REGULATION OF THE GOVERNMENT OF THE REPUBLIC OF INDONESIA

NUMBER 71 OF 2019

ON

ORGANIZATION OF ELECTRONIC SYSTEMS AND TRANSACTIONS[1]

BY THE GRACE OF GOD ALMIGHTY

PRESIDENT OF THE REPUBLIC OF INDONESIA,

Considering:

a. that with the existence of very rapid development of information technology in bid to encourage digital-economy growth and enforcement of state sovereignty over electronic information within the Unitary State of the Republic of Indonesia, comprehensive regulation on the utilization of information technology and electronic transactions is deemed necessary;

b. that Regulation of the Government Number 82 of 2012 on Organization of Electronic Systems and Transactions is no longer compatible with the development of public legal needs, hence it is required to be replaced;

c. that based on considerations as referred to in letter a and letter b, it is deemed necessary to establish Regulation of the Government on Organization of Electronic Systems and Transactions;

In view of:

1. Article 5 paragraph (2) of 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 of 2008 Number 58, Supplement to the State Gazette of the Republic of Indonesia Number 4843) as amended by Law Number 19 of 2016 on

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

Amendment to Law Number 11 of 2008 on Electronic Information and Transactions (State Gazette to the Republic of Indonesia of 2016 Number 251, Supplement to the State Gazette of the Republic of Indonesia Number 5952);

HAS DECIDED:

To enact:

REGULATION OF THE GOVERNMENT ON ORGANIZATION OF ELECTRONIC SYSTEMS AND TRANSACTIONS.

CHAPTER 1
GENERAL PROVISIONS

Article 1

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

1. Electronic System is a set of electronic devices and procedures which function to prepare, collect, process, analyze, store, display, publish, send, and/or disseminate Electronic Information.
2. Electronic Transaction is legal act which is performed by using computer, computer network, and/or other electronic media.
3. Electronic Agent is device of an Electronic System which is created to perform an act against a certain Electronic Information automatically as organized by Person.
4. Electronic System Provider is every Person, state organizer, Enterprise, and the public who provide, manage, and/or operate Electronic System, individually or jointly, to Electronic System User for its own and/or other's needs.
5. Public Electronic System Provider is the organization of Electronic System by State Organizer Body or institution as appointed by the State Organizer Body.
6. Private Electronic System Provider is the organization of Electronic System by Person, Enterprise, and the public.
7. Ministry or Agency is State Organizer Body which has the duty to supervise and issue regulation within its sector.

8. Electronic Information is a single or collection of Electronic Data, including but not limited to text, sound, image, map, design, photo, electronic data interchange (EDI), electronic mail (*surat elektronik*), telegram, telex, telecopy or its kind, letter, mark, number, Access code, symbol, or perforation which has been processed and has meaning or may be understood by person who is capable to understand it.
9. Electronic Document is every Electronic Information which is created, forwarded, sent, received, or stored in the forms of analog, digital, electromagnetic, optical, or its kind, that may be viewed, displayed, and/or heard through computer or Electronic System, including but not limited to text, sound, image, map, design, photo or its kind, letter, mark, number, Access code, symbol or perforation which has definition or meaning or may be understood by person who is capable to understand it.
10. Information Technology is a technique to collect, prepare, store, process, publish, analyze, and/or disseminate information.
11. Subscriber is every Person, state organizer, Enterprise, and the public who utilize goods, services, facilities, or information that are provided by Electronic System Provider.
12. Hardware is a single or set of devices which is connected to Electronic System.
13. Software is a single or set of programs, computers, procedures, and/or documentations which are related to the operation of Electronic System.
14. Electronic System Feasibility Test is a set of objective assessment processes against every Electronic System components, both performed independently and/or performed by institution who is in charge and competent.
15. Access is activity to perform interaction with Electronic System that is independent or online.
16. Organization of Electronic Transaction is a set of Electronic Transaction activities which are performed by Sender and Acceptor by using Electronic System.
17. Electronic Contract is agreement of the parties which is made through Electronic System.
18. Sender is legal subject who sends Electronic Information and/or Electronic Document.
19. Acceptor is legal subject who accepts Electronic Information and/or Electronic Document from the Sender.

20. Digital Certificate is certificate that is electronic in nature which contains Digital Signature and identity that shows legal subject status of the parties to Electronic Transaction which is issued by Digital Certification Provider.
21. Digital Certification Provider is incorporated entity which functions as the trusted party, who grants and audits Digital Certificate.
22. Digital Signature is signature which consists of Electronic Information that is affixed, associated or related to other Electronic Information which is used as verification and authentication tool.
23. Signor is legal subject who is associated with or related to Digital Signature.
24. Digital Signature Application [*Perangkat Pembuat Tanda Tangan Elektronik*] is Software or Hardware which is configured and used to generate Digital Signature.
25. Digital Signature Generation Data is personal code, biometric code, cryptographic code, and/or code that is generated from the modification of conventional signature to Digital Signature, including other code which is generated from the development of Information Technology.
26. Reliability Certification Agency is independent agency which is established by acknowledged professionals, legalized, and supervised by the Government, with the authority to audit and issue Reliability Certificate in Electronic Transaction.
27. Reliability Certificate is document which states that Business who organizes Electronic Transaction has passed conformity audit or test from Reliability Certification Agency.
28. Business is every individual or enterprise, either taking form as incorporated or unincorporated entity, which is established and domiciled or operate activities within the jurisdiction of the Republic of Indonesia, individually or jointly, through agreement on the organization of business activities within various economic sectors.
29. Personal Data is every data on individual, both identified and/or identifiable individually or combined with another information, either directly or indirectly, through Electronic and/or non-electronic System.
30. Electronic Data is data in electronic forms which is not limited to text, sound, image, map, design, photo, electronic data interchange (EDI), electronic mail (*surat*

elektronik), telegram, telex, telecopy or its kind, letter, mark, number, Access code, symbol, or perforation.

31. Domain Name is internet address of state organizer, Person, Enterprise, and/or the public, which may be used to communicate through internet, in the forms of code or composition of unique characters to show certain location on the internet.
32. Domain Name Registry is the organizer who is responsible to perform management, operation, and maintenance of the organization of Electronic System of Domain Names.
33. Domain Name Registrar is Person, Enterprise, or the public who provides Domain Name registration service.
34. Domain Name User is Person, State Organizer Body, Enterprise, or the public who submits registration for the use of Domain Name to the Domain Name Registrar.
35. State Organizer Body, hereinafter referred to as Body, is legislative, executive, and judicial institutions on central and regional levels, and other bodies which are established based on laws and regulations.
36. Person is individual, either Indonesian nationals, foreign nationals, or incorporated entities.
37. Enterprise is individual company or partnership company, either taking form as incorporated or unincorporated entity.
38. Government is Minister or other official as appointed by the President.
39. Minister is minister who organizes governmental affairs within the communication and informatics sector.

CHAPTER II
ORGANIZATION OF ELECTRONIC SYSTEMS

First Division
General

Article 2

(1) Organization of Electronic System is performed by Electronic System Provider.

(2) Electronic System Provider as referred to in paragraph (1) encompasses:
   a. Public Electronic System Provider; and
   b. Private Electronic System Provider.

(3) Public Electronic System Provider encompasses:
   a. Body; and
   b. institution as appointed by the Body.

(4) Public Electronic System Provider as referred to in paragraph (2) letter a does not encompass Public Electronic System Provider who is regulatory and supervisory authority of financial sector.

(5) Private Electronic System Provider as referred to in paragraph (2) letter b encompasses:
   a. Electronic System Provider who is regulated or supervised by Ministry or Agency based on provisions under laws and regulations; and
   b. Electronic System Provider who owns online portal, sites, or application through the internet, which is used to:
      1. provide, manage, and/or operate offer and/or trading of goods and/or services;
      2. provide, manage, and/or operate financial transaction services;
      3. delivery of paid digital material or content through data network, either by downloading via portal or site, delivery through electronic mail, or through other application to user's device;
      4. provide, manage, and/or operate communication services, including, but not limited to, short message, voice call, video call, electronic mail, and online conversation in the forms of digital platform, network services and social media;
      5. search engine services, services which provide Electronic Information in the forms of text, sound, image, animation, music, video, film, and game or combination of its part and/or entire part; and/or
      6. processing of Personal Data for operational activities as public services which relate to Electronic Transaction activities.

Article 3

(1) Any Electronic System Provider should organize Electronic System in reliable and secure manners, as well as be responsible for the proper operation of Electronic System.

(2) Electronic System Provider is responsible for the organization of its Electronic System.

(3) Provision as referred to in paragraph (2) does not prevail in case the occurrence of force majeure [*keadaan memaksa*], error, and/or negligence of Electronic System's user can be proven.

Article 4

Insofar that it is not addressed otherwise under separate law, any Electronic System Provider must operate Electronic System which fulfills the following minimum requirements:

a. able to redisplay Electronic Information and/or Electronic Document intact in accordance with the retention period as determined under laws and regulations;

b. able to protect the availability, integrity, authentication, confidentiality, and accessibility of Electronic Information in the course of organization of such Electronic System;

c. able to operate in accordance with procedure or instruction of organization of such Electronic System;

d. accompanied with procedure or instruction which is published in language, information, or symbol which is understandable by parties relating to the organization of such Electronic System; and

e. have sustainable mechanism to protect the newness, clarity, and accountability of procedure or instruction.

Article 5

(1) Electronic System Provider must ensure its Electronic System does not contain Electronic Information and/or Electronic Document which are prohibited by provisions under laws and regulations.

(2) Electronic System Provider must ensure its Electronic System does not facilitate the dissemination of Electronic Information and/or Electronic Document which is prohibited by provisions under laws and regulations.
(3) Provisions on the obligations of Electronic System Provider as referred to in paragraph (1) and paragraph (2) are addressed under Regulation of the Minister.

Second Division
Registration of Electronic Systems

Article 6

(1) Any Electronic System Provider as referred to under Article 2 paragraph (2) must perform registration.
(2) Obligation to perform registration by Electronic System Provider is performed before the Electronic System starts to be used by Electronic System User.
(3) Registration of Electronic System Provider as referred to in paragraph (1) is submitted to the Minister through electronically-integrated business licensing services in accordance with provisions under laws and regulations.
(4) Further provisions on registration of Electronic System Provider as referred to in paragraph (3) refer to norms, standards, procedures, and criteria as addressed under Regulation of the Minister.

Third Division
Hardware

Article 7

(1) Hardware which is used by Electronic System Provider should:
    a. fulfill security, interconnectivity and compatibility aspects with the system that is used;
    b. have technical supporting, maintenance and/or aftersales services from seller or provider; and
    c. have guarantee on the sustainability of the service.

(2) Fulfillment of requirements as mentioned in paragraph (1) should be performed through certification or other equivalent evidence.

Fourth Division
Software

Article 8

Software which is used by Electronic System Provider should:

a. be guaranteed on the security and reliability of proper operation; and
b. ensure the sustainability of the service.

