Paragraph 2
Electronic Signatures

Article 59

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

(2) In the event an Electronic Signature is used to represent a Business Entity, the said Electronic Signature is referred to as an electronic seal.

(3) The Electronic Signature as referred to in section (1) and section (2) has valid legal force and effect to the extent it fulfils the following requirements:

a. Electronic Signature Creation Data is associated only with a Signatory;
b. Electronic Signature Creation Data during the electronic signing process is only within the control of the Signatory;
c. any changes to the Electronic Signature occurring after the time of signing may be known;
d. any changes to Electronic Information relating to the Electronic Signature after the time of signing may be known;
e. necessary methods are utilized to identify the Signatory; and
f. necessary methods are in place to show that the Signatory has granted its approval for the relevant Electronic Information.

Article 60

(1) An Electronic Signature functions as an authentication and verification tool on:
   a. the identity of a Signatory; and
   b. the integrity and authenticity of Electronic Information.

(2) Electronic Signatures include:
   a. Certified Electronic Signatures; and
   b. Uncertified Electronic Signatures.

(3) The Certified Electronic Signatures as referred to in section (2) letter a shall:
   a. fulfil the validity of legal force and legal effect of Electronic Signatures as referred to in Article 59 section (3);
   b. use Electronic Certificates created by using the services Indonesian Certification Authorities; and
   c. be made using certified Electronic Signature Creation Equipment.

(4) The uncertified Electronic Signatures as referred to in section (2) letter b are made without using the services of an Indonesian Certification Authority.

Paragraph 3
Electronic Signature Creation Data

Article 61

(1) An Electronic Signature Creation Data shall uniquely associate only to a Signatory and may be used to identify a Signatory.

(2) The Electronic Signature Creation Data as referred to in section (1) may be made by a Certification Authority.

(3) The Electronic Signature Creation Data as referred to in section (1) and section (2) shall fulfil the following requirements:
   a. if cryptographic codes are used, an Electronic Signature Creation Data shall be not easily identifiable from Electronic Signature verification data through certain calculations, over a certain time period, and with reasonable instruments;
   b. Electronic Signature Creation Data is stored in an electronic media under the control of the Signatory; and
   c. data relating to the Signatory must be stored in a data storage place or facility which uses a reliable system owned by a Certification Authority that is able to detect any changes and fulfil the following requirements:
      1. only an authorized person is able to enter new data, as well as change, exchange or replace data;
      2. the authenticity of information on the identity of the Signatory may be examined; and
      3. other technical changes violating security requirements may be detected or known by the Certification Authority.

d. if any Electronic Signature Creation Data is made by a Certification Authority, the entire process of creation of Electronic Signature Creation Data is guaranteed in terms of its safety and confidentiality by the Certification Authority.

(4) A Signatory shall keep the confidentiality of and be responsible for Electronic Signature Creation Data.

Article 62

(1) In a signing process, a mechanism shall be implemented to ensure that the Electronic Signature verification data relating to the Electronic Signature Creation Data remains valid or is not revoked.

(2) In the signing process, a mechanism shall be implemented to ensure that the Electronic Signature Creation Data:
a. is not reported missing;
b. is not reported to have been transferred to any unauthorized persons; and
c. is under the control of the Signatory.

(3) Before a signing is performed, the Electronic Information to be signed shall be known and understood by the Signatory.

(4) Approval of the Signatory for Electronic Information to be signed with an Electronic Signature shall apply an affirmation mechanism and/or such other mechanism which indicates the intent and purpose of the Signatory in being bound to an Electronic Transaction.

(5) An Electronic Signature on Electronic Information at least:
a. is made using Electronic Signature Creation Data; and
b. indicates the time of the signing.

(6) Any changes to the Electronic Signature and/or signed Electronic Information made after the time of the signing

shall be identified, detected, or recognized through certain methods or procedures.

Article 63

(1) A Signatory may entrust its Electronic Signature Creation Data to a Certification Authority.

(2) The Electronic Signature Creation Data as referred to in section (1) may be entrusted only to an Indonesian Certification Authority.

(3) In the event a Certification Authority stores Electronic Signature Creation Data, the Certification Authority must:
   a. ensure that the use of the Electronic Signature Creation Data is solely under the control of the Signatory;
   b. use a certified Electronic Signature Creation Equipment in the process of storing Electronic Signature Creation Data; and
   c. ensure that the adopted mechanism for the use of Electronic Signature Creation Data for Electronic Signatures applies at least a combination of 2 (two) authentication factors.

(4) Provisions on the Certified Electronic Signature Creation Equipment as referred to in section (3) letter b are established by a Ministerial Regulation.

Article 64

(1) Prior to the use of an Electronic Signature, a Certification Authority must ensure initial identification of a Signatory through the following ways:
   a. the Signatory submits its identity to the Certification Authority;
   b. the Signatory carries out registration with the Certification Authority; and

c. if necessary, the Certification Authority may confidentially delegate identity data of the Signatory to other Certification Authorities with the approval of the Signatory.

(2) The mechanism for using Electronic Signature Creation Data for Electronic Signatures applies a combination of at least 2 (two) authentication factors.

(3) The process of verification of signed Electronic Information may be carried out by examining Electronic Signature verification data to trace any changes to the signed data.

Paragraph 4
Electronic Seals

Article 65

The regulations on Electronic Signatures apply mutatis mutandis to electronic seal regulations.

Paragraph 5
Electronic Time Stamps

Article 6**6**

Electronic time stamp services comprise:
a. certified electronic time stamp services; and
b. uncertified electronic time stamp services.

Article 67

(1) A certified electronic time stamp shall fulfil the following requirements:
   a. binding the date and time on Electronic Information and/or Electronic Documents to prevent the possibility of Electronic Information and/or Electronic Documents being changed undetected;

b. referring to an accurate source of time related to coordinated universal time;
c. using an Electronic Certificate made by an Indonesian Certification Authority; and
d. being signed using an Electronic Signature or electronic seal operated by an Indonesian Certification Authority or using an equivalent method.

(2) A certified electronic time stamp shall provide:
a. accurate date and time; and
b. integrity of Electronic Information and/or Electronic Documents related to the said date and time.

(3) Uncertified electronic time stamp services are provided without using the services of an Indonesian Certification Authority.

(4) Further provisions regarding certified electronic time stamps are regulated by a Ministerial Regulation.

Paragraph 6
Electronic Registered Delivery Services

Article 68

Electronic registered delivery services comprise:
a. certified electronic registered delivery services; and
b. uncertified electronic registered delivery services.

