

DRAFT
REGULATION OF THE GOVERNMENT OF THE REPUBLIC OF INDONESIA
NUMBER OF
ON
THE AMENDMENT TO REGULATION OF THE GOVERNMENT NUMBER 82 OF 2012 ON THE
ORGANIZATION OF ELECTRONIC SYSTEMS AND TRANSACTIONS

BY THE GRACE OF GOD ALMIGHTY

THE PRESIDENT OF THE REPUBLIC OF INDONESIA,

Considering:

- a. that with the rapid development of information technology and to enforce state sovereignty over electronic information in the territory of the Unified Nation of the Republic of Indonesia, it has been deemed necessary to adjust the regulation on the organization of electronic systems and transactions;
- b. that to implement the provisions of Article 26 paragraph (5) and Article 40 paragraph (6) of Law Number 19 of 2016 on the Amendment to Law Number 11 of 2008 on Electronic Information and Transactions, it has been deemed necessary to make changes to several provisions set out in Regulation of the Government Number 82 of 2012 on the Organization of Electronic Systems and Transactions;
- c. that based on the considerations as referred to in letter a and letter b, it has been deemed necessary to establish Regulation of the Government Number 82 of 2012 on the Organization of Electronic Systems and Transactions.

Observing:

1. Article 5 paragraph (2) of the 1945 Constitution of the Republic of Indonesia;
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 the Amendment to Law Number 11 of 2008 on Electronic Information and Transactions (State Gazette of the Republic of Indonesia of 2016 Number 251, Supplement to the State Gazette of the Republic of Indonesia Number 5952);
3. Regulation of the Government Number 82 of 2012 on the Organization of Electronic Systems and Transactions (State Gazette of the Republic of Indonesia of 2012 Number, Supplement to the State Gazette of the Republic of Indonesia Number 5348).

HAS DECIDED:

To establish:

**REGULATION OF THE GOVERNMENT ON THE AMENDMENT TO REGULATION OF THE GOVERNMENT
NUMBER 82 OF 2012 ON THE ORGANIZATION OF ELECTRONIC SYSTEMS AND TRANSACTIONS.**

Article I

Several provisions set out in Regulation of the Government Number 82 of 2012 on the Organization of

Electronic System and Transactions (State Gazette of the Republic of Indonesia of 2012 Number 189, Supplement to the State Gazette of the Republic of Indonesia Number 5348) have now been amended as follows:

1. The provisions of number 5 and number 12 have been amended, between number 27 and number 28 of Article 1 are inserted 3 (three) numbers, namely number 27a, number 27b, and number 27c, and between number 34 and number 35 of Article 1 is inserted 1 (one) number, namely number 34a, therefore Article 1 reads as follows:

“Article 1

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

1. Electronic System is a series of electronic procedure and device that serve to prepare, collect process, analyze, store, display, publish, transmit, and/or disseminate Electronic Information.
2. An electronic Transaction is a legal act which is carried out by the use of Computer, Computer network, and/or other electronic media.
3. Electronic Agent is a device of an Electronic System made to automatically act on a certain Electronic Information which is organized by a Person.
4. Electronic System Provider is any Person, state administrator, Business Entity, and community that individually or jointly provide, manage, and/or operate Electronic System to Electronic System Users for its own interest and/or the interest of other parties.
5. Sectoral Regulatory and Supervisory Agency is any Agency in charge of supervising the implementation of sectoral duties and issue regulations toward the said sector.
6. Electronic Information is one or a group of electronic data, including but not limited to texts, sound, images, maps, designs, photos, electronic data interchange (EDI), electronic mails, telegrams, telex, telecopies or the like, alphabets, marks, numbers, Access codes, symbols, or perforations that has been processed and that has meaning or can be understood by people capable of understanding them.
7. Electronic Document is any Electronic Information which are made, forwarded, transmitted, received, or stored in analog, digital, electromagnetic, optical, or similar form, and which can be viewed, displayed, and/or heard through computer or Electronic System, including but not limited to texts, sound, images, maps, designs, photos or the like, alphabets, marks, numbers, Access codes, symbols or perforations that has meaning or can be understood by people who are able to understand it.
8. Information Technology is a technique to collect, prepare, store, process, publish, analyze, and/or disseminate information.
9. Electronic System User is any Person, state administrator, Business Entity, and community who use goods, services, facilities or information provided by Electronic System Providers.
10. Hardware is one or a series of devices connected in an Electronic System.
11. Software is one or a series of computer programs, procedures, and/or documentation related to the operation of Electronic System.
12. Electronic System Feasibility Test is a series of objective assessment process toward each Electronic System component, either carried out independently and/or carried out by an authorized and competent institutions.
13. Access is the activity of performing interaction with a stand-alone or networked Electronic System.
14. Organization of Electronic Transaction is a series of Electronic Transaction activities performed by Senders and Receivers using Electronic Systems.
15. Electronic Contract is an agreement of the parties which is made through an Electronic System.
16. Sender is the legal subject who send Electronic Information and/or Electronic Documents.