Article 9

(1) Developer who provides Software which is specifically developed for Public Electronic System Provider must handover the source code and documentation of Software to the relevant Body or institution.
(2) Relevant Body or institution as referred to in paragraph (1) must store the source code and documentation of Software in question in the means in accordance with provisions under laws and regulations.
(3) In case the means as referred to in paragraph (2) are not yet available, the Body or institution may store source code and documentation of Software at trusted third party as the source code escrow.
(4) Developer must guarantee the acquisition and/or Access to source code and documentation of Software to the trusted third party as referred to in paragraph (3).
(5) Public Electronic System Provider must ensure the confidentiality of source code of Software that is used and only be used for the interests of Public Electronic System Provider.
(6) Further provisions on obligation on the handover of source code and documentation of Software to the Body or institution as referred to in paragraph (1) and storage of source code and documentation of Software to the trusted third party as referred to in paragraph (3) are addressed under Regulation of the Minister.

Fifth Division
Experts

Article 10

(1) Experts who are hired by Electronic System Provider should possess competence within the Electronic System or Information Technology sector.

(2) Experts as referred to in paragraph (1) must fulfill provisions under laws and regulations.

Sixth Division
Governance of Electronic Systems

Article 11

(1) Electronic System Provider should guarantee:
   a. availability of service level agreement [*perjanjian tingkat layanan*];
   b. availability of information security agreement against Information Technology services which are used; and
   c. security of information and internal communication means which are organized.

(2) Electronic System Provider as referred to in paragraph (1) should guarantee every components and integration of the entire Electronic Systems to properly operate.

Article 12

Electronic System Provider should implement risk management against damages or losses as incurred.

Article 13

Electronic System Provider should have governance policies, working operational procedures, and audit mechanisms which are performed periodically against Electronic System.

Article 14

(1) Electronic System Provider must implement Personal Data protection principles in the course of performing Personal Data processing, including:
   a. collection of Personal data is performed in limited and specific manners, legal, fair, within the knowledge and consent of Personal Data subject;
   b. processing of Personal Data is performed in accordance with its purposes;
   c. processing of Personal Data is performed by guaranteeing rights of Personal Data subject;
   d. processing of Personal Data is performed accurately, comprehensively, not misleading, update, accountably, and give regards to the purposes of Personal Data processing;
   e. processing of Personal Data is performed by protecting the security of Personal Data from being lost, misused, Access and unlawful disclosure, as well as modification or tampering of Personal Data;
   f. processing of Personal Data is performed by notifying the purposes of collection, processing activity, and failure of Personal Data protection; and
   g. processing of Personal Data is destructed and/or erased, unless it is still within the retention period in accordance with the needs based on provisions under laws and regulations.

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

(3) Processing of Personal Data should fulfill provisions on the existence of lawful consent from Personal Data subject for 1 (one) or several certain purposes which have been informed to the Personal Data subject.

(4) Asides from the existence of consent as referred to in paragraph (1), processing of Personal Data should fulfill the provisions which are required for:

a. fulfillment of performance of agreement in case the Personal Data subject becomes one of the parties or to fulfill request of Personal Data subject when going to perform the agreement;
b. fulfillment of legal obligation of Personal Data controller in accordance with provisions under laws and regulations;
c. fulfillment of protection of vital interest (*kepentingan yang sah*) of Personal Data subject;
d. enforcement of authority of Personal Data controller based on provisions under laws and regulations;
e. fulfillment of obligation of Personal Data controller within public service for public interests; and/or
f. fulfillment of other vital interests of Personal Data controller and/or Personal Data subject.

(5) If failure in protection of Personal Data under its management occurs, Electronic System Provider must notify in writing to such Personal Data subject.

(6) Provisions on technical processing of Personal Data are addressed in accordance with provisions under laws and regulations.

Article 15

(1) Any Electronic System Provider must erase irrelevant Electronic Information and/or Electronic Document which are under its control, upon request of relevant Person.

(2) Obligation for the erasure of irrelevant Electronic Information and/or Electronic Document as referred to in paragraph (1) consists of:
a. right to erasure (*penghapusan*); and
b. right to delisting (*pengeluaran dari daftar mesin pencari*).

(3) Electronic System Provider who is obliged to erase Electronic Information and/or Electronic Document as referred to in paragraph (1) is Electronic System Provider who obtains and/or processes Personal Data under its control.

Article 16

(1) Irrelevant Electronic Information and/or Electronic Document, of which, right to erasure (*penghapusan*) is performed against, as referred to under Article 15 paragraph (2) letter a, consists of Personal Data which:
   a. is acquired and processed without consent of Personal Data subject;
   b. consent has been withdrawn by Personal Data subject;
   c. is unlawfully acquired and processed;
   d. is no longer in accordance with the acquisition purposes based on agreement and/or provisions under laws and regulations;
   e. the use has exceeded the time period in accordance with agreement and/or provisions under laws and regulations; and/or
   f. is displayed by Electronic System Provider, which inflicts losses to Personal Data subject.

(2) Obligation on the erasure of Electronic Information and/or Electronic Document as referred to in paragraph (1) does not apply in case such Electronic Information and/or Electronic Document must be stored or prohibited to be erased by Electronic System Provider in accordance with provisions under laws and regulations.

Article 17

(1) Request for the erasure of irrelevant Electronic Information and/or Electronic Document, of which, right to delisting (*pengeluaran dari daftar mesin pencari*) is performed against, as referred to under Article 15 paragraph (2) letter b, is performed based on court stipulation.

(2) Request for the stipulation on the erasure of Electronic Information and/or Electronic Document to local district court is performed by the relevant person as the Personal Data subject in accordance with provisions under laws and regulations.

(3) Request for the stipulation on the erasure as referred to in paragraph (2) should contain:
   a. identity of applicant;
   b. identity of Electronic System Provider and/or Electronic System address;
   c. irrelevant Personal Data within the control of Electronic System Provider; and

d. grounds for erasure request.

(4) In case the court grants request for the stipulation on the erasure as referred to in paragraph (2), Electronic System Provider must perform erasure of irrelevant Electronic Information and/or Electronic Document.

(5) Court stipulation as referred to in paragraph (4) becomes the basis for the erasure request of irrelevant Electronic Information and/or Electronic Document by the relevant Person to Electronic System Provider.

Article 18

(1) Any Electronic System Provider must provide erasure mechanism for irrelevant Electronic Information and/or Electronic Document in accordance with provisions under laws and regulations.

(2) Erasure mechanism as referred to in paragraph (1) at least contains provisions on:
   a. provision of communication channel between Electronic System Provider with Personal Data subject;
   b. feature on erasure of irrelevant Electronic Information and/or Electronic Document which makes possible for Personal Data subject to perform erasure of its Personal Data; and
   c. administration of erasure request of irrelevant Electronic Information and/or Electronic Document.

(3) Further provisions on erasure mechanism as referred to in paragraph (1) and paragraph (2) are addressed under Regulation of the Minister.

(4) Provisions on erasure mechanism within certain sectors may be formulated by relevant Ministry or Agency after coordinating with the Minister.

Article 19

(1) Electronic System Provider should implement good and accountable governance of Electronic Systems.

(2) Governance as referred to in paragraph (1) at least fulfill requirements on:
   a. availability of procedure or instruction for the organization of Electronic System which is documented and/or published using language, information, or symbol

that is understandable by parties relating to the organization of such Electronic System;

b. existence of sustainable mechanism to maintain the newness and clarity of implementing guideline procedure;
c. existence of institutional and completeness of supporting personnel for the proper operation of Electronic System;
d. existence of implementation of performance management in Electronic System which is organized to ensure that the Electronic System properly operates; and
e. existence of plan to maintain the sustainability of organization of Electronic System under its management.

(3) Asides from requirements as referred to in paragraph (2), relevant Ministry or Agency may determine other requirements which are established under laws and regulations.

Article 20

(1) Public Electronic System Provider must have business continuity plan to overcome interference or disaster in accordance with risks from impacts as caused.
(2) Public Electronic System Provider must perform management, processing, and/or storage of Electronic System and Electronic Data within Indonesian territories.
(3) Public Electronic System Provider may perform management, processing, and/or storage of Electronic System and Electronic Data outside Indonesian territories in case the storage technology is unavailable in domestic scope.
(4) Criteria on unavailable storage technology in domestic scope as referred to in paragraph (3) is determined by committee which is composed by ministry which organizes governmental affairs within the sector of communication and informatics, agency which is in charge for affairs on review and implementation of technology, agency which is in charge for cybersecurity affairs, and relevant Ministry or Agency.
(5) Establishment of committee as referred to in paragraph (4) is determined by the Minister.
(6) In case Public Electronic System Provider uses third-party services, the Public Electronic System Provider must perform data classification in accordance with the occurred risks.

(7) Further provisions on data classification in accordance with the risks as referred to in paragraph (6) are addressed under Regulation of the Minister.

Article 21

(1) Private Electronic System Provider may perform management, processing, and/or storage of Electronic System and Electronic Data within Indonesian territories and/or outside of Indonesian territories.
(2) In case against Electronic System and Electronic Data, management, processing, and/or storage outside of Indonesian territories are performed [*sic*], Private Electronic System Provider must ensure the effectiveness of supervision by Ministry or Agency and law enforcement.
(3) Private Electronic System Provider must provide Access to Electronic System and Electronic Data in the event of supervision and law enforcement in accordance with provisions under laws and regulations.
(4) Provisions on management, processing, and storage of Electronic System and Electronic Data for Private Electronic System Provider within financial sector are further addressed by regulatory and supervisory authority of financial sector.

Seventh Division
Security of Organization of Electronic Systems

Article 22

(1) Electronic System Provider must provide audit trail [*rekam jejak audit*] against every activity on the organization of Electronic Systems.
(2) Audit trail as referred to in paragraph (1) is used for supervisory, law enforcement, dispute resolution, verification, testing, and other examination purposes.

Article 23

Electronic System Provider must perform security against Electronic System components.

Article 24

(1) Electronic System Provider must have and carry out procedures and means for securing Electronic System in preventing interference, failure, and losses.

(2) Electronic System Provider must provide security system which covers procedures and prevention and mitigation systems of threats and attacks which cause interference, failure, and losses.

(3) In case failure or serious system interference occurs as the consequence of conduct of other party against Electronic System, Electronic System Provider must secure Electronic Information and/or Electronic Document and immediately report, in the first instance, to law enforcers and relevant Ministry of Agency.

(4) Further provisions on security system as referred to in paragraph (2) are addressed under regulation of the head of agency which performs governmental affairs within the cybersecurity sector.

Article 25

Electronic System Provider must redisplay Electronic Information and/or Electronic Document intact in accordance with format and retention period as determined based on provisions under laws and regulations.

Article 26

(1) Electronic System Provider must maintain confidentiality, integrity, authentication, accessibility, availability, and search-ability of an Electronic Information and/or Electronic Document in accordance with provisions under laws and regulations.

(2) In the course of organization of Electronic System which is designated for Electronic Information and/or Electronic Document which may be transferred, Electronic Information and/or Electronic Document should be unique and explain its possession and ownership.

Article 27

Electronic System Provider should guarantee the functionality of Electronic System in accordance with its designation, by keep regarding interoperability and compatibility with the previous Electronic System and/or related Electronic System.

Article 28

(1) Electronic System Provider must perform education toward Electronic System User.
(2) Education as referred to in paragraph (1) at least addresses rights, obligations and responsibilities of all related parties, as well as procedure for the submission of complaint.

Article 29

Electronic System Provider must convey information to Electronic System User, at least on:

a. identity of Electronic System Provider;
b. transacted object;
c. feasibility or security of Electronic System;
d. use procedures of device;
e. contract requirements;
f. procedure to reach consensus;
g. guarantee on privacy and/or Personal Data protection; and
h. complaint call center.