Article 69

(1) A Certified Certification Authority that provides certified electronic registered delivery services must guarantee:
a. integrity of delivered data;
b. Data Senders are identifiable;
c. Data Recipients are identifiable; and
d. accuracy of date and time of data deliveries and receipts.

(2) The certified electronic registered delivery services as referred to in section (1) shall fulfil at least the following requirements:
   a. operated by 1 (one) or more Indonesian Certification Authorities;
   b. Senders may be accurately identified;
   c. Recipients' addresses may be identified prior to data deliveries;
   d. deliveries and receipts of data are secured by Electronic Signatures and electronic seals from an Indonesian Certification Authority;
   e. any changes to data in the process of data deliveries or receipts may be known to the Senders and the Recipients; and
   f. time and date of deliveries, receipts, and change of data may be displayed with certified electronic time stamps.

(3) If a data delivery involves 2 (two) or more Indonesian Certification Authorities, all requirements as referred to in section (2) apply to all Indonesian Certification Authorities involved.

(4) Uncertified electronic registered delivery services are made without using the services of an Indonesian Certification Authority.

(5) Further provisions regarding electronic registered delivery services are regulated by a Ministerial Regulation.

Paragraph 7
Website Authentications

Article 70

Website authentications comprise:
a. certified website authentications; and
b. uncertified website authentications.

Article 71

(1) A Certification Authority that provides website authentication services shall have a reliable method that is able to identify Persons or Business Entities that are responsible for operating websites which use website authentication services.

(2) A website authentication aims to guarantee trust in electronic transactions through websites.

(3) A certified website authentication shall use an Electronic Certificate issued by an Indonesian Certification Authority.

(4) Information that shall be contained in an Electronic Certificate used for website authentication includes, but is not limited to:
   a. names of Persons, Business Entities, or Agencies operating the website;
   b. addresses of Persons, Business Entities, or Agencies that at least explain the cities of domicile of the said Persons, Business Entities, or Agencies;
   c. Domain Names operated by website operators;
   d. validity periods of the Electronic Certificates;
   e. identities of Certification Authorities issuing Electronic Certificates; and
   f. Electronic Certificate numbers.

(5) An uncertified website authentication is made without using the services of an Indonesian Certification Authority.

(6) Further provisions regarding the certified website authentication as referred to in section (3) are regulated by a Ministerial Regulation.

Paragraph 8
Preservation of Electronic Signatures and/or Electronic Seals

Article 72

(1) Preservations of Electronic Signatures and/or electronic seals comprise:
    a. preservations of certified Electronic Signatures and/or electronic seals; and
    b. preservations of uncertified Electronic Signatures and/or electronic seals.
(2) The preservations of certified Electronic Signatures and/or electronic seals shall meet the following requirements:
    a. use an Electronic Certificate made through the services of an Indonesian Certification Authority; and
    b. the Certified Electronic Signature and/or electronic seal contained in Electronic Information and/or Electronic Documents may still be validated despite the Electronic Certificates having already expired.
(3) The preservations of uncertified Electronic Signatures and/or electronic seals are made without using the services of an Indonesian Certification Authority.
(4) Further provisions regarding the preservations of certified Electronic Signatures and/or electronic seals are regulated by a Ministerial Regulation.

CHAPTER VI
TRUSTMARK CERTIFICATION PROVIDERS

Article 73

(1) A Business Actor that carries out Electronic Transactions may be certified by a Trustmark Certification Provider.

(2) A Trustmark Certification Provider shall have its domicile in Indonesia.

(3) A Trustmark Certification Provider is established by professionals.

(4) The professionals which establish the Trustmark Certification Provider as referred to in section (3) include at least the following professions:
   a. Information Technology consultants;
   b. Information Technology auditors; and
   c. legal consultants in the field of Information Technology.

(5) A Trustmark Certification Provider shall be registered in a list of Trustmark Certification Providers issued by the Minister.

(6) Further provisions regarding the requirements for establishing Trustmark Certification Providers are regulated by a Ministerial Regulation.

Article 74

(1) A Trustmark is intended to protect consumers in Electronic Transactions.

(2) The Trustmark as referred to in section (1) constitutes a guarantee that a Business Actor has fulfiled the criteria determined by the Trustmark Certification Provider.

(3) A Business Actor which has fulfiled the criteria as referred to in section (2) is entitled to use the Trustmark on its pages and/or other Electronic Systems.

Article 75

(1) A Trustmark Certification Provider may issue a Trustmark through a Trustmark Certification process.

(2) The Trustmark Certification process as referred to in section (1) covers an examination on complete and correct information from a Business Actor and its Electronic System.

(3) The complete and correct information as referred to in section (2) includes but is not limited to information that:
   a. contains the identity of the Business Actor;
   b. contains policies and procedures for privacy protection;
   c. contains policies and procedures for system security; and
   d. contains a statement of guarantee on goods and/or services offered.

Article 76

(1) A Trustmark issued by a Trustmark Certification Provider includes the following categories:
   a. identity registration;
   b. Electronic System security; and
   c. privacy policies.

(2) Compliance with the categorization as referred to in section (1) determines the level of the Trustmark.

(3) Further provisions regulating Trustmark levels as referred to in section (2) are regulated by a Ministerial Regulation.

Article 77

Supervision of Trustmark Certification Providers is carried out by Minister.

Article 78

(1) To obtain recognition, a Trustmark Certification Provider is subject to an administrative fee.

(2) Any revenues from the administrative fee as referred to in section (1) constitute non-tax state income.

CHAPTER VII
DOMAIN NAME MANAGEMENT

Article 79

(1) Domain Name management is operated by Domain Name managers.

(2) Domain Names comprise:
   a. generic top-level Domain Names;
   b. the Indonesian top-level Domain Name;
   c. second-level Indonesian Domain Names; and
   d. lower-level Indonesian Domain Names.

(3) The Domain Name managers as referred to in section (1) comprise:
   a. The Domain Name Registry; and
   b. Domain Name Registrars.

Article 80

(1) The Domain Name managers as referred to in Article 79 section (3) may be assumed by the Government and/or the public.

(2) The public as referred to in section (1) shall be in the form of an Indonesian legal entity.

(3) A Domain Name manager is determined by the Minister.

Article 81

(1) The Domain Name Registry as referred to in Article 79 section (3) letter a carry out the management of top-level generic Domain Names and the Indonesian top-level Domain Name.

(2) The Domain Name Registry may grant authority on registrations of generic top-level Domain Names and the Indonesian top-level Domain Name to Domain Name Registrars.

(3) The Domain Name Registry has the following functions:
   a. providing inputs on plans to regulate Domain Names to the Minister;
   b. carrying out supervision of Domain Name Registrars; and
   c. resolving Domain Name disputes.