17. Receiver is the legal subject who receive Electronic Information and/or Electronic Documents from its Sender.
18. Electronic Certificate is an electronic certificate containing Electronic Signature and identity that shows the legal subject status of the parties in the Electronic Transaction issued by an electronic certification organizer.
19. Electronic Signature is a signature consisting of Electronic Information which is attached, associated or linked with other Electronic Information and that are used as verification and authentication tools.
20. Signatory is the legal subject associated or linked with an Electronic Signature.
21. Electronic Signature Organizer is a legal entity serving as the trusted party which facilitates the creation of an Electronic Signature.
22. Electronic Signature Service Support (Pendukung Layanan Tanda Tangan Elektronik) is a legal entity serving as the party supporting the implementation of the use of Electronic Signatures.
23. Electronic Signature Creation Data are personal codes, biometric codes, cryptography codes, and/or codes generated from the conversion of a manual signature into an Electronic Signature, including other codes resulting from the development of Information Technology.
24. Reliability Certification Agency is an independent institution established by professionals that are acknowledged, authorized, and supervised by the Government with authority to audit and issue Certificate of Reliability in Electronic Transactions.
25. Certificate of Reliability is a document which states that the Business which organize Electronic Transactions has passed an audit or conformity test from the Reliability Certification Agency.
26. Business is an individual person or a business entity, either in the form of incorporated entity or unincorporated entity, which is established and domiciled or conduct activities in the jurisdiction of the state of the Republic of Indonesia, either individually or jointly, through an agreement for organizing business activities in various economic sectors.
27. Personal Data is a certain individual data stored, maintained, and has its validity retained, as well as its confidentiality protected.
- 27a. Electronic Data is data in electronic form that are not limited to texts, sound, images, maps, designs, photos, electronic data interchange (EDI), electronic mails, telegrams, telex, telecopies or the like, alphabets, marks, numbers, Access codes, symbols, or perforations.
- 27b. Strategic Electronic Data are Electronic Data that has strategic impacts toward the smoothness of state administration, and state security and defense.
- 27c. High-Risk Electronic Data are high-risk Electronic Data with an impact limited to the interests of electronic data owners and their sector.
28. Domain Name is the internet address of a state administrator, Person, Business Entity, and/or community, which can be used in communicating through the internet, and which take the form of unique codes or character arrangements to indicate a specific location on the internet.
29. Domain Name Registry is any organizer responsible for carrying out the management, operation, and maintenance of the Organization of Electronic System of Domain Names.
30. Domain Name Registrar is any Person, Business Entity, or community who provides Domain Name registration services.
31. Domain Name User is any Person, State Administrator Agency, Business Entity, or community who file a registration for the use of Domain Names to a Domain Name Registrar.
32. State Administration Agency, from this point onward is referred to as Agency, are central and regional level legislative, executive and judicial institutions and other agencies established by laws and regulations.
33. Person is any individual person, be it an Indonesian citizen, a foreign citizen, or a legal entity.

34. Business Entity is any sole proprietorship or partnership company, be it an incorporated entity or unincorporated entity.
- 34a. Government is the Minister or other officials appointed by the President.
35. Minister is the minister responsible for government affairs in the sector of communication and informatics.”

2. The provision of Article 4 letter g has been amended, therefore Article 4 reads as follows:

“Article 4

The Organization of Electronic System as referred to in Article 3 paragraph (1) encompass the regulation on:

- a. registration;
 - b. Hardware;
 - c. Software;
 - d. expert staff;
 - e. governance;
 - f. safeguarding;
 - g. Electronic System Feasibility Test; and
 - h. supervision.”
3. Between paragraph (1) and paragraph (2) of Article 5 is inserted 1 (one) paragraph, namely paragraph (1a), between paragraph (4) and paragraph (5) of Article 5 is inserted 3 (three) paragraphs, namely paragraph (4a), paragraph (4b), and paragraph (4c), and the provision of paragraph (5) of Article 5 has been amended, therefore Article 5 reads as follows:

“Article 5

- (1) Providers of Electronic System for public services are required to undertake a registration process.
- (1a) The Providers of Electronic System for public services as referred to in paragraph (1) are comprised of:
 - a. Electronic System Providers regulated or supervised by Sectoral Regulatory and Supervisory Agencies in accordance with provisions of laws and regulations;
 - b. Electronic System Providers in the form of an Agency;
 - c. Electronic System Providers that owns:
 1. online portals, sites, or apps through the internet used to facilitate offering and/or trading of goods and/or services;
 2. Electronic Systems that involves online payment or financial transaction facilities through data communication or internet networks;
 3. Electronic Systems used for processing Electronic Information that contains or requires the deposit of funds or something equated with funds;
 4. Electronic Systems used for data processing, handling or storing, including Personal Data, for operational activities serving the community that are related to Electronic Transaction activities;
 5. Electronic Systems used for transmitting paid digital contents through data

networks, be it by way of downloading through portals/sites, delivery through electronic mails, or through other applications to the device of users; and/or

6. Electronic Systems that provides, manage, and/or operate communication services, such as short messages, voice calls, video calls, electronic mails, and online conversations in the form of digital platform; search engine services; social media and networking services; and electronic information providing services in the form of texts, sound, images, animations, music, videos, films, and games or a combination of part and/or all of them.

- (2) Providers of Electronic Service for non-public services may undertake the registration process.
- (3) The mandatory registration of Providers of Electronic System for public services as referred to in paragraph (1) shall be carried out before the Electronic Systems starts to be publicly used.
- (4) The registration as referred to in paragraph (1) and paragraph (2) shall be submitted to the Minister.
- (4a) To implement the registration as referred to in paragraph (4), the Minister may coordinate with Sectoral Regulatory and Supervisory Agencies.
- (4b) The Electronic System Providers as referred to in paragraph (1) and paragraph (2) who has met all the requirements shall be incorporated into the list of Electronic System Providers.
- (4c) In the implementation of the registration as referred to in paragraph (1), the Minister implements the data sharing and electronically-integrated (online) system.
- (5) Further provisions on the implementation of the registration as referred to in paragraph (1), paragraph (2) to paragraph (4c) shall be regulated under a Regulation of the Minister."

4. The provision of Article 11 has been removed.

5. Between Article 15 and Article 16 are inserted 4 (four) articles, namely Article 15A, Article 15B, Article 15C, and Article 15D, therefore they read as follows:

"Article 15A

- (1) Every Electronic System Provider is required to erase irrelevant Electronic Information and/or Electronic Documents that are under its control upon a request from the Person concerned based on a court decree.
- (2) The Electronic System Providers that are required to erase the Electronic Information and/or Electronic Documents as referred to in paragraph (1) are Electronic System Providers who obtain and/or process Personal Data under their control.
- (3) The obligation to erase Electronic Information and/or Electronic Documents as referred to in paragraph (1) does not apply in the case of the said Electronic Information and/or Electronic Documents are required to be stored or are prohibited to be erased by Electronic System Providers in accordance with provisions of laws and regulations.

Article 15B

The irrelevant Electronic Information and/or Electronic Documents as referred to in Article 15A paragraph (1) are comprised of any Personal Data which:

- a. is obtained and processed without approval from Personal Data owners;
- b. has the approval withdrawn by Personal Data owners;
- c. is obtained and processed through unlawful means;

- d. no longer conforms to its purpose of acquisition in accordance with the agreement and/or provisions of laws and regulations;
- e. its use has exceeded the period in accordance with the agreement and/or provisions of laws and regulations; and/or
- f. is displayed by Electronic System Providers and which cause a loss to Personal Data owners.

Article 15C

- (1) The application for Electronic Information and/or Electronic Document erasure decree to the local district court shall be filed by the Person concerned as the owner of Personal Data.
- (2) The application for an erasure decree as referred to in paragraph (1) cannot be substituted, unless stipulated otherwise in accordance with provisions of laws and regulations.
- (3) The application for an erasure decree as referred to in paragraph (1) and paragraph (2) should contain:
 - a. applicant's identity;
 - b. Electronic System Provider's identity and/or Electronic System address;
 - c. the irrelevant Personal Data that are under the control of Electronic System Providers; and
 - d. the reason for requesting erasure.
- (4) In the case of the court granted the application for erasure decree as referred to in paragraph (1) and paragraph (2), then Electronic System Providers are required to carry out the erasure of irrelevant Electronic Information and/or Electronic Documents.
- (5) The court decree as referred to in paragraph (4) serve as the basis for an irrelevant Electronic Information and/or Electronic Document erasure request by the Person concerned to the Electronic System Provider.

Article 15D

- (1) Every Electronic System Provider is required to provide a mechanism for the erasure of irrelevant Electronic Information and/or Electronic Documents requested by the Person concerned.
- (2) The erasure mechanism as referred to in paragraph (1) shall, at a minimum, contain provisions as regards:
 - a. the provision of a communication channel between Electronic System Providers and Personal Data owners;
 - b. data collection on the request for erasure of irrelevant Electronic Information and/or Electronic Documents;
 - c. technical instructions for the erasure;
 - d. the term of completion for the erasure; and
 - e. the party authorized to carry out the erasure.
- (3) The data collection as referred to in paragraph (2) letter b are comprised of:
 - a. the court decree document;
 - b. Electronic System address; and
 - c. the irrelevant Electronic Information and/or Electronic Documents to be erased, including its display.