Article 30

(1) Electronic System Provider must provide features in accordance with the characteristics of Electronic System that is used by it.
(2) Features as referred to in paragraph (1) at least in the forms of facilities to:
    a. perform correction;
    b. cancel order;
    c. give confirmation or reconfirmation;
    d. choose to continue or stop performing next activity;

e. view information as submitted in the forms of offer of Electronic Contract or advertisement;
f. check status on the success or failure of Electronic Transaction; and
g. read agreement before performing Electronic Transaction.

Article 31

Electronic System Provider must protect its user and the general public from losses which are incurred by the Electronic System under its organization.

Article 32

(1) Any person who works within the organization of Electronic System environment must secure and protect infrastructures and facilities of Electronic System or information which is channeled through Electronic System.
(2) Electronic System Provider must provide, educate, and train personnel who are in charge and responsible for security and protection of infrastructures and facilities of Electronic System.

Article 33

For the purposes of criminal legal proceedings, Electronic System Provider must provide Electronic Information and/or Electronic Data which is contained in Electronic System or Electronic Information and/or Electronic Data which are produced by Electronic System upon valid request from investigator for certain criminal acts in accordance with authorities as addressed under the law.

Eighth Division
Electronic System Feasibility Test

Article 34

(1) Electronic System Provider must perform Electronic System Feasibility Test.
(2) Obligation as referred to in paragraph (1) may be implemented against every components or part of components in Electronic System in accordance with the

characteristics of the needs for protection and strategic nature of organization of Electronic System.

Ninth Division
Supervision

Article 35

(1) Minister is authorized to perform supervision against the organization of Electronic System.
(2) Supervision as referred to in paragraph (1) encompasses monitoring, control, examination, search, and security.
(3) Provisions on supervision of organization of Electronic System within certain sectors must be formulated by relevant Ministry or Agency after coordinating with the Minister.

CHAPTER III
ELECTRONIC AGENT PROVIDERS

First Division
Electronic Agents

Article 36

(1) Electronic System Provider may independently organize its Electronic System or through Electronic Agent.
(2) Electronic Agent as referred to in paragraph (1) is a part of Electronic System.
(3) Obligations of Electronic System Provider apply in *mutatis mutandis* manner against Electronic Agent provider.
(4) Electronic Agent may take form in:
    a. visual;
    b. audio;
    c. Electronic Data; and
    d. other forms.

Article 37

(1) Electronic Agent provider must contain or convey information to protect user's rights in Electronic Agent under its organization, at least encompasses information on:
   a. identity of Electronic Agent provider;
   b. transacted object;
   c. feasibility or security of Electronic Agent;
   d. use procedures of device;
   e. contract requirements;
   f. procedure to reach consensus;
   g. guarantee on privacy and/or Personal Data protection; and
   h. complaint call center.

(2) Electronic Agent provider must contain or provide features in the event of protecting user's rights in Electronic Agent under its organization in accordance with the characteristics of Electronic Agent that is used by it.

(3) Features as referred to in paragraph (2) may take form as facilities to:
   a. perform correction;
   b. cancel order;
   c. give confirmation or reconfirmation;
   d. choose to continue or stop performing next activity;
   e. view information as submitted in the forms of offer of Electronic Contract or advertisement;
   f. check status on the success or failure of transaction; and/or
   g. read agreement prior to the performance of transaction.

(4) Electronic Agent provider should provide features in Electronic Agent under its operation which enable its users to perform modification of information which are undergoing transaction process.

Article 38

(1) Electronic Agent may be organized for more than 1 (one) interest of Electronic System Provider that are based on agreement between the parties.

(2) Agreement as referred to in paragraph (1) should at least contain:

a. rights and obligations;
b. liability;
c. complaint mechanism and dispute resolution;
d. time period;
e. costs and fees;
f. scope of services; and
g. choice of law.

(3) In case Electronic Agent is organized for more than 1 (one) interest of Electronic System Provider, Electronic Agent provider must give equal treatment against Electronic System Provider who uses such Electronic Agent.

(4) In case Electronic Agent is organized for more than 1 (one) interest of Electronic System Provider, such Electronic Agent provider is considered as the independent Electronic System Provider.

Second Division

Obligations

Article 39

(1) In the course of organization of Electronic Agent, Electronic Agent provider should regard the principles on:
a. precautionary;
b. security and integration of Information Technology system;
c. control of security over Electronic Transaction activities;
d. cost effectiveness and efficiency; and
e. customer protection in accordance with provisions under laws and regulations.

(2) Electronic Agent provider must have and carry out standard operating procedures which fulfill principles on security control of data on user and Electronic Transaction.

(3) Principles on security control of data on user and Electronic Transaction as referred to in paragraph (2) encompass:
a. confidentiality;
b. integrity;

c. availability;
d. authentication;
e. authorization; and
f. non-repudiation [*kenirsangkalan*].

Article 40

(1) Electronic Agent provider must:
a. perform authentication testing on identity and examine authorization of Electronic System User who performs Electronic Transaction;
b. have and carry out policy and procedure to take action if there is indication on data theft;
c. ensure control on authorization and Access right to system, database, and application of Electronic Transaction;
d. prepare and carry out method and procedure to protect and/or keep confidential of data integrity, record, and information relating to Electronic Transaction;
e. have and carry out standard and control over use and protection of data if the service provider has access to such data;
f. have business continuity plan, including effective contingency plan to ensure the availability of system and service of Electronic Transaction in sustainable manner; and
g. have procedure on handling unforeseeable events, which is quick and precise to reduce the impact of an incident, fraud, and failure of Electronic System.

(2) Electronic Agent provider must prepare and determine procedure to guarantee Electronic Transaction, so that it cannot be refuted by customers.

CHAPTER IV
ORGANIZATION OF ELECTRONIC TRANSACTIONS

First Division
Scope of Organization of Electronic Transactions

Article 41

(1) Organization of Electronic Transaction may be performed within public or private scope.

(2) Organization of Electronic Transaction within public scope encompasses Organization of Electronic Transaction by:
   a. Body;
   b. institution as appointed by Body;
   c. inter-Body;
   d. among appointed institutions;
   e. between Body with appointed institution; and
   f. between Body or institution with Business in accordance with provisions under laws and regulations.

(3) Organization of Electronic Transaction within private scope encompasses Electronic Transaction:
   a. among Businesses;
   b. between Business with customer; and
   c. among individuals.

Second Division

Requirements for the Organization of Electronic Transactions

Article 42

(1) Organization of Electronic Transactions must use Digital Certificate that is issued by Indonesian Digital Certification Provider.

(2) Organization of Electronic Transactions may use Reliability Certificate.

(3) In the event of the use of Reliability Certificate as referred to in paragraph (2), Organization of Electronic Transactions must use Reliability Certificate as issued by registered Reliability Certification Agency.

Article 43

Organization of Electronic Transactions as performed by Public Electronic System Provider should give regards to the aspects of security, reliability, and efficiency.

Article 44

(1) Sender must ensure that sent Electronic Information is accurate and non-spamming [*tidak bersifat mengganggu*].
(2) Further provisions on sending of Electronic Information are addressed under Regulation of the Minister.

Third Division

Requirements for Electronic Transactions

Article 45

(1) Electronic Transaction which is performed by the parties constitutes legal consequences to the parties.
(2) Organization of Electronic Transaction which is performed by the parties should regard:
    a. good faith;
    b. precautionary principle;
    c. transparency;
    d. accountability; and
    e. reasonableness.

Article 46

(1) Electronic Transaction may be performed based on Electronic Contract or other contractual forms as a form of agreement which is performed by the parties.
(2) Electronic Contract is considered to be valid if:
    a. there is consent of the parties;
    b. performed by capable legal subjects or those who are authorized to represent in accordance with provisions under laws and regulations;

c. there is a specific subject matter; and
d. object of transaction must not be in contradictory with laws and regulations, decency, and public order.

Article 47

(1) Electronic Contract and other contractual forms as referred to under Article 46 paragraph (1) which are designated to Indonesian citizens must be made in Indonesian Language.
(2) Electronic Contract which is made using standard clause should be in accordance with provisions on standard clause as addressed under laws and regulations.
(3) Electronic Contract at least contains:
    a. data on identities of the parties;
    b. objects and specifications;
    c. Electronic Transaction requirements;
    d. price and costs;
    e. procedures in case there is annulment by the parties;
    f. provisions which grant rights to the losing party to be able to return the goods and/or request replacement of product in case of hidden defect; and
    g. choice of law for the settlement of Electronic Transaction.

Article 48

(1) Business who offers product through Electronic System should provide complete and correct information relating to requirements of contract, producer, and product which are offered.
(2) Business must provide clarity of information on offer of contract or advertisement.
(3) Business must provide time period for customer and/or acceptor of contract to return goods which are sent and/or services which are provided if they are not in conformity with the contract or there is hidden defect.
(4) Business must convey information on goods which have been sent and/or provided services.

(5) Business cannot ask customer on obligation to pay the goods which have been sent and/or services which are provided without underlying contract.

Article 49

(1) Electronic Transaction is incorporated when consent of the parties is reached.
(2) Unless addressed otherwise by the parties, consent as referred to in paragraph (1) exists when the offer of transaction which is sent by the Sender has been accepted and approved by the Acceptor.
(3) Consent as referred to in paragraph (2) may be performed through:
    a. acceptance act which states approval; or
    b. acceptance act and/or use of object by Electronic System User.

Article 50

(1) In the course of Organization of Electronic Transaction, the parties should guarantee:
    a. provision of correct data and information; and
    b. availability of means and services, as well as complaint settlement.
(2) In the course of Organization of Electronic Transaction, the parties should decide choice of law equally against the performance of Electronic Transaction.

CHAPTER V
ORGANIZATION OF DIGITAL CERTIFICATION

First Division
Digital Certificates

Article 51

(1) Electronic System Provider as referred to under Article 2 paragraph (2) must possess Digital Certificate.
(2) Electronic System User may use Digital Certificate in Electronic Transaction.
(3) In order to possess Digital Certificate, Electronic System Provider and Electronic System User should submit application to Indonesian Digital Certification Provider.

(4) If necessary, the Ministry or Agency may make it mandatory for Electronic System User to use Digital Certificate in Electronic Transaction.
(5) Further provisions on the use of Digital Certificate as referred to in paragraph (4) are addressed by Ministry or Agency.
(6) Further provisions on procedures for the possession of Digital Certificate are addressed under Regulation of the Minister.

Second Division
Digital Certification Providers

Article 52

Digital Certification Provider is authorized to perform:

a. examination of prospective owner and/or holder of Digital Certificate, issuance of Digital Certificate, extension of validity period of Digital Certificate, blocking and revocation of Digital Certificate, validation of Digital Certificate; and formulation of list of active and revoked Digital Certificate;
b. generation, verification, and validation of Digital Signature and/or other services using Digital Certificate.

Article 53

(1) Digital Certification Provider is comprised of:
    a. Indonesian Digital Certification Provider; and
    b. foreign Digital Certification Provider.
(2) Organization of Indonesian digital certification adopts single root [*satu induk*] principle.
(3) Indonesian Digital Certification Provider must obtain recognition from the Minister by rooting to the root Digital Certification Provider as organized by the Minister.
(4) Indonesian Digital Certification Provider should obtain assessment from accredited Digital Certification Provider certification agency.
(5) Foreign Digital Certification Provider operating in Indonesia should be registered in Indonesia.