(4) Further provisions regarding the resolution of Domain Name disputes as referred to in section (3) letter c are regulated by a Ministerial Regulation.

Article 82

(1) A Domain Name Registrar as referred to in Article 79 section (3) letter b carries out the management of second-level Indonesian Domain Names and lower-level Indonesian Domain Names.

(2) Domain Name Registrars comprise:
   a. Agency Domain Name Registrars; and
   b. Non-Agency Domain Name Registrars.

(3) The Agency Domain Name Registrars carry out the registrations of second-level Indonesian Domain Names and lower-level Indonesian Domain Names for the needs of Agencies.

(4) The Agency Domain Name Registrar as referred to in section (3) is assumed by the Minister.

(5) For military purposes, the Agency Domain Name Registrar as referred to in section (3) is assumed by a minister who undertakes government affairs in the fields of defense and security.

(6) Non-Agency Domain Name Registrars carry out registrations of second-level Indonesian Domain Names for commercial and non-commercial users.

(7) Non-Agency Domain Name Registrars must be registered with the Minister.

Article 83

(1) Domain Name registrations are carried out based on the first registrant principle.

(2) The Registered Domain Name as referred to in section (1) shall fulfil the following requirements:
   a. be in accordance with the provisions of laws and regulations;
   b. be in line with the public's propriety standards; and
   c. be in good faith.

(3) The Domain Name Registry and Domain Name Registrars have the authority to:
   a. deny Domain Name registrations if a Domain Name fails to fulfil the requirements as referred to in section (2);
   b. temporarily deactivate the use of a Domain Name; or
   c. erase a Domain Name if the Domain Name user violates the provisions of this Government Regulation.

Article 84

(1) The Domain Name Registry and Domain Name Registrars must manage Domain Names in an accountable manner.

(2) In the event the Domain Name Registry or a Domain Name Registrar intends to terminate its management, the Domain Name Registry or the Domain Name Registrar must hand over the entire Domain Name management to the Minister not later than 3 (three) months beforehand.

Article 85

(1) A Domain Name indicating an Agency may only be registered and/or used by the relevant Agency.

(2) An Agency shall use a Domain Name which is consistent with its name.

Article 86

(1) The Domain Name Registry and Domain Name Registrars accept Domain Name registrations based on applications of Domain Name Users.

(2) The Domain Name Users as referred to in section (1) are responsible for the Domain Names they register.

Article 87

(1) The Domain Name Registry and/or Domain Name Registrars are entitled to receive revenues by imposing Domain Name registration and/or usage fees on Domain Name Users.

(2) In the event the Domain Name Registry and Domain Name Registrars as referred to in section (1) are Non-Agency Domain Name managers, the Domain Name Registry and the Domain Name Registrars must deposit to the state part of their revenues from the registrations and use of Domain Names, to be calculated from a percentage of revenues.

(3) The revenues as referred to in section (1) and the state revenues as referred to in section (2) constitute non-tax state income.

Article 88

Supervision of Domain Name management is carried out by the Minister.

Article 89

Further provisions regarding requirements and procedures for the determination of Domain Name managers are regulated by a Ministerial Regulation.

CHAPTER VIII
ROLES OF THE GOVERNMENT

Article 90

Roles of the Government in the operations of Electronic Systems and Transactions include:

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

b. protecting the public interest from all types of disturbances resulting from the misuse of Electronic Information and Electronic Transactions that disturb public order, in accordance with the provisions of laws and regulations;

c. preventing the distribution and use of Electronic Information and/or Electronic Documents that contain any prohibited contents in accordance with the provisions of laws and regulations; and

d. determining the Agencies or institutions that have strategic Electronic Data which must be protected.

Article 91

The roles of the Government in facilitating the utilization of Information Technology and Electronic Transactions as referred to in Article 90 letter a include:

a. policy stipulation;
b. policy implementation;
c. infrastructure facilitation;
d. promotion and education; and
e. supervision.

Article 92

Infrastructure facilitation as referred to in Article 91 letter c includes:

a. development and operation of a national Electronic System gateway;

b. development and operation of Information Technology forensic facilities;

c. operation of root electronic certification;

d. operation of national data centers and disaster recovery centers in an integrated manner for the undertaking of electronic-based government affairs;

e. means of securing Electronic Systems to prevent attacks on vital information infrastructure in strategic sectors;

f. facilities for the depositing or storing of source codes of and documentation on the software of Agencies; and

g. other means required to facilitate the utilization of Information Technology and Electronic Transactions in accordance with the provisions of laws and regulations.

Article 93

(1) The promotion and education as referred to in Article 91 letter d are carried out by an Agency in accordance with its authorities based on the provisions of laws and regulations in order to realize utilization of Information Technology and Electronic Transactions that is safe, ethical, intelligent, creative, productive and innovative.

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

Article 94

(1) The roles of the Government in protecting public interest from all types of disturbances resulting from the misuse of Electronic Information and Electronic Transactions that disturb public order as referred to in Article 90 letter b include:
   a. determination of national cybersecurity strategies which form part of the national security strategies, including the development of a cybersecurity culture;
   b. regulation of information security standards;
   c. regulation of vital information infrastructure protection operations;
   d. regulation of Electronic System operation risk management;
   e. regulation of human resources in Electronic System protection operations;
   f. fostering and supervision of vital information infrastructure protection operations;
   g. fostering and supervision of Electronic System operation risk management;
   h. fostering and supervision of human resources in Electronic System protection operations;
   i. Electronic Information protection operations;
   j. information security incidents handling operations;
   k. emergency response management operations; and
   l. other functions required to protect public interest from all types of disturbances.

(2) The authority as referred to in section (1) may be exercised through cooperation with other parties.

Article 95

The roles of the Government in preventing the distribution and use of any Electronic Information and/or Electronic Documents

that contain prohibited contents in accordance with the provisions of laws and regulations as referred to in Article 90 are in the forms of:

a. access termination; and/or

b. instruction to Electronic System Operators to terminate Access

to the said Electronic Information and/or Electronic Documents.

Article 96

The Access termination as referred to in Article 95 is carried out against Electronic Information and/or Electronic Documents with the following classifications:

a. violating the provisions of laws and regulations;

b. creating public unrest and disturbing public order; and

c. informing means to or providing Access to any Electronic Information and/or Electronic Documents that contain prohibited contents in accordance with the provisions of laws and regulations.

Article 97

(1) The public may submit applications for the Access termination against Electronic Information and/or Electronic Documents as referred to in Article 96 to the Minister.

(2) The relevant Ministries or Agencies coordinate with the Minister on the Access termination against Electronic Information and/or Electronic Documents as referred to in Article 96.