- (4) Further provisions on the erasure mechanism as referred to in paragraph (1) and paragraph (2) shall be stipulated under a Regulation of the Minister.
- (5) Provisions on the erasure mechanism in certain sectors can be formulated by the relevant Sectoral Regulatory and Supervisory Agency after coordinating with the Minister."

6. The provision of paragraph (2) of Article 17 has been amended, therefore Article 17 reads as follows:

"Article 17

- (1) Electronic System Providers are required to have a plan on the continuity of activities to overcome any interference or disaster in accordance with the risks of impacts it caused.
- (2) Electronic System Providers are required to place and process Strategic Electronic Data at a data center and disaster recovery center within Indonesian territory.
- (3) Further provisions on the mandatory placement and processing at data center and disaster recovery center within Indonesian territory as referred to in paragraph (2) shall be regulated by the relevant Sectoral Regulatory and Supervisory Agency in accordance with provisions of laws and regulations after coordinating with the Minister."

7. The title of Division Eight of CHAPTER II has been amended, therefore Division Eight reads as follows:

"Division Eight

Electronic System Feasibility Test"

8. The provisions of paragraph (1), paragraph (3), and paragraph (4) of Article 30 have been amended, and paragraph (2) of Article 30 has been removed, therefore Article 30 reads as follows:

"Article 30

- (1) Electronic System Providers for public service are required to undertake an Electronic System Feasibility Test.
- (2) Removed.
- (3) The obligation as referred to in paragraph (1) shall be carried out toward Electronic System components.
- (4) Provisions on the Electronic System Feasibility Test as referred to in paragraph (1) shall be stipulated under a Regulation of the Minister."

9. The provision of Article 31 has been removed.

10. The provision of Article 32 has been removed.

11. The provisions of paragraph (1) and paragraph (3) of Article 41 have been amended, therefore Article 41 reads as follows:

"Article 41

- (1) The Organization of Electronic Transaction in public or private sphere that uses Electronic Systems for public service purposes are required to use Certificate of Reliability and Electronic

Certificate.

- (2) In the case of using a Certificate of Reliability, the organization of Electronic Transactions in the public sphere must be certified by a registered Indonesian Reliability Certification Agency.
- (3) In the case of using an Electronic Certificate, the organization of Electronic Transactions in public sphere are required to use the services of electronic certification organizers that are under a parent organization (penyelenggara sertifikasi elektronik berinduk)."

12. The provision of paragraph (3) of Article 42 has been amended, therefore Article 42 reads as follows:

"Article 42

- (1) The Organization of Electronic Transactions in the private sphere may use Certificate of Reliability and/or Electronic Certificate.
- (2) In the case of using a Certificate of Reliability, the organization of Electronic Transactions in the private sphere may be certified by a registered Indonesian Reliability Certification Agency.
- (3) In the case of using an Electronic Certificate, the organization of Electronic Transactions in the private sphere may use the services of electronic certification organizers that are under a parent organization.

13. The provision of Article 43 paragraph (1) letter b has been removed, therefore Article 43 reads as follows:

"Article 43

- (1) The Organization of Electronic Transactions in the territory of the State of the Republic of Indonesia must:
 - a. pay attention to aspects of security, reliability, and efficiency;
 - b. Removed.
 - c. utilize the national gateway, if in its organization involves more than one Electronic System Providers; and
 - d. utilize domestic Electronic System networks.
- (2) In the case of the national gateway and Electronic System networks as referred to in paragraph (1) letter c and letter d cannot be implemented yet, then the organization of Electronic Transactions may utilize other medium or foreign facilities after securing approval from the relevant Sectoral Regulatory and Supervisory Agency.
- (3) In the fulfillment as referred to in paragraph (1), the parties in Electronic Transactions are required to pay attention to laws and regulations from the relevant Sectoral Regulatory and Supervisory Agency."

14. The provision of paragraph (3) of Article 58 has been amended, therefore Article 58 reads as follows:

"Article 58

- (1) Before an Electronic Signature is used, Electronic Signature Organizers are required to confirm the initial identification of the Signatory by way of:
 - a. the Signatory submitting an identity to the Electronic Signature Organizer;
 - b. the Signatory undertake a registration with Electronic Signature Organizers or Service Supports; and
 - c. in case of being deemed necessary, Electronic Signature Organizers may confidentially

delegate a Signatory's identity data to other Electronic Signature Organizers or Electronic Signature