(6) Further provisions on registration of foreign Digital Certification Provider as referred to in paragraph (5) are addressed under Regulation of the Minister.

Article 54

(1) Recognition of Indonesian Digital Certification Provider as referred to under Article 53 paragraph (3) is granted by the Minister after the Indonesian Digital Certification Provider fulfills requirements of recognition process as addressed under Regulation of the Minister.
(2) Recognition list of Indonesian Digital Certification Provider, including services which are provided by them, is made, maintained, and published by the Minister.
(3) Further provisions on recognition procedures for Indonesian Digital Certification Provider are addressed under Regulation of the Minister.

Article 55

(1) Indonesian Digital Certification Provider is entitled to obtain revenues by collecting service fees from Digital Certificate users.
(2) Indonesian Digital Certification Provider must deposit any revenues from service fees for the use of Digital Certificate, which are calculated from the percentage of state revenue.
(3) Revenues as referred to in paragraph (1) and paragraph (2) are non-tax state revenue.

Third Division

Supervision

Article 56

(1) Minister performs supervision against:
    a. organization of Indonesian digital certification; and
    b. foreign Digital Certification Provider.
(2) Supervision for the organization of Indonesian digital certification as referred to in paragraph (1) letter a encompasses:

a. recognition; and
b. operation of facilities of root Digital Certification Provider for Indonesian Digital Certification Provider.

(3) Further provisions on the supervision of organization of Indonesian digital certification and foreign Digital Certification Provider are addressed under Regulation of the Minister.

Fourth Division
Digital Certification Provider Services

Sub-Division 1
General

Article 57

(1) Indonesian Digital Certification Provider provides certified services.
(2) Services as referred to in paragraph (1) encompass:
a. Digital Signature; and/or
b. other services using Digital Certificate.
(3) Other services as referred to in paragraph (2) letter b encompass:
a. digital stamp;
b. electronic time stamps;
c. recorded electronic delivery services;
d. website authentication; and/or
e. preservation of Digital Signature and/or digital stamp.

Article 58

(1) Indonesian Digital Certification Provider bears losses incurred by intention or negligence against Person, Enterprise or Body because of its failure in complying with its obligations as addressed under this Regulation of the Government.

(2) Indonesian Digital Certification Provider is considered to be intentional or negligent, unless such Indonesian Digital Certification Provider is able to prove that the incurred losses occur not due to its intention or negligence.

(3) Inquisitorial liability against intention or negligence as committed by parties who are not Indonesian Digital Certification Provider becomes the liability of Person, Enterprise or Body who suffers losses.

Sub-Division 2

Digital Signature

Article 59

(1) Digital Signature which is used in Electronic Transaction may be produced through various signing procedures.

(2) In case the use of Digital Signature represents Enterprise, its Digital Signature is referred to as digital stamp.

(3) Digital Signature as referred to in paragraph (1) and paragraph (2) has valid legal power and legal consequences, provided that the following requirements are fulfilled:

a. Digital Signature Generation Data only attaches to the Signor;
b. Digital Signature Generation Data during the digital signing process only lies within the control of the Signor;
c. any modifications to Digital Signature which occur subsequent to signing period may be known;
d. any modifications to Electronic Information which are related to such Digital Signature subsequent to signing period may be known;
e. there is certain method which is used to identify who is the Signor; and
f. there is certain method to show that the Signor has provided consent against the relevant Electronic Information.

Article 60

(1) Digital Signature functions as the authentication and verification tool over:

a. identity of the Signor; and

b. integrity and authentication of Electronic Information.

(2) Digital Signature encompasses:
   a. certified Digital Signature; and
   b. non-certified Digital Signature.

(3) Certified Digital Signature as referred to in paragraph (2) letter a should:
   a. fulfill the validity of legal power and legal consequences of Digital Signature as referred to under Article 59 paragraph (3);
   b. use Digital Certificate which is created by the service of Indonesian Digital Certification Provider; and
   c. be made by using certified Digital Signature Application.

(4) Non-certified Digital Signature as referred to in paragraph (2) letter b is made without using the service of Indonesian Digital Certification Provider.

Sub-Division 3

Digital Signature Generation Data

Article 61

(1) Digital Signature Generation Data should uniquely refer only to the Signor and may be used to identify the Signor.

(2) Digital Signature Generation Data as referred to in paragraph (1) may be made by Digital Certification Provider.

(3) Digital Signature Generation Data as referred to in paragraph (1) and paragraph (2) should fulfill these provisions:
   a. if using cryptography code, Digital Signature Generation Data should not be known easily from Digital Signature verification data through certain calculation, within a certain period of time, and using reasonable tool;
   b. Digital Signature Generation Data is stored in an electronic media which is under the possession of the Signor; and
   c. data which is related to the Signor must be stored in data storage space or means, which uses trusted system as owned by Digital Certification Provider that may detect the existence of modification and fulfills these requirements:

1. only the person who is given the authority that is able to input new data, modify, exchange, or replace data;
2. information on the authentication of identity of the Signor may be checked; and
3. other technical modifications which breach security requirements may be detected or known by the provider.

d. if Digital Signature Generation Data is created by Digital Certification Provider, then the security and confidentiality of all the process for the generation of Digital Signature Generation Data are guaranteed by Digital Certification Provider;

(4) Signor must keep the confidentiality and be responsible over Digital Signature Generation Data.

Article 62

(1) During the signing process, it must be performed a mechanism to ensure that Digital Signature verification data in relation to Digital Signature Generation Data is still valid or not revoked.

(2) During the signing process, it must be performed a mechanism to ensure Digital Signature Generation Data:
   a. is not reported missing;
   b. is not reported exchanging hands to ineligible person; and
   c. is within the control of the Signor.

(3) Before signing is executed, Electronic Information which will be signed must be known and understood by the Signor.

(4) Consent of the Signor against Electronic Information which will be signed using Digital Signature must use affirmative mechanism and/or other mechanisms which show the purpose and objective of the Signor to be bound to an Electronic Transaction.

(5) Digital Signature in Electronic Information should at least:
   a. be made using Digital Signature Generation Data; and
   b. put the signing period.

(6) Modification of Digital Signature and/or Electronic Information which is signed subsequent to the signing period should be known, detected, or identified through certain method or certain way.

Article 63

(1) Signor may entrust its Digital Signature Generation Data at Digital Certification Provider.

(2) Digital Signature Generation Data as referred to in paragraph (1) may only be entrusted to Indonesian Digital Certification Provider.

(3) In case Digital Certification Provider stores Digital Signature Generation Data, Digital Certification Provider must:

a. ensure the use of Digital Signature Generation Data only within the control of the Signor;

b. use certified Digital Signature Application during the storing process of Digital Signature Generation Data; and

c. ensure mechanism that is used for the use of Digital Signature Generation Data for Digital Signature that [*sic*] implements combination of at least 2 (two) factor authentication.

(4) Provisions on certified Digital Signature Application as referred to in paragraph (3) letter b are addressed under Regulation of the Minister.

Article 64

(1) Before the Digital Signature is used, Digital Certification Provider must ensure the preliminary identification of the Signor by way of:

a. Signor submits identity to Digital Certification Provider;

b. Signor performs registration to Digital Certification Provider; and

c. if necessary, Digital Certification Provider may secretly transfer identity data of the Signor to other Digital Certification Provider based on consent of the Signor.

(2) Mechanism that is used for the use of Digital Signature Generation Data implements combination of at least 2 (two) factor authentication.

(3) Verification process of Electronic Information which is signed may be performed by examining Digital Signature verification data to search any modification of data which is signed.

Sub-Division II

Digital Stamp

Article 65

Regulation on Digital Signature applies in *mutatis mutandis* manner for the regulation of digital stamp.

Sub-Division III

Electronic Time Stamps

Article 66

Electronic time stamp services encompass:

a. certified electronic time stamp services; and
b. non-certified electronic time stamp services.

Article 67

(1) Requirements for certified electronic time stamps should fulfill the following requirements:
   a. binds date and time in Electronic Information and/or Electronic Document to prevent the possibility that the Electronic Information and/or Electronic Document is modified without being detected;
   b. refers to the accurate time source which relates to the coordinated universal time;
   c. uses Digital Certificate which is created from the service of Indonesian Digital Certification Provider; and
   d. be signed using Digital Signature or digital stamp which is organized by Indonesian Digital Certification Provider or using equivalent method.

(2) Certified electronic time stamps should provide:

a. time and date accurately; and
b. the integrity of Electronic Information and/or Electronic Document relating to said time and date.

(3) Non-certified electronic time stamp services are created without using the service of Indonesian Digital Certification Provider.

(4) Further provisions on certified electronic time stamps are addressed under Regulation of the Minister.

Sub-Division 6

Recorded Electronic Delivery Services

Article 68

Recorded electronic delivery service is comprised of:

a. certified recorded electronic delivery service; and
b. non-certified recorded electronic delivery service.

Article 69

(1) Certified Digital Certification Provider which organizes certified recorded electronic delivery service must guarantee:
   a. integrity of transmitted data;
   b. identifiable data of the Sender;
   c. identifiable data of the Acceptor; and
   d. accuracy of time and date of sending and acceptance of data.

(2) Certified recorded electronic delivery service as referred to in paragraph (1) should fulfill the following requirements at minimum:
   a. be organized by 1 (one) or more Indonesian Digital Certification Provider;
   b. able to identify the Sender accurately;
   c. able to identify Acceptor's address before the sending of data;
   d. sending and acceptance of data are secured by Digital Signature and digital stamp from Indonesian Digital Certification Provider;

e. modification of data in the process of sending or acceptance of data can be known by the Sender and Acceptor; and

f. time and date of sending, acceptance, and modification of data may be displayed using certified electronic time stamps.

(3) If the sending of data involves 2 (two) or more Indonesian Digital Certification Providers, all of the requirements as referred to in paragraph (2) apply for all involved Indonesian Digital Certification Providers.

(4) Non-certified recorded electronic delivery service is created without using the service of Indonesian Digital Certification Provider.

(5) Further provisions on recorded electronic delivery service are addressed under Regulation of the Minister.

Sub-Division V

Website Authentication

Article 70

Website authentication is comprised of:

a. certified website authentication; and

b. non-certified website authentication.

Article 71

(1) Digital Certification Provider who provides website authentication service should have reliable method which is able to identify Person or Enterprise who is responsible for the organization of website that uses website authentication service.

(2) Website authentication is aimed to guarantee the trust in transacting electronically through website.

(3) Certified website authentication should use Digital Certificate as created from the service of Indonesian Digital Certification Provider.

(4) Information which should be contained in Digital Certificate that is used for website authentication, including but not limited to:

a. name of Person, Enterprise, or Body as the website organizer;

b. address of Person, Enterprise, or Body, at least describes the city where the Person, Enterprise, or Body operates;
c. Domain Name which is operated by website organizer;
d. validity period of Digital Certificate;
e. identity of Digital Certification Provider who issues Digital Certificate; and
f. number of Digital Certificate

(5) Non-certified website authentication is created without using the service of Indonesian Digital Certification Provider.

(6) Further provisions on certified website authentication as referred to in paragraph (3) are addressed under Regulation of the Minister.