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

(4) The judiciary may order the Access termination against Electronic Information and/or Electronic Documents as referred to in Article 96 to the Minister.

(5) Provisions regarding the procedures of application for the Access termination as referred to in section (1) through section (4) are regulated by a Ministerial Regulation.

Article 98

(1) Electronic System Operators must terminate Access against Electronic Information and/or Electronic Documents as referred to in Article 96.

(2) The Electronic System Operators as referred to in section (1) cover internet Access service providers, network and telecommunication service operators, content providers and link providers which provide Electronic Information and/or Electronic Documents traffic networks.

(3) An Electronic System Operator that fails to terminate such Access may be held legally liable based on the provisions of laws and regulations.

(4) Further provisions regarding the implementation of the obligation to terminate Access as referred to in section (1) are regulated by a Ministerial Regulation.

Article 99

(1) The Government determines Agencies or institutions that have strategic Electronic Data that must be protected.

(2) Agencies or institutions that have strategic Electronic Data that must be protected as referred to in section (1) include those in:
   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 as stipulated by the President.

(3) Agencies or institutions that have strategic Electronic Data as referred to in section (1) shall make Electronic Documents and their electronic backup and connect them to certain data centers for data security purposes.

(4) Further provisions regarding the obligation to make Electronic Documents and the electronic backup and to connect them to certain data centers as referred to in section (3) are regulated by a regulation of the head of the government agency in charge of cyber security affairs.

CHAPTER IX
ADMINISTRATIVE SANCTIONS

Article 100

(1) Any violations against the provisions of Article 4, Article 5 section (1) and section (2), Article 6 section (1), Article 9 section (1) and section (4), Article 14 section (1) and section (5), Article 15 section (1), Article 17 section (4), Article 18 section (1), Article 21 section (2) and section (3), Article 22 section (1), Article 23, Article 24 section (1), section (2) and section (3), Article 25, Article 26 section (1), Article 28 section (1), Article 29, Article 30 section (1), Article 31, Article 32 section (1) and section (2), Article 33, Article 34 section (1), Article 37 section (1) and section (2), Article 38 section (3), Article 39 section (2), Article 40 section (1) and section (2), Article 42 section (1) and section (3), Article 51 section (1),

Article 53 section (3), Article 55 section (2), Article 63 section (3), Article 64 section (1), Article 69 section (1), Article 82 section (7), Article 84 section (1) and section (2), Article 87 section (2), and Article 98 section (1) are subject to administrative sanctions.

(2) The administrative sanctions as referred to in section (1) may be in the forms of:
   a. written reprimands;
   b. administrative fines;
   c. temporary suspension;
   d. Access termination; and/or
   e. delisting from the list.

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

(4) The imposition of administrative sanctions as referred to in section (2) letter c and letter d are carried out through a coordination with leaders of the relevant Ministries or Agencies.

(5) The imposition of administrative sanctions as referred to in section (2) and section (3) does not abrogate criminal and civil liabilities.

Article 101

Further provisions regarding procedures for the imposition of administrative sanctions and for the filing of objection to any imposition of administrative sanctions are regulated by a Ministerial Regulation.

CHAPTER X
TRANSITIONAL PROVISIONS

Article 102

(1) Upon this Government Regulation coming into effect, Electronic System Operators that have been operating before the promulgation of this Government Regulation must make adjustments in accordance with the provision of Article 6 section (1) within a period of 1 (one) year.

(2) Upon this Government Regulation coming into effect, Public Electronic System Operators that have been operating before the promulgation of this Government Regulation must make adjustments in accordance with the provision of Article 20 section (2) within a period of 2 (two) years.

CHAPTER XI
CLOSING PROVISIONS

Article 103

(1) Upon this Government Regulation coming into effect, the implementing regulations of Government Regulation Number 82 of 2012 on Electronic System and Transaction Operations remains valid to the extent they do not conflict with and have not been replaced by any new regulations in accordance with this Government Regulation.

(2) Upon this Government Regulation coming into effect, Government Regulation Number 82 of 2012 on Electronic System and Transaction Operations (State Gazette of the Republic of Indonesia Year 2012 Number 189, Supplement to the State Gazette of the Republic of Indonesia Number 5348) is revoked and declared invalid.

Article 104

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

In order that every person may know hereof, it is ordered to promulgate this Government Regulation by its placement in the State Gazette of the Republic of Indonesia.

Established in Jakarta
on 4 October 2019

PRESIDENT OF THE REPUBLIC OF INDONESIA,

signed

JOKO WIDODO

Promulgated in Jakarta
on 10 October 2019

Interim MINISTER OF LAWS AND HUMAN RIGHTS OF THE REPUBLIC OF INDONESIA,

signed

TJAHJO KUMOLO

STATE GAZETTE OF THE REPUBLIC OF INDONESIA YEAR 2019
NUMBER 185

Certified true copy
MINISTRY OF STATE SECRETARIAT OF THE REPUBLIC OF INDONESIA
Deputy of Laws and Regulations,

[signed]

Lydia Silvanna Djaman

ELUCIDATION
ON
GOVERNMENT REGULATION
OF THE REPUBLIC OF INDONESIA
NUMBER 71 OF 2019
ON
ELECTRONIC SYSTEM AND TRANSACTION OPERATIONS

I. GENERAL OVERVIEW

Several provisions in Law Number 11 of 2008 on Electronic Information and Transactions mandate the formulation of further provisions in a Government Regulations. The provisions on Trustmark Certification Provider, Electronic Signatures, Certification Authority, Electronic System Operators, Electronic Transaction Operators, Electronic Agent Operators, and Domain Name management have been regulated in Government Regulation Number 82 of 2012 on Electronic System and Transaction Operations. However, Government Regulation Number 82 of 2012 on Electronic System and Transaction Operations needs to be adjusted to technological development and public need.

The establishment of this Government Regulation also aims to further regulate several provisions in Law Number 19 of 2016 on Amendment to Law Number 11 of 2008 on Electronic Information and Transactions that were formulated to guarantee recognition and respect for the rights and freedoms of others and for meeting demands which are fair and in accordance with considerations of security and public order in a democratic society. Some provisions that need further regulation are:

a. the obligation of each Electronic System Operator to erase the irrelevant Electronic Information and/or Electronic Documents under their control upon request of the Person concerned based on a court order; and

b. the roles of the Government in facilitating the use of Information Technology and Electronic Transactions, protecting public interest from all types of disturbances as a result of misuse of Electronic Information and Electronic Transactions that violate public order, and preventing the distribution and use of Electronic Information and/or Electronic Documents which contain prohibited contents in accordance with the provisions of laws and regulations.

This Government Regulation contains provisions on:

a. category of Electronic System Operators;
b. obligations of Electronic System Operators;
c. erasure and/or access termination against irrelevant electronic information and/or electronic documents;
d. Electronic Systems and Electronic Data placement;
e. supervision of Electronic System operations;
f. Electronic Agents operations;
g. Electronic Transactions operations;
h. Electronic Certification operations;
i. Domain Name management;
j. Government's role in the operations of Electronic System and Transaction; and
k. administrative sanctions.

II. ARTICLE BY ARTICLE

Article 1

Self explanatory.

Article 2

Section (1)

Self explanatory.

Section (2)

Self explanatory.

Section (3)

Letter a

Self explanatory.

Letter b

"institutions appointed by Agencies" mean any institutions that carry out the operation of public Electronic System on behalf of the appointing Agencies.

Section (4)

"Authorities regulating and supervising the financial sector" means authorities in the sectors of monetary, payment system, macroprudential, banking, capital market, insurance, pension funds, financial institutions, and other financial services institutions.

Section (5)

Letter a

Self explanatory.

Letter b

"An Electronic System Operator which has an online portal, site, or online application through the internet" means an Electronic System Operator whose Electronic System is used in Indonesian territory, and / or offered to be used in Indonesian territory.

Number 1

Self explanatory.

Number 2

Self explanatory.

Number 3

Self explanatory.

Number 4

Self explanatory.

Number 5

Self explanatory.

Number 6

Personal Data Processing comprises the acquirement and collection, processing and analysis, correction and updating, display, announcement, transfer, distribution, or disclosure, and/or erasure or destruction of Personal Data.

Article 3

Section (1)

"Reliable" means that the Electronic System has the ability to fulfil its usage needs.

"Secure" means that the Electronic System is physically and non-physically protected.

"Due operations" means that the Electronic System has the ability in accordance with its specifications.

Section (2)

"Responsible" means the Electronic System Operator who is legally responsible for the operation of the said Electronic System

Section (3)

Self explanatory.

Article 4

Self explanatory.

Article 5

Self explanatory.

Article 6

Self explanatory.

Article 7

Section (1)

Letter a

"Interconnectivity" means the ability to connect with each other so they can function properly.

Interconnectivity includes interoperability capabilities.

"Compatibility" means the suitability of one Electronic System with another Electronic System.

Letter b

Self explanatory.

Letter c

Self explanatory.

Section (2)

Certification evidence may be acquired through third parties accredited in Indonesia or by obtaining other evidence as supporting documents stating compliance with the requirements from certification bodies outside of Indonesia.

Article 8

Letter a

"Have its operational security and reliability duly guaranteed" means that the Electronic System Operator shall guarantee that the Software does not contain other instructions which are improper or hidden instructions that are illegal (malicious code), such as time bomb instructions, virus programs, trojans, worms, and backdoor. This security may be provided by checking the source code.

Letter b

Self explanatory.

Article 9

Section (1)

"Source codes" mean a series of commands, statements, and/or declarations written in computer programming languages that can be read and understood by a person.

Section (2)

Self explanatory.

Section (3)

"Source code escrow" means a profession or independent party that is competent to provide a source code storage service for computer programs or Softwares for the benefit of the operator to be able to access, acquire, or submit source code to the users.

Section (4)

Self explanatory.

Section (5)

Self explanatory.

Section (6)

Self explanatory.

Article 10

Section (1)

"An expert" means a person who has special knowledge and skills in the field of Electronic Systems that is academically or practically accountable.

Section (2)

Self explanatory.

Article 11

Section (1)

Letter a

“Service level agreements” mean statements regarding the level of service quality of an Electronic System.

Letter b

Self explanatory.

Letter c

Self explanatory.

Section (2)

Self explanatory.

Article 12

"Apply risk management" means conducting risk analysis and formulating mitigation and countermeasures to overcome threats, disturbances, and obstacles to the Electronic System it manages.

Article 13

"Governance policies" include, among others, policies regarding the activities of building organizational structures, business processes, and performance management, as well as providing personnel supporting the operation of the Electronic Systems to ensure that the Electronic Systems may operate properly.

Article 14

Section (1)

Self explanatory.

Section (2)

Self explanatory.

Section (3)

"Valid consent" means a consent submitted explicitly and may not be in secret or on the basis of mistake, negligence, or dures.

Section (4)

Letter a

Self explanatory.

Letter b

Self explanatory.

Letter c

“Vital interest" means the need/necessity to protect very essential matters about an individual's existence.

Letter d

Self explanatory.

Letter e

Self explanatory.

Letter f

Self explanatory.

Section (5)

Self explanatory.

Section (6)

Self explanatory.

Article 15

Section (1)

Self explanatory.

Section (2)

Letter a

Self explanatory.

Letter b

"Right to delisting" means that the Electronic System Operator that operates the search engine should remove the display and/or terminate the Access to irrelevant Electronic Information and/or Electronic Documents based on a court order.

Section (3)

Self explanatory.

Article 16

Self explanatory.

Article 17

Self explanatory.

Article 18

Self explanatory.

Article 19

Section (1)

Good and accountable Electronic System governance (Good IT governance) comprises the processes of planning, implementation, operation, maintenance, and documentation.

Section (2)

Self explanatory.

Section (3)

Self explanatory.

Article 20

Section (1)

"Business continuity plan" means a series of processes carried out to ensure the continuity of activities in the event of a disturbance or disaster.

Section (2)

Self explanatory.

Section (3)

Self explanatory.

Section (4)

Self explanatory.

Section (5)

Self explanatory.

Section (6)

Self explanatory.

Section (7)

Self explanatory.

Article 21

Self explanatory.

Article 22

Section (1)

The audit trail mechanism comprises:

a. maintaining transaction log maintenance in accordance with the operator's data retention policy, in accordance with the provisions of laws and regulations;
b. giving notification to consumers when a transaction has been successfully carried out;
c. assuring the availability of an audit trail function in order to be able to detect businesses and/or

incursions that shall be reviewed or evaluated periodically; and

d. conducting audit trail that shall be in accordance with the standards set by the Electronic System Operator in the event that the audit processing system and trail are the responsibility of a third party.

Section (2)

"Other examinations" include inspections for mitigation or incident response handling.

Article 23

Electronic System Components comprise:

a. Software;
b. Hardware;
c. experts;
d. Electronic System security system; and
e. Electronic System governance.

Article 24

Section (1)

"Disruptions" mean any actions that are destructive or have a serious impact on the Electronic System so that the Electronic System does not work properly.