Sub-Division 8

Preservation of Digital Signature and/or Digital Stamp

Article 72

(1) Preservation of Digital Signature and/or digital stamp consists of:
a. preservation of certified Digital Signature and/or digital stamp; and
b. preservation of non-certified Digital Signature and/or digital stamp.

(2) Preservation of certified Digital Signature and/or digital stamp should fulfill the following requirements:
a. using Digital Certificate as created from the service of Indonesian Digital Certification Provider; and
b. certified Digital Signature and/or digital stamp which are contained in Electronic Information and/or Electronic Document may still be validated, even though the validity period of its Digital Signature has expired.

(3) Preservation of non-certified Digital Signature and/or digital stamp is created without using the service of Indonesian Digital Certification Provider.

(4) Further provisions on preservation of certified Digital Signature and/or digital stamp are addressed under Regulation of the Minister.

CHAPTER VI
RELIABILITY CERTIFICATION AGENCY

Article 73

(1) Business who organizes Electronic Transaction may be certified by Reliability Certification Agency.
(2) Reliability Certification Agency should be domiciled in Indonesia.
(3) Reliability Certification Agency is established by professionals.
(4) Professionals who establish Reliability Certification Agency as referred to in paragraph (3) at least encompass the following professions:
    a. Information Technology consultants;
    b. Information Technology auditors; and
    c. legal counsels within the Information Technology sector.
(5) Reliability Certification Agency should be listed in the list of Reliability Certification Agency as issued by the Minister.
(6) Further provisions on requirements for the establishment of Reliability Certification Agency are addressed under Regulation of the Minister.

Article 74

(1) Reliability Certificate is designated to protect customer in Electronic Transaction.
(2) Reliability Certificate as referred to in paragraph (1) is the guarantee that Business has fulfilled criteria as determined by Reliability Certification Agency.
(3) Business who has fulfilled criteria as referred to in paragraph (2) is entitled to use Reliability Certificate on the page and/or other Electronic Systems.

Article 75

(1) Reliability Certification Agency may issue Reliability Certificate through Reliability Certification process.
(2) Reliability Certification process as referred to in paragraph (1) encompasses examination of complete and correct information from the Business, as well as its Electronic System.

(3) Complete and correct information as referred to in paragraph (2) includes but not limited to information which:
   a. contains identity of the Business;
   b. contains privacy protection policy and procedure;
   c. contains system security policy and procedure; and
   d. contains warranty on offered goods and/or services.

Article 76

(1) Reliability Certificate which is issued by Reliability Certification Agency encompasses these categories:
   a. identity registration;
   b. security of Electronic System; and
   c. privacy policy.
(2) Fulfillment of categorization as referred to in paragraph (1) determines the Reliability Certificate level.
(3) Further provisions on regulation of Reliability Certificate level as referred to in paragraph (2) are addressed under Regulation of the Minister.

Article 77

Supervision of Reliability Certification Agency is performed by the Minister.

Article 78

(1) In order to obtain recognition of Reliability Certification Agency, administrative fees are imposed.
(2) Any revenues from administration fees as referred to in paragraph (1) are non-tax state revenue.

CHAPTER VII
MANAGEMENT OF DOMAIN NAMES

Article 79

(1) Management of Domain Name is organized by Domain Name manager.
(2) Domain Names are comprised of:
    a. generic top-level Domain Name;
    b. Indonesian top-level Domain Name;
    c. second-level Indonesian Domain Name; and
    d. derivative-level Indonesian Domain Name.
(3) Domain Name manager as referred to in paragraph (1) is comprised of:
    a. Domain Name Registry; and
    b. Domain Name Registrar.

Article 80

(1) Domain Name manager as referred to under Article 79 paragraph (3) may be organized by the Government and/or the public.
(2) The public as referred to in paragraph (1) should take form as Indonesian incorporated entity.
(3) Domain Name manager is determined by the Minister.

Article 81

(1) Domain Name Registry as referred to under Article 79 paragraph (3) letter a performs management of generic top-level Domain Name and Indonesian top-level Domain Name.
(2) Domain Name Registry may delegate authority for the registration of generic top-level Domain Name and Indonesian top-level Domain Name to Domain Name Registrar.
(3) Domain Name Registry has the functions to:
    a. provide inputs toward the regulatory plan of Domain Names to the Minister;
    b. perform supervision toward Domain Name Registrar; and
    c. resolve Domain Name disputes.

(4) Further provisions on resolution of Domain Name disputes as referred to in paragraph (3) letter c are addressed under Regulation of the Minister.

Article 82

(1) Domain Name Registrar as referred to under Article 79 paragraph (3) letter b performs management of second-level Indonesian Domain Name and derivative-level Indonesian Domain Name.
(2) Domain Name Registrar is comprised of:
    a. Body Domain Name Registrar; and
    b. non-Body Domain Name Registrar.
(3) Body Domain Name Registrar performs registration of second-level Indonesian Domain Name and derivative-level Indonesian Domain Name for the needs of the Body.
(4) Body Domain Name Registrar as referred to in paragraph (3) is performed by the Minister.
(5) For military purposes, Body Domain Name Registrar as referred to in paragraph (3) is performed by the minister who organizes governmental affairs within the defence and security sector.
(6) Non-Body Domain Name Registrar performs registration of second-level Indonesian Domain Name for commercial and non-commercial users.
(7) Non-Body Domain Name Registrar must be registered at the Minister.

Article 83

(1) Registration of Domain Name is performed based on first-to-file principle.
(2) Registered Domain Name as referred to in paragraph (1) should fulfill these requirements:
    a. be in conformity with provisions under laws and regulations;
    b. proprieties as prevailing in the society; and
    c. good faith.
(3) Domain Name Registry and Domain Name Registrar have the authorities to:

a. reject registration of Domain Name if the Domain Name fails to fulfill requirements as referred to in paragraph (2);
b. temporary deactivate the use of Domain Name; or
c. erase Domain Name if the Domain Name user violates provisions under this Regulation of the Government.

Article 84

(1) Domain Name Registry and Domain Name Registrar must organize management of Domain Name in accountable manner.
(2) In case Domain Name Registry and Domain Name Registrar intend to terminate its management, the Domain Name Registry and Domain Name Registrar must handover the whole management of Domain Name to the Minister no later than 3 (three) months prior.

Article 85

(1) Domain Name which indicates Body may only be registered and/or used by the relevant Body.
(2) Body should use Domain Name in accordance with the name of the relevant Body.

Article 86

(1) Domain Name Registry and Domain Name Registrar receive registration of Domain Name upon request from Domain Name User.
(2) Domain Name User as referred to in paragraph (1) is responsible for Domain Name as registered by it.

Article 87

(1) Domain Name Registry and/or Domain Name Registrar are entitled to receive revenues by collecting fees from registration and/or use of Domain Name from Domain Name User.
(2) In case the Domain Name Registry and Domain Name Registrar as referred to in paragraph (1) are non-Body Domain Name Registrar, the Domain Name Registry

and Domain Name Registrar must deposit a part of its revenues from registration and use of Domain Name, as calculated from the percentage of revenues, to the state.

(3) Revenues as referred to in paragraph (1) and state revenue as referred to in paragraph (2) are non-tax state revenue.

Article 88

Supervision toward management of Domain Name is performed by the Minister.

Article 89

Further provisions on requirements and procedures for the determination of Domain Name manager are addressed under Regulation of the Minister.

CHAPTER VIII
GOVERNMENTS' ROLE

Article 90

Governments' Roles in the organization of Electronic Transaction and system encompass:

a. facilitate the utilization of Information Technology and Electronic Transaction in accordance with provisions under laws and regulations;
b. protect public interests from any types of interferences as a result from the misuse of Electronic Information and Electronic Transaction which interferes public order, in accordance with provisions under laws and regulations;
c. perform prevention on the dissemination and use of Electronic Information and/or Electronic Document which contain contents that are prohibited in accordance with provisions under laws and regulations; and
d. determine Body or institution which possesses Strategic Electronic Data that must be protected.

Article 91

Governments' Roles to facilitate the utilization of Information Technology and Electronic Transaction as referred to under Article 90 letter a encompass:

a. establishment of policies;
b. enforcement of policies;
c. facilitation of infrastructures;
d. promotion and education; and
e. supervision.

Article 92

Facilitation of infrastructures as referred to under Article 91 letter c encompasses:

a. development and organization of national Electronic System gateway;
b. development and organization of Information Technology forensic facilities;
c. organization of root digital certification;
d. organization of integrated national data center and disaster recovery center in the event of organization of electronic-based governmental affairs;
e. security means to Electronic System to prevent attack toward vital information infrastructures within strategic sectors;
f. means for the deposit or storage of source code and documentation of software for Body; and
g. other means which are required to facilitate the utilization of Information Technology and Electronic Transaction based on provisions under laws and regulations.

Article 93

(1) Promotion and education as referred to under Article 91 letter d are performed by Body in accordance with its authority based on provisions under laws and regulations to realize the secure, ethical, smart, creative, productive, and innovative utilization of Information Technology and Electronic Transaction.
(2) Organization of promotion and education may involve stakeholders, including the public and/or Information Technology and Electronic Transaction activists.

Article 94

(1) Governments' Roles to protect public interests from any types of interferences as a result from the misuse of Electronic Information and Electronic Transaction which interferes public order as referred to under Article 90 letter b encompass:
   a. establishment of national cybersecurity strategies which become the part of national security strategies, including the empowerment of cybersecurity culture;
   b. regulation on information security standards;
   c. regulation on the organization of protection of vital information infrastructures;
   d. regulation on risk-management on the organization of Electronic System;
   e. regulation on human resources in the organization of protection of Electronic System;
   f. development and supervision on the organization of protection of vital information infrastructures;
   g. development and supervision of risk-management on the organization of Electronic System;
   h. development and supervision of human resources in the organization of protection of Electronic System;
   i. organization of security of Electronic Information;
   j. organization of handling of information security incidents;
   k. organization of incident-response handling; and
   l. other functions as required to protect public interests from any types of interferences.

(2) Authorities as referred to in paragraph (1) may be exercised through cooperation with other parties.

Article 95

Governments' Roles to perform prevention on the dissemination and use of Electronic Information and/or Electronic Document which contain contents that are prohibited in accordance with provisions under laws and regulations or illegal contents as referred to under Article 90 letter c take form as:

a. termination of Access; and/or

b. order to Electronic System Provider to perform termination of Access against such Electronic Information and/or Electronic Document.

Article 96

Termination of Access is performed toward Electronic Information and/or Electronic Document as referred to under Article 95 with the following classifications:

a. violate provisions under laws and regulations;
b. disturb the public and interfere public order; and
c. inform the way or provide Access to Electronic Information and/or Electronic Document which contain contents which are prohibited in accordance with provisions under laws and regulations.

Article 97

(1) The public may file request for termination of Access to Electronic Information and/or Electronic Document as referred to under Article 96 to the Minister.
(2) Related Ministry or Agency enters into coordination with the Minister for the termination of Access to Electronic Information and/or Electronic Document as referred to under Article 96.
(3) Law enforcers may request termination of Access to Electronic Information and/or Electronic Document as referred to under Article 96 to the Minister.
(4) Judiciary agencies may order termination of Access to Electronic Information and/or Electronic Document as referred to under Article 96 to the Minister.
(5) Provisions on procedures for the request for termination of Access as referred to in paragraph (1) up to paragraph (4) are addressed under Regulation of the Minister.