"Failures" mean the cessation of part or all of the functions of the Electronic System which are essential so that the Electronic System does not function properly.

"Losses" mean the impact of damage to the Electronic System, both material and immaterial in nature, which has legal consequences for users, operators, and other third parties.

Section (2)

"Systems for the prevention and overcoming" comprises antivirus, anti spamming, firewall, intrusion detection, prevention system, and/or management of information security management system.

Section (3)

Self explanatory.

Section (4)

Self explanatory.

Article 25

Self explanatory.

Article 26

Section (1)

Self explanatory.

Section (2)

"Transferable Electronic Information and/or Electronic Documents" means eligible papers or valuable papers in electronic forms.

"Electronic Information and/or Electronic Documents shall be unique" means that the Electronic Information and/or Electronic Documents and/or the recording of Electronic Information and/or Electronic Documents are the only ones that represent a certain value.

"Electronic Information and/or Electronic Documents shall explain their control" means the Electronic Information and / or Electronic Documents shall be able to explain the nature of the control represented by the control system or recording system of the Electronic Information and/or Electronic Documents concerned.

"Electronic Information and/or Electronic Documents shall explain their ownership" means the Electronic Information and/or Electronic Documents shall explain the nature of ownership represented by the existence of technological control facilities that guarantee there is only one legal copy (single authoritative copy) and it does not change.

Article 27

"Interoperability" menas the ability of different Electronic Systems to be able to work in an integrated manner.

"Compatibility" means the compatibility of one Electronic System with another Electronic System.

Article 28

Section (1)

Self explanatory.

Section (2)

Education that may be provided to Electronic System Users comprises:

a. conveying to Electronic System Users the importance of maintaining the security of Personal Identification Number (PIN)/password) for example by:
    1. keeping it as secret and not revealing your PIN/password to anyone including an employee of the operator;
    2. changing PIN/password regularly;
    3. using a PIN/password that is not easily guessed such as the use of a personal identity in the form of date of birth;
    4. not writing down PIN/password; and
    5. having different PIN/passwords for every product.
b. explaining to Electronic System Users regarding the various modes of crime of Electronic Transactions; and
c. conveying to Electronic System Users regarding the procedures for filing claims.

Article 29

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

Article 30

Section (1)

Provision of features is intended to protect the rights or interests of Electronic System Users.

Section (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

Section (1)

Self explanatory.

Section (2)

Self explanatory.

Section (3)

Self explanatory.

Section (4)

Letter a

"Visual" form means a display that can be seen or read, including a graphical display of a website.

Letter b

"Audio" form means anything that can be heard, including telemarketing services.

Letter c

"Electronic Data" forms comprise electronic data capture (EDC), radio frequency identification (RFI), and barcode recognition.

Electronic data capture (EDC) means an Electronic Agent for and on behalf of the Electronic System Operator in collaboration with network providers. EDC may be used independently by banking institutions and/or jointly with other financial or non-financial institutions.

In the event that an Electronic Transaction is carried out using the Bank X's card on Bank Y's EDC, Bank Y shall forward the transaction to Bank X, through the said network operator.

Letter d

Self explanatory.

Article 37

Section (1)

Letter a

Information about the identity of the Electronic Agent Operator at least contains a logo or a name indicating the identity.

Letter b

Self explanatory.

Letter c

Self explanatory.

Letter d

Self explanatory.

Letter e

Self explanatory.

Letter f

Self explanatory.

Letter g

Self explanatory.

Letter h

Self explanatory.

Section (2)

Self explanatory.

Section (3)

Self explanatory.

Section (4)

Self explanatory.

Article 38

Section (1)

Self explanatory.

Section (2)

Self explanatory.

Section (3)

"Equal treatment" includes the imposition of the same tariffs, facilities, requirements and procedures.

Section (4)

Self explanatory.

Article 39

Section (1)

Self explanatory.

Section (2)

Self explanatory.

Section (3)

Letter a

"Confidentiality" means a definition that is in accordance with the legal concept of confidentiality of information and communication electronically.

Letter b

"Integrity" means a definition that is in accordance with the legal concept of integrity of Electronic Information.

Letter c

"Availability" means a definition that is in accordance with the legal concept of availability of Electronic Information.

Letter d

"Authenticity" means a definition that is in accordance with the legal concept of authentication which includes the originality of the contents of an Electronic Information.

Letter e

"Authorization" means a definition that is in accordance with the legal concept of authorization based on the scope of duties and functions of an organization and management.

Letter f

"Non-repudiation" means a definition that is in accordance with the legal concept of nonrepudiation.

Article 40

Section (1)

Letter a

In testing identity authenticity and validating the authorizations of Electronic System Users, it is necessary to pay attention to, among others:

1. written policies and procedures to ensure the ability to test the authenticity of identity and check the authority of Users of Electronic Systems;
2. methods for testing authenticity; and
3. combination of at least 2 (two) authentication factors (two factor authentication mechanism), namely "what you know" (PIN/password), "what you have" (magnetic card with chip, token, digital signature), "what you are" or "biometrics" (retina and fingerprints).

Letter b

Self explanatory.

Letter c

Self explanatory.

Letter d

Protection of the confidentiality of Personal Data Users of Electronic Systems shall also be met in the event that the operator uses the services of other parties (outsourcing).

Letter e

Self explanatory.

Letter f

Self explanatory.

Letter g

Procedures for handling of unexpected occurrences shall also be met in the event that the operator uses the services of another party (outsourcing).

Section (2)

In formulating and stipulating procedures for ensuring that Electronic Transactions may not be disclaimed by consumers, it shall consider that:

a. the Electronic Transaction system has been designed to reduce the possibility of unintended transactions by authorized users;
b. the entire identity of the party conducting the transaction has been authenticated; and
c. financial transaction data is protected from possible tampering and any changes may be detected.

Article 41

Self explanatory.

Article 42

Self explanatory.

Article 43

Self explanatory.

Article 44

Section (1)

This provision is intended to protect Electronic System Users from sending unsolicited Electronic Information (spam).

Common forms of spam are among others e-mail spam, instant message spam, usenet newsgroup spam, web search engine spam, blog spam, news spam on mobile phones, and Internet forum spam.

Section (2)

Self explanatory.

Article 45

Section (1)

Self explanatory.

Section (2)

Letter a

Self explanatory.

Letter b

Self explanatory.

Letter c

Self explanatory.

Letter d

Self explanatory.

Letter e

"Reasonableness" means a definition that is referring to the element of propriety that applies in accordance with developing business habits or practices.

Article 46

Section (1)

Electronic Transactions may comprise several forms or variants, including:

a. an agreement that is not done electronically but the contractual relationship is completed electronically;
b. an agreement that is done electronically and the contractual relationship is completed electronically; and
c. an agreement that is done electronically and the contractual relationship is settled not electronically.

Section (2)

Self explanatory.

Article 47

Section (1)

Self explanatory.

Section (2)

"Laws and regulations" comprise the Law on Consumer Protection.

Section (3)

Self explanatory.

Article 48

Section (1)

"Complete and correct information" comprises:

a. information containing the identity and status of a legal subject and their competencies, be it as a producer, supplier, operator or intermediary;
b. other information that explains certain matters which constitute a legal condition of the agreement and explains the goods and/or services offered, such as the name, address, and description of the goods/services.

"Contract" means among others agreement or cooperation.

Section (2)

Self explanatory.

Section (3)

Self explanatory.

Section (4)

Self explanatory.

Section (5)

Self explanatory.

Article 49

Section (1)

Self explanatory.

Section (2)

Electronic Transactions occur when an agreement is reached between the parties in the form of checking of data, identity, personal identification number (PIN) or password.

Section (3)

Letter a

"An act of acceptance stating approval" comprises clicking an electronic agreement by an Electronic System User.

Letter b

Self explanatory.

Article 50

Section (1)

Self explanatory.

Section (2)

"Proportionate" means considering the interests of both parties equally.

Article 51

Section (1)

The obligation to use Electronic Certificates applies to SSL Encryption.

Section (2)

Self explanatory.

Section (3)

Electronic Certificate Ownership means one of the efforts to improve the implementation security of the Electronic System in addition to other security efforts.

Electronic Certificate Ownership serves to support the security of the operation of the Electronic System which includes, among others, confidentiality, authenticity, integrity, and non-repudiation.

Section (4)

Self explanatory.

Section (5)

Self explanatory.

Section (6)

The Ministerial Regulation provides, among other things, the procedure for submitting electronic certification applications submitted through a Certification Authority or Registration Authority appointed by a Certification Authority.

Article 52

Letter a

"Examine" means an examination of the physical presence of the prospective certificate holder, which may be carried out using an online method if the examination uses biometrics.

Letter b

Electronic Signature means an approval of Electronic Information and/or Electronic Documents carried out by an Individual or individual representing a Business Entity or an Agency.

Article 53

Section (1)

Letter a

"Indonesian Certification Authority" means a Certification Authority that is certified so that

supervision can be carried out on the operation and to be a differentiator that the Certification Authority of Indonesia may be an escrow that guarantees the authenticity of electronic identity.

Letter b

Self explanatory.

Section (2)

"One-root principle" means that Indonesian Certification Authority of is rooted to the Root CA held by the Minister and the certificate is signed using the certificate of the Root CA.

Section (3)

Self explanatory.

Section (4)

Self explanatory.

Section (5)

"Registered" does not mean registering as an Indonesian Business Entity but registering its company as a Foreign Certification Authority to the Minister.

Section (6)

Self explanatory.

Article 54

Self explanatory.

Article 55

Self explanatory.

Article 56

Self explanatory.

Article 57

Section (1)

Self explanatory.

Section (2)

Self explanatory.

Section (3)

Letter a

Electronic seal means an electronic signature used by a Business Entity or an Agency to guarantee the authenticity and integrity of an electronic information and/or electronic document.

Letter b

Electronic time stamps mean the signs which bind the time and date with the Electronic Information and/or Electronic Documents using reliable methods.

Letter c

Registered electronic delivery services mean services that provides delivery of Electronic Information and/or Electronic Documents and provides evidence related to the delivery of Electronic Information and/or Electronic Documents and protects Electronic Information and/or Electronic Documents sent from the risk of loss, theft, damage or illegal changes.

Letter d

Website Authentication means a service that identifies the website owner and links the website to the Person or Business Entity that receives the Electronic Certificate of the website using a reliable method.

Letter e

Preservation of Electronic Signature and/or electronic seal is a service that guarantees the legal strength of Electronic Signature and electronic seal in an Electronic Information and/or Electronic Document may still be validated even though the Electronic Certificate validity period has expired.

Article 58

Section (1)

In the event that the Indonesian Certification Authority cooperates with other Electronic System Operator in the operation of part of its infrastructure or services, any loss or negligence that occur will remain the liability of the Indonesian Certification Authority.

Section (2)

Self explanatory.

Section (3)

Self explanatory.

Article 59

Self explanatory.

Article 60

Section (1)

Electronic Signatures function like manual signatures in terms of representing the identity of a Signatory. Authenticating a manual signature may be done through verification or examination of the Electronic Signature specimen from the Signatory.

In Electronic Signatures, the Electronic Signature Creation Data acts as a specimen of Electronic Signature from a Signatory.

Electronic Signature shall be able to be used by competent experts to carry out examination and verification that Electronic Information signed with Electronic Signature does not change after being signed.

Section (2)

The legal consequences of the use of certified or uncertified Electronic Signatures affect the strength of the evidentiary value.

Section (3)

Self explanatory.

Section (4)

Self explanatory.

Article 61

Section (1)

"Uniquely" means that any code that is used or functioned as Electronic Signature Creation Data shall refer only to one legal subject or an entity that represents an identity.

Section (2)

Self explanatory.

Section (3)

Letter a

Electronic Signature Creation Data generated by cryptographic techniques in general have a probability-based mathematical correlation with Electronic Signature verification data. Therefore the selection of the cryptographic code to be used shall consider the adequacy of the level of difficulty faced and the resources that shall be prepared by those who try to falsify the Electronic Signature Creation Data.

Letter b

"Electronic media" means a facility, means, or equipment used to collect, store, process and/or distribute Electronic Information that is used temporarily or permanently.

Letter c

"Data relating to the Signatory" means all data that may be used to identify the identity of the Signatory such as name, address, place and date of birth, as well as the manual signature specimen code.

"Reliable system" means a system that follows the procedure of using Electronic Signatures

which ensures the authenticity and integrity of Electronic Information. This may be recognized by considering several factors, including:

1. finance and resources;
2. the quality of Hardware and Software;
3. certification and application procedures and data retention;
4. availability of Electronic Signature Creation Data; and
5. audits by independent institutions.

Letter d

Self explanatory.

Section (4)

Self explanatory.

Article 62

Section (1)

Self explanatory.

Section (2)

Self explanatory.

Section (3)

Self explanatory.

Section (4)

Self explanatory.

Section (5)

Self explanatory.