Article 98

(1) Electronic System Provider must perform termination of Access to Electronic Information and/or Electronic Document as referred to under Article 96.
(2) Electronic System Provider as referred to in paragraph (1) encompasses the internet Access service provider, network and telecommunication service provider, content

provider, and link provider, who provide Electronic Information and/or Electronic Document traffic networks.

(3) Electronic System Provider who fails to perform termination of Access may be attributed with liability based on provisions under laws and regulations.

(4) Further provisions on the implementation of obligation on termination of Access as referred to in paragraph (1) are addressed under Regulation of the Minister.

Article 99

(1) Government determines Body or institution which possesses strategic electronic data that must be protected.

(2) Body or institution which possesses strategic Electronic Data that must be protected as referred to in paragraph (1), encompasses:

a. the sector of governmental administration;
b. the sector of energy and mineral resources;
c. the sector of transportation;
d. the sector of finance;
e. the sector of health;
f. the sector of information technology and communication;
g. the sector of food;
h. the sector of defence; and
i. other sectors as determined by the President.

(3) Body or institution which possesses strategic Electronic Data as referred to in paragraph (1) should create Electronic Document and its electronic backup record and connects it to certain data center for data security purposes.

(4) Further provisions on obligation to create Electronic Document and its electronic backup record and connects it to certain data center as referred to in paragraph (3) are addressed under regulation of the head of agency which is in charge for cybersecurity affairs.

CHAPTER IX
ADMINISTRATIVE SANCTIONS

Article 100

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

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

(3) Administrative sanctions are handed down by the Minister in accordance with provisions under laws and regulations.

(4) Imposition of administrative sanctions as referred to in paragraph (2) letter c and letter d is performed through coordination with the heads of relevant Ministry and/or Agency.

(5) Imposition of administrative sanctions as referred to in paragraph (2) and paragraph (3) does not eliminate any criminal and civil liabilities.

Article 101

Further provisions on procedures for the imposition of administrative sanctions and filing of objection against the imposition of administrative sanctions are addressed under Regulation of the Minister.

CHAPTER X
TRANSITIONAL PROVISIONS

Article 102

(1) When this Regulation of the Government enters into force, Electronic System Provider who has been in operation prior to the promulgation of this Regulation of the Government, must make adjustments with provisions under Article 6 paragraph (1) within a time period of 1 (one) year.

(2) When this Regulation of the Government enters into force, Public Electronic System Provider which has been in operation prior to the promulgation of this Regulation of the Government, must make adjustments with provisions under Article 20 paragraph (2) within a time period of 2 (two) years.

CHAPTER XI
FINAL PROVISIONS

Article 103

(1) When this Regulation of the Government enters into force, implementing regulations of Regulation of the Government Number 82 of 2012 on Organization of Electronic Systems and Transactions are declared to be valid insofar that they are not in contradictory or yet replaced with the new one based on this Regulation of the Government.

(2) When this Regulation of the Government enters into force, Regulation of the Government Number 82 of 2012 on Organization of Electronic Systems and Transactions (State Gazette of the Republic of Indonesia of 2012 Number 189, Supplement to the State Gazette Number 5348) is revoked and declared invalid.

Article 104

This Regulation of the Government enters into force on promulgation date.

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

Enacted in Jakarta
on 4 October 2019

PRESIDENT OF THE REPUBLIC OF INDONESIA,
signed
JOKO WIDODO

Promulgated in Jakarta
on 10 October 2019

Acting MINISTER OF LAW AND HUMAN RIGHTS
OF THE REPUBLIC OF INDONESIA,
signed.
TJAHJO KUMOLO

STATE GAZETTE OF THE REPUBLIC OF INDONESIA OF 2019 NUMBER 185

ELUCIDATION OF

REGULATION OF THE GOVERNMENT OF THE REPUBLIC OF INDONESIA

NUMBER 71 OF 2019

ON

ORGANIZATION OF ELECTRONIC SYSTEMS AND TRANSACTIONS

I. GENERAL

A number of provisions under the Law Number 11 of 2008 on Electronic Information and Transactions mandate further regulation under Regulation of the Government, namely regulation on Reliability Certification Agency, Digital Signature, Digital Certification Provider, Electronic System Provider, Organization of Electronic Transaction, Electronic Agent provider, and management of Domain Name have been addressed under Regulation of the Government Number 82 of 2012 on Organization of Electronic Systems and Transactions, it is deemed necessary to be adjusted with technology development and public needs.

Establishment of this Regulation of the Government is also intended to further address several provisions under Law Number 19 of 2016 on Amendment to Law Number 11 of 2008 on Electronic Information and Transactions as established to ensure the recognition and respect toward rights and freedoms of other people and to fulfill fair demands in accordance with considerations on security and public interest within a democratized society. Several provisions which are required to be further addressed are:

a. obligations for any Electronic System Provider to erase irrelevant Electronic Information and/or Electronic Document which are under its control upon request of the relevant Person based on court stipulation; and
b. Government's roles in facilitating the utilization of Information Technology and Electronic Transaction, protect public interest from any types of interferences as a result of misuse of Electronic Information and Electronic Transaction which interrupts the public interest, and prevent the dissemination and use of Electronic

Information and/or Electronic Document which contain contents as prohibited in accordance with provisions under laws and regulations.

Material scope under this Regulation of the Government encompasses:

a. category of Electronic System Provider;
b. obligations of Electronic System Provider;
c. erasure and/or termination of Access to irrelevant Electronic Information and/or Electronic Document;
d. placement of Electronic System and Electronic Data;
e. supervision of organization of Electronic System;
f. organization of Electronic Agent;
g. Organization of Electronic Transaction;
h. organization of Digital Certification;
i. management of Domain Names;
j. Government's roles in the organization of Electronic Systems and Transactions; and
k. administrative sanctions.

II. ARTICLE BY ARTICLE

Article 1

Self-explanatory.

Article 2

Paragraph (1)

Self-explanatory.

Paragraph (2)

Self-explanatory.

Paragraph (3)

Letter a

Self-explanatory.

Letter b

"Institution as appointed by the Body" refers to institution which performs organization of public Electronic System on behalf of appointing Body.

Paragraph (4)

"Regulatory and supervisory authority of financial sector", *inter alia*, authority within the sectors of monetary, payment system, macro-prudential, banking, capital market, as well as insurance, pension fund, financing agency, and other financial-services agencies.

Paragraph (5)

Letter a

Self-explanatory.

Letter b

"Electronic System Provider who owns online portal, sites, or application through the internet" refers to Electronic System Provider whose Electronic System is used within Indonesian territories, and/or offered within Indonesian territories.

Point 1

Self-explanatory.

Point 2

Self-explanatory.

Point 3

Self-explanatory.

Point 4

Self-explanatory.

Point 5

Self-explanatory.

Point 6

Processing of Personal Data encompasses acquisition and collection, processing and analysis, rectification and update, display, publication, transfer, dissemination, or disclosure, and/or erasure or destruction of Personal Data.

Article 3

Paragraph (1)

"Reliable" denotes that Electronic System has the capabilities in accordance with the needs of its use.

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

"Proper operation" denotes that Electronic System has the capabilities in accordance with its specifications.

Paragraph (2)

"Responsible" denotes that Electronic System Provider who is legally held responsible against the organization of such Electronic System.

Paragraph (3)

Self-explanatory.

Article 4

Self-explanatory.

Article 5

Self-explanatory.

Article 6

Self-explanatory.

Article 7

Paragraph (1)

Letter a

"Interconnectivity" refers to the ability to be connected to one another, so that it can function properly. Interconnectivity covers the interoperability ability.

"Compatibility" refers to the conformity between one Electronic System with another Electronic System.

Letter b

Self-explanatory.

Letter c

Self-explanatory.

Paragraph (2)

Certification evidence may be obtained through accredited third parties in Indonesia or other supporting evidences as the supporting evidence [*sic*] that declares the fulfillment of requirements from certification agency outside of Indonesia.

Article 8

Letter a

"Be guaranteed the security and reliability of proper operation" refers to Electronic System Provider guarantees Software does not contain instruction other than it should be or hidden instruction which is illegal (malicious code), such as time bomb instruction, virus program, trojan, worm, and backdoor. This safety may be performed by checking the source code.

Letter b

Self-explanatory.

Article 9

Paragraph (1)

"Source code" refers to a set of orders, statements, and/or declarations which are written in computer programming code that may be read and understood by person.

Paragraph (2)

Self-explanatory.

Paragraph (3)

"Trusted third party as the source code escrow (*penyimpan kode sumber*)" refers to profession or independent party who is competent in organizing escrow services for source codes of computer programs or Software so that

source codes may be accessed, obtained, or handed over from provider to the users.

Paragraph (4)

Self-explanatory.

Paragraph (5)

Self-explanatory.

Paragraph (6)

Self-explanatory.

Article 10

Paragraph (1)

"Experts" refer to workforces who have special knowledge and skill within the Electronic System sector that may be held accountable both academically and practically.

Paragraph (2)

Self-explanatory.

Article 11

Paragraph (1)

Letter a

"Service level agreement (*perjanjian tingkat layanan*)" refers to statement on service quality level of an Electronic System.

Letter b

Self-explanatory.

Letter c

Self-explanatory.

Paragraph (2)

Self-explanatory.

Article 12

"Implement risk management" refers to performing risk analysis and formulating mitigation measures and countermeasures to overcome threats, interferences, and obstacles against Electronic System under its management.

Article 13

"Governance policies" refer to, *inter alia*, including policy on activities to develop organizational structure, business process (*proses bisnis*), and performance management, as well as recruitment of supporting personnel for the operation of Electronic System to ensure the Electronic System is able to operate properly.

Article 14

Paragraph (1)

Self-explanatory.

Paragraph (2)

Self-explanatory.

Paragraph (3)

"Lawful consent" refers to consent that is explicitly expressed, cannot be hidden or based on mistake, negligence, or duress.

Paragraph (4)

Letter a

Self-explanatory.

Letter b

Self-explanatory.

Letter c

"Vital interest (*kepentingan yang sah*)" refers to needs/necessity to protect a very important matter on the existence of a person.

Letter d

Self-explanatory.

Letter e

Self-explanatory.

Letter f

Self-explanatory.

Paragraph (5)

Self-explanatory.

Paragraph (6)

Self-explanatory.

Article 15

Paragraph (1)

Self-explanatory.

Paragraph (2)

Letter a

Self-explanatory.

Letter b

Obligation for right to delisting (*mengeluarkan dari daftar mesin pencari*) encompasses Electronic System Provider who operates search engine to erase the display and/or terminate Access to such irrelevant Electronic Information and/or Electronic Document based on court stipulation.

Paragraph (3)

Self-explanatory.

Article 16

Self-explanatory.

Article 17

Self-explanatory.

Article 18

Self-explanatory.

Article 19

Paragraph (1)

Good Electronic System governance (IT Governance) encompasses planning, implementation, operation, maintenance, and documentation processes.

Paragraph (2)

Self-explanatory.

Paragraph (3)

Self-explanatory.

Article 20

Paragraph (1)

"Business continuity plan (*rencana keberlangsungan kegiatan*)" refers to a set of processes which are performed to ensure the continuity of businesses in a condition of undergoing interference or disaster.

Paragraph (2)

Self-explanatory.

Paragraph (3)

Self-explanatory.

Paragraph (4)

Self-explanatory.

Paragraph (5)

Self-explanatory.

Paragraph (6)

Self-explanatory.

Paragraph (7)

Self-explanatory.

Article 21

Self-explanatory.

Article 22

Paragraph (1)

Audit trail (*rekam jejak audit*) mechanism encompasses:

a. maintain transaction log in accordance with data retention policy of provider, in accordance with provisions under laws and regulations;
b. give notification to customers if a transaction has been successfully performed;
c. ensure the availability of audit trail function to be able to detect attempt and/or the occurrence of intrusion which should be reviewed or evaluated periodically; and
d. in case the processing and audit trail system are responsibility of third parties, then said audit trail process should be in accordance with standards as determined by the Electronic System Provider.

Paragraph (2)

"Other examination" refers to, *inter alia*, examination for the purpose of mitigation or incident response (*penanganan tanggap darurat*).

Article 23

Components of Electronic System are comprised of:

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

Article 24

Paragraph (1)

"Interference" refers to any acts which are destructive or having serious impact to Electronic System, so that such Electronic System does not operate properly.

"Failure" refers to partial or whole stoppage of essential Electronic System functions, so that the Electronic System does not function properly.

"Losses" refers to consequences from the malfunction of Electronic System which has legal consequences for users, providers, and other third parties, either materially or immaterially.

Paragraph (2)

"Prevention and mitigation systems" refer to, *inter alia*, antivirus, anti-spamming, firewall, intrusion detection, prevention system, and/or management of information security management system.

Paragraph (3)

Self-explanatory.

Paragraph (4)

Self-explanatory.

Article 25

Self-explanatory.

Article 26

Paragraph (1)

Self-explanatory.

Paragraph (2)

"Electronic Information and/or Electronic Document which may be transferred" refers to commercial paper or commercial paper in electronic form.

"Electronic Information and/or Electronic Document should be unique" refers to Electronic Information and/or Electronic Document and/or recordation of such Electronic Information and/or Electronic Document is the only one that represents a certain value.

"Electronic Information and/or Electronic Document should explain possession" denotes that such Electronic Information and/or Electronic Document should explain the possession nature that is represented by control system or recordation system of the relevant Electronic Information and/or Electronic Document.

"Electronic Information and/or Electronic Document should explain its ownership" denotes that such Electronic Information and/or Electronic Document should explain the ownership nature that is represented by the existence of technology control mean which guarantees that there is only a single authoritative copy (*satu salinan yang sah*) and does not change.

Article 27

"Interoperability" refers to the capability of different Electronic Systems to operate in integration.

"Compatibility" refers to the conformity of one Electronic System with another Electronic System.

Article 28

Paragraph (1)

Self-explanatory.

Paragraph (2)

Education which may be conveyed to Electronic System User, *inter alia*:

a. convey to the Electronic System User on the importance of protecting security of Personal Identification Number (PIN)/password, for instance:
    1. keep confidential and does not tell PIN/password to anyone, including to the officers of the provider;
    2. change PIN/password periodically;
    3. use PIN/password which is not easily guessed, such as the use of personal identity in the forms of date of birth;
    4. do not take note of PIN/password; and
    5. PIN/password for one product should be different from PIN/password of other products.
b. convey to Electronic System User on various criminal modes on Electronic Transaction; and
c. convey to Electronic System User on procedures and processes for filing of claims.

Article 29

Obligation to convey information to Electronic System User is intended to protect the interests of Electronic System User.

Article 30

Paragraph (1)

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

Paragraph (2)

Self-explanatory.

Article 31

Self-explanatory.

Article 32

Self-explanatory.

Article 33

Self-explanatory.

Article 34

Self-explanatory.

Article 35

Self-explanatory.

Article 36

Paragraph (1)

Self-explanatory.

Paragraph (2)

Self-explanatory.

Paragraph (3)

Self-explanatory.

Paragraph (4)

Letter a

"Visual form" refers to display which may be viewed or read, *inter alia*, graphic display of a website.

Letter b

"Audio form" refers to anything which can be heard, *Inter alia*, telemarketing services.

Letter c

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

Electronic data capture (EDC) is Electronic Agent for and on behalf of Electronic System Provider who enters into cooperation with network provider. EDC may be used independently by bank financial agency and/or jointly with other financial or non-financial agency.

In case Electronic Transaction is performed by using card of Bank X at EDC owned by Bank Y, then Bank Y will forward said transaction to Bank X, through such network provider.

Letter d

Self-explanatory.

Article 37

Paragraph (1)

Letter a

Information on identity of Electronic Agent provider at least contains logo or name which shows 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.

Paragraph (2)

Self-explanatory.

Paragraph (3)

Self-explanatory.

Paragraph (4)

Self-explanatory.

Article 38

Paragraph (1)

Self-explanatory.

Paragraph (2)

Self-explanatory.

Paragraph (3)

"Equal treatment" refers to, *inter alia*, imposition of equal tariffs, facilities, requirements, and procedures.

Paragraph (4)

Self-explanatory.

Article 39

Paragraph (1)

Self-explanatory.

Paragraph (2)

Self-explanatory.

Paragraph (3)

Letter a

"Confidentiality" is in accordance with the legal concept on confidentiality (*kerahasiaan*) of electronic information and communication.

Letter b

"Integrity" is in accordance with the legal concept on integrity (*keutuhan*) of Electronic Information.

Letter c

"Availability" is in accordance with the legal concept on availability (*ketersediaan*) of Electronic Information.

Letter d

"Authentication" is in accordance with the legal concept on authentication (*keautentikan*) which covers the originality (*keaslian*) of content of an Electronic Information.

Letter e

"Authorization" is in accordance with the legal concept on authorization (*otorisasi*) based on the scope of duties and functions within an organization and management.

Letter f

"Non-repudiation" is in accordance with the legal concept on non-repudiation (*nirsangkal*).

Article 40

Paragraph (1)

Letter a

In the course of performing authentication testing on identity and examination on authorization of Electronic System User, the following matters should be regarded, *inter alia*:

1. written policies and procedures to ensure the ability to test the authentication of identity and examine the authority of Electronic System User;
2. method to test the authentication; and
3. combination of at least 2 (two) factor authentication (*dua faktor autentikasi*), namely “what you know” (PIN/password), “what you have” (magnetic card with chip, token, digital signature), “what you are” or “biometric” (retina and fingerprint).

Letter b

Self-explanatory.

Letter c

Self-explanatory.

Letter d

Protection of confidentiality of Personal Data of Electronic System User should also be fulfilled in case the provider uses outsourcing services (*jasa pihak lain*).

Letter e

Self-explanatory.

Letter f

Self-explanatory.

Letter g

Handling procedures on unforeseeable events should also be fulfilled in case the provider uses outsourcing (*pihak lain*) services.

Paragraph (2)

In preparing and determining procedures to guarantee Electronic Transaction, so that it cannot be refuted by customer, regards should be given to:

a. Electronic Transaction system which has been designed to reduce the possibilities on the performance of unintended (*tidak sengaja*) transactions by eligible users;
b. every identities of parties who perform transaction have been tested for its authentication or originality; and
c. data on financial transaction is protected from possibility of modification and any modification may be detected.

Article 41

Self-explanatory.

Article 42

Self-explanatory.

Article 43

Self-explanatory.

Article 44

Paragraph (1)

This provision is intended to protect Electronic System User from the delivery of Electronic Information which is spam (*mengganggu*) in nature.

Spam forms which are generally known are e-mail spam, instant messaging spam, usenet newsgroup spam, web search engine spam (*spam mesin pencari informasi web*), blog spam, news spam on cellphone, and Internet forum spam.

Paragraph (2)

Self-explanatory.

Article 45

Paragraph (1)

Self-explanatory.

Paragraph (2)

Letter a

Self-explanatory.

Letter b

Self-explanatory.

Letter c

Self-explanatory.

Letter d

Self-explanatory.

Letter e

"Reasonableness" refers to propriety element which applies in accordance with developed business customs or practices.

Article 46

Paragraph (1)

Electronic Transactions may encompass several forms or variants, *inter alia*:

a. agreement is not performed electronically, but the performance of contractual relationship is settled electronically;
b. agreement is performed electronically and performance of contractual relationship is settled electronically; and
c. agreement is performed electronically and performance of contractual relationship is settled non-electronically.

Paragraph (2)

Self-explanatory.

Article 47

Paragraph (1)

Self-explanatory.

Paragraph (2)

"Laws and regulations" refer to, *inter alia*, Law on Customer Protection.

Paragraph (3)

Self-explanatory.

Article 48

Paragraph (1)

"Complete and correct information" encompasses:

a. information which contains identity, as well as status of legal subject and its competence, either as producer, supplier, provider or intermediary;
b. other information which explains certain matters which become the prerequisite for the validity of agreement, as well as explain offered goods and/or services, such as name, address, and description of goods/services.

"Contract" covers agreement or cooperation.

Paragraph (2)

Self-explanatory.

Paragraph (3)

Self-explanatory.

Paragraph (4)

Self-explanatory.

Paragraph (5)

Self-explanatory.

Article 49

Paragraph (1)

Self-explanatory.

Paragraph (2)

Electronic Transaction incorporates when agreement between the parties, which may take form as checking of data, identity, personal identification number (*nomor identifikasi pribadi*/PIN) or password (*sandi lewat*/*kata sandi*).

Paragraph (3)

Letter a

"Acceptance act which states approval", *inter alia*, by clicking the agreement electronically by Electronic System User.

Letter b

Self-explanatory.

Article 50

Paragraph (1)

Self-explanatory.

Paragraph (2)

"Equally" refers to consideration of interests of both parties in fair (*adil*) manner.

Article 51

Paragraph (1)

Obligation to use Digital Certificate is specifically for SSL Encryption.

Paragraph (2)

Self-explanatory.

Paragraph (3)

Possession of Digital Certificate is one of the measures to increase security on the organization of Electronic System asides from other security measures.

Ownership of Digital Certificate has the function to support the security on the organization of Electronic System which encompasses, *inter alia*, confidentiality, authentication, integrity, and non-repudiation (*kenirsangkalan*).

Paragraph (4)

Self-explanatory.

Paragraph (5)

Self-explanatory.

Paragraph (6)

Regulation of the Minister addresses, *inter alia*, regulation on procedures to submit digital certification application which is submitted through Digital Certification Provider or Registration Authority (*otoritas pendaftaran*) which is appointed by the Digital Certification Provider.

Article 52

Letter a

"Examination" refers to examination on the physical existence of prospective certificate owner, may be performed electronically online if the examination uses biometric.

Letter b

Digital Signature refers to agreement of Electronic Information and/or Electronic Document which is performed by individual or individual who represents Enterprise or Body.

Article 53

Paragraph (1)

Letter a

"Indonesian Digital Certification Provider" refers to Digital Certification Provider who obtains certification, so that supervision on its organization may be performed, as well as to become the differentiator that Indonesian Digital Certification Provider may act as trusted third party which becomes the guarantor on the originality of digital identity.

Letter b

Self-explanatory.

Paragraph (2)

"Single root principle" refers to Indonesian Digital Certification Provider who roots with root Digital Certification Provider which is organized by the Minister and its certificate is signed using root Digital Certification Provider's certificate.

Paragraph (3)

Self-explanatory.

Paragraph (4)

Self-explanatory.

Paragraph (5)

"Registered" does not refer to register as Indonesian Enterprise, instead register its company as foreign Digital Certification Provider to the Minister.

Paragraph (6)

Self-explanatory.

Article 54

Self-explanatory.

Article 55

Self-explanatory.

Article 56

Self-explanatory.

Article 57

Paragraph (1)

Self-explanatory.

Paragraph (2)

Self-explanatory.

Paragraph (3)

Letter a

Digital stamp is Digital Signature which is used by Enterprise or Body to guarantee the originality and integrity of an Electronic Information and/or Electronic Document.

Letter b

Electronic time stamp is stamp which binds between time and date with Electronic Information and/or Electronic Document by using the reliable method.

Letter c

Recorded electronic delivery service is service which provides delivery of Electronic Information and/or Electronic Document and provides evidence relating to delivery of Electronic Information and/or Electronic Document

and protects Electronic Information and/or Electronic Document which is delivered, from the risks of lost, stolen, damaged, or unlawful modification.

Letter d

Website authentication is service which identifies the website owner and connect such website to Person or Enterprise who receives website's Digital Certificate by using reliable method.

Letter e

Preservation of Digital Signature and/or digital stamp is service which guarantees the legal power of Digital Signature and digital stamp within an Electronic Information and/or Electronic Document may still be validated, although the validity period of its Digital Certificate has expired.

Article 58

Paragraph (1)

If Indonesian Digital Certification Provider enters into cooperation with other Digital Certification Provider for the organization of a part of its infrastructures or services, then losses or negligence which occurs still become the liability of Indonesian Digital Certification Provider.

Paragraph (2)

Self-explanatory.

Paragraph (3)

Self-explanatory.

Article 59

Self-explanatory.

Article 60

Paragraph (1)

Digital Signature has the function similar to conventional signature in terms of representing identity of the Signor.

In terms of authentication (*pembuktian keaslian*) of conventional signature, it may be performed through verification or examination of Digital Signature specimen of the Signor.

For Digital Signature, Digital Signature Generation Data has the role as Digital Signature specimen of the Signor.

Digital Signature should be usable by competent experts to perform examination and inquisitorial that the Electronic Information which is signed by such Digital Signature does not experience any modification after being signed.

Paragraph (2)

Legal consequences from the use of certified or non-certified Digital Signature affects the power of inquisitorial value [*kekuatan nilai pembuktian*].

Paragraph (3)

Self-explanatory.

Paragraph (4)

Self-explanatory.

Article 61

Paragraph (1)

"Unique" refers to any code, regardless of its type, which is used or functioned as Digital Signature Generation Data, should refer to only a single legal subject or single entity who represents single identity.

Paragraph (2)

Self-explanatory.

Paragraph (3)

Letter a

Digital Signature Generation Data which is produced using cryptography technique generally has mathematical correlation based on probability with Digital Signature verification data. Hence, the choosing of cryptography code which will be used should consider the adequacy of difficulty level which is encountered and resources which must be prepared by the party who attempts to forge Digital Signature Generation Data.

Letter b

"Electronic media" refers to facilities, means, or devices which are used to collect, store, process, and/or disseminate Electronic Information that is used temporarily or permanently.

Letter c

"Data which is related to the Signor" refers to all data which may be used to identify the identity of the Signor, such as name, address, place and date of birth, as well as specimen code of conventional signature.

"Trusted system" refers to system which follows procedures for the use of Digital Signature which ensure the authenticity and integrity of Electronic Information. Such matter may be seen by considering several factors, *inter alia*:

1. finance and resources;
2. quality of Hardware and Software;
3. procedures for certificate and application, as well as data retention;
4. availability of Digital Signature Generation Data; and
5. audit by independent agency.

Letter d

Self-explanatory.

Paragraph (4)

Self-explanatory.

Article 62

Paragraph (1)

Self-explanatory.

Paragraph (2)

Self-explanatory.

Paragraph (3)

Self-explanatory.

Paragraph (4)

Self-explanatory.

Paragraph (5)

Self-explanatory.

Paragraph (6)

Examples of this provision are as follows:

a. Modification to Digital Signature after the signing period should cause the Electronic Information, as it is affixed to, does not function properly, damaged, or cannot be displayed if the Digital Signature is affixed and/or bound to Electronic Information which is signed. The technique of affixing and binding Digital Signature to Electronic Information which is signed may cause the occurrence of new Electronic Information or Electronic Document which:
    1. is seen as a whole which cannot be separated; or
    2. looks separate and Electronic Information which is signed may be read by commoners, while the Digital Signature takes form as code and/or image.
b. Modification to Digital Signature after the Signing period should cause a part or the whole Electronic Information to be invalid or not applicable if the Digital Signature is logically associated with Electronic Information which is signed by it. Modification which occurs against Electronic Information which is signed should cause inconformity between Digital Signature with the related Electronic Information that can be clearly seen through verification mechanism.

Article 63

Self-explanatory.

Article 64

Paragraph (1)

Self-explanatory.

Paragraph (2)

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

a. something that is owned individually (what you have), such as ATM card or smart card;
b. something that is known individually (what you know), such as PIN/password or cryptography key; and
c. something that is trait/characteristic of an individual (what you are), such as voice pattern (*pola suara*), handwriting dynamics (*dinamika tulisan tangan*), or fingerprint (*sidik jari*).

Paragraph (3)

Self-explanatory.

Article 65

Self-explanatory.

Article 66

Self-explanatory.

Article 67

Self-explanatory.

Article 68

Self-explanatory.

Article 69

Self-explanatory.

Article 70

Self-explanatory.

Article 71

Paragraph (1)

Self-explanatory.

Paragraph (2)

Self-explanatory.

Paragraph (3)

Self-explanatory.

Paragraph (4)

Letter a

Self-explanatory.

Letter b

"Address" refers to at least the description on the city as domicile where person or Enterprise operates.

Letter c

Self-explanatory.

Letter d

Self-explanatory.

Letter e

Self-explanatory.

Letter f

Self-explanatory.

Paragraph (5)

Self-explanatory.

Paragraph (6)

Self-explanatory.

Article 72

Self-explanatory.

Article 73

Paragraph (1)

Self-explanatory.

Paragraph (2)

Self-explanatory.

Paragraph (3)

Self-explanatory.

Paragraph (4)

Letter a

Information Technology Consultant encompasses information security profession.

Letter b

Self-explanatory.

Letter c

Self-explanatory.

Paragraph (5)

Self-explanatory.

Paragraph (6)

Self-explanatory.

Article 74

Self-explanatory.

Article 75

Self-explanatory.

Article 76

Paragraph (1)

letter a

Identity registration refers to Reliability Certificate which reliability guarantee is limited to security that the identity of Business is correct.

Validation which is performed by Reliability Certification Agency is only toward identity of Business which at least contains name of legal subject, status of legal subject, address or domicile, phone number, email address, business license, and Taxpayer Identification Number (*Nomor Pokok Wajib Pajak* – NPWP).

Reliability Certification Agency which issues this Reliability Certificate gives search certainty that identity of the Business is correct.

letter b

Security of Electronic System refers to Reliability Certificate which reliability guarantee gives certainty that the delivery and data exchange process through Actor's website.

Security of business is protected by using data exchange process security technology, such as SSL/secure socket layer protocol.

This Reliability Certificate guarantees that there is security system in tested data exchange process.

Vulnerability seal (*pengamanan terhadap kerawanan*) refers to Reliability Certificate which reliability guarantee gives certainty that there is information security management that is implemented by Business by referring to certain Electronic System security standards based on provisions under laws and regulations.

letter c

Privacy policy refers to Reliability Certificate which reliability guarantee gives certainty that the confidentiality of customers' Personal Data is protected properly.

Paragraph (2)

Self-explanatory.

Paragraph (3)

Self-explanatory.

Article 77

Self-explanatory.

Article 78

Self-explanatory.

Article 79

Paragraph (1)

Self-explanatory.

Paragraph (2)

Letter a

"Generic top-level Domain Name" refers to top-level Domain Name which is comprised of three or more characters in hierarchy of domain naming system other than country code Top Level Domain (*domain tingkat tinggi negara*). For example ".nusantara" or ".java".

Letter b

"Indonesian top-level Domain Name" refers to top-level domain in the hierarchy of domain naming system which shows Indonesian code (.id) in accordance with the country code list in ISO 3166-1 which is used and recognized by Internet Assigned Numbers Authority (IANA).

Letter c

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

Letter d

Examples of derivative-level Indonesian Domain Name is kominfo.go.id.

Paragraph (3)

Letter a

These are included within the scope of definition of Domain Name Registry, namely function and role of 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" refers to, *inter alia*, Indonesia National Single Window (INSW) and electronically-integrated business licensing services (online single submission).

Letter b

Self-explanatory.

Letter c

Self-explanatory.

Letter d

Organization of integrated national data center and disaster recovery center is designated for public application and Strategic Electronic Data.

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

"Violate provisions under laws and regulations" refers to, *inter alia*, Electronic Information and/or Electronic Document which contain the elements of pornography, gambling, slander and/or defamation, fraud, hate against ethnicity, religion, race, and inter-group relations (*suku, agama, ras, dan antargolongan* – SARA), violence and/or child violence, intellectual property infringement, violation of trading of goods and services through electronic system, terrorism and/or radicalism, separatism and/or prohibited dangerous organization, breach of information security, violation to customer protection, violation in health sector, violation of drug and food supervision.

Letter b

"Disturb the public and/or interfere public order" refers to, *inter alia*, information and facts which are hoaxed.

Letter c

Self-explanatory.

Article 97

Self-explanatory.

Article 98

Paragraph (1)

"Termination of Access" refers to, *inter alia*, blocking of Access, deletion of account, and/or erasure of content.

Paragraph (2)

Self-explanatory.

Paragraph (3)

Self-explanatory.

Paragraph (4)

Self-explanatory.

Article 99

Paragraph (1)

"Body or institution which possesses strategic Electronic Data" refers to Body or institution which has vital information infrastructures within the determined sector.

Paragraph (2)

Self-explanatory.

Paragraph (3)

Interconnectedness to certain data center for data security purposes is performed in case there is incident which must be reported to agency which is in charge for cybersecurity affairs.

Paragraph (4)

Self-explanatory.

Article 100

Paragraph (1)

Imposition of sanction under this provision is only designated for parties who commit administrative sanctions, while imposition of violations which are moral or civil in nature are not imposed with administrative sanctions.

Paragraph (2)

Letter a

Self-explanatory.

Letter b

Self-explanatory.

Letter c

"Temporary suspension" refers to partial or whole suspension of components or services of the relevant Electronic System for a certain period of time.

Letter d

"Termination of Access" refers to, *inter alia*, blocking of Access, deletion of account, and/or erasure of content.

Letter e

Self-explanatory.

Paragraph (3)

Self-explanatory.

Paragraph (4)

Self-explanatory.

Paragraph (5)

Self-explanatory.

Article 101

Self-explanatory.

Article 102

Self-explanatory.

Article 103

Self-explanatory.

Article 104

Self-explanatory.

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

Translator's Notes for 2nd Edition

Terms	Previous	Current
Pengguna Sistem Elektronik	Electronic System User	Subscriber