Section (6)

Examples of this provision are as follows:

a. Changes to the Electronic Signature after the signing time shall result in the Electronic Information to which it is attached not functioning properly, damaged, or unable to be displayed if the Electronic Signature is attached and/or related to the signed Electronic Information. The technique of attaching and linking an Electronic

Signature to signed Electronic Information may lead to the occurrence of new Electronic Information or Electronic Documents that:

1. are seen as an inseparable whole; or
2. appear to be separate and the signed Electronic Information can be read by lay person while the Electronic Signature is in the form of a code and/or picture.

b. Changes to Electronic Signatures after the signing time shall result in some or all Electronic Information being invalid if the Electronic Signature is logically associated with the signed Electronic Information. Changes that occur to the signed Electronic Information shall cause a discrepancy between the Electronic Signature and the related Electronic Information which can be clearly seen through a verification mechanism.

Article 63

Self explanatory.

Article 64

Section (1)

Self explanatory.

Section (2)

Authentication factors that may be chosen to be combined may be divided into 3 (three) types, namely:

a. something that is individually owned (what you have) such as an ATM card or smart card;
b. something that is known individually (what you know) for example PIN/password or cryptographic key; and
c. something that is the characteristic of an individual (what you are) for example voice patterns, handwriting dynamics, or fingerprints.

Section (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

Section (1)

Self explanatory.

Section (2)

Self explanatory.

Section (3)

Self explanatory.

Section (4)

Letter a

Self explanatory.

Letter b

"Addresses" mean information that at least explains the cities of domicile where the person or Business Entity is operating.

Letter c

Self explanatory.

Letter d

Self explanatory.

Letter e

Self explanatory.

Letter f

Self explanatory.

Section (5)

Self explanatory.

Section (6)

Self explanatory.

Article 72

Self explanatory.

Article 73

Section (1)

Self explanatory.

Section (2)

Self explanatory.

Section (3)

Self explanatory.

Section (4)

Letter a

Information Technology Consultants comprise the information security profession.

Letter b

Self explanatory.

Letter c

Self explanatory.

Section (5)

Self explanatory.

Section (6)

Self explanatory.

Article 74

Self explanatory.

Article 75

Self explanatory.

Article 76

Section (1)

Letter a

Identity registration means a Trustmark whose guarantee of reliability is limited only on securing that the Business Actor's identity is correct.

Validation carried out by the Trustmark Certification Provider only applies to the identity of a Business Actor that at least contains the name of the legal subject, legal subject's status, address or position, telephone number, e-mail address, business permit, and Taxpayer Identification Number (NPWP) if they are not already registered in the electronically integrated business licensing service/Online Single Submission system.

The Trustmark Certification Provider that issues this Trustmark provides search certainty that the Business Actor's identity is correct.

Letter b

Electronic System Security is a Trustmark whose guarantee of reliability provides certainty that the process of delivering or exchanging data are conducted through the Actor's website.

Business is protected by using security technology to process data exchange such as SSL/secure socket layer protocol.

This Trustmark guarantees that there is a security system in the data exchange process that has been tested.

Security against vulnerability (vulnerability seal) means a Trustmark whose guarantee of reliability provides certainty that there is an information security management system implemented by a

Business Actor with reference to certain Electronic System security standards in accordance with provisions of laws and regulations.

Letter c

Privacy policy means a Trustmark whose guarantee of reliability provides certainty that the consumer's Personal Data is protected properly.

Section (2)

Self explanatory.

Section (3)

Self explanatory.

Article 77

Self explanatory.

Article 78

Self explanatory.

Article 79

Section (1)

Self explanatory.

Section (2)

Letter a

"Generic Top-Level Domain Name" means a top level Domain Name consisting of three or more characters in the domain naming system hierarchy other than the country code Top Level Domain. For example ".nusantara" or ".java".

Letter b

"Indonesian Top-Level Domain Name " means a top level domain in the domain naming system hierarchy that shows Indonesian code (.id) according to the list of country codes in ISO 3166-1 used and recognized by the Internet Assigned Numbers Authority (IANA).

Letter c

Examples of second-level Indonesian Domain Names are co.id, go.id, ac.id, or.id, or mil.id.

Letter d

Example of a lower-level Indonesian Domain Name is kominfo.go.id.

Section (3)

Letter a

Definition of the Domain Name Registry comprises the function and role of the ccTLD manager.

Letter 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

Letter a

"National Electronic System gateway" comprises the Indonesian National Single Window (INSW) and electronically integrated business licensing service (online single submission).

Letter b

Self explanatory.

Letter c

Self explanatory.

Letter d

General applications and strategic Electronic Data are operated in an integrated data center and national disaster recovery center.

Letter e

Self explanatory.

Letter f

Self explanatory.

Letter g

Self explanatory.

Article 93

Self explanatory.

Article 94

Self explanatory.

Article 95

Self explanatory.

Article 96

Letter a

"Violating the provisions of laws and regulations" comprises Electronic Information and/or Electronic Documents that contain elements of pornography, gambling, slander and/or defamation, fraud, hatred of ethnicity, religion, race, and intergroup, violence and/or violence against children, violations of intellectual property, violations of trade in goods and services through electronic systems, terrorism and/or radicalism, separatism and/or prohibited dangerous organizations, violations of information security, violations of consumer protection, violations in health sector, violations of medicine and food supervision.

Letter b

"Creating public unrest and disturbing public order" comprises falsified information and/or facts.

Letter c

Self explanatory.

Article 97

Self explanatory.

Article 98

Section (1)

"Terminate Access" comprises Access blocking, account closure, and/or content erasure.

Section (2)

Self explanatory.

Section (3)

Self explanatory.

Section (4)

Self explanatory.

Article 99

Section (1)

"Agencies or institutions that have strategic Electronic

Data" means agencies or institutions that have vital information infrastructure in the specified sector.

Section (2)

Self explanatory.

Section (3)

Connections to certain data centers for data security purposes are carried out in the event of occurrence of incidents that must be reported to institution in charge of cyber security matters.

Section (4)

Self explanatory.

Article 100

Section (1)

Imposition of sanctions in this provision is only intended for parties who commit administrative violations, whereas those concerning moral or civil violations are not subject to administrative sanctions.

Section (2)

Letter a

Self explanatory.

Letter b

Self explanatory.

Letter c

"Temporary suspension" means a termination of some or all components or services in the Electronic System concerned for a certain period of time.

Letter d

“Access termination" comprises Access blocking, account closure, and/or content removal.

Letter e

Self explanatory.

Section (3)

Self explanatory.

Section (4)

Self explanatory.

Section (5)

Self explanatory.

Article 101

Self explanatory.

Article 102

Self explanatory.

Article 103

Self explanatory.

Article 104

Self explanatory.

SUPPLEMENT TO STATE GAZETTE OF THE REPUBLIC OF INDOENSIA NUMBER 6400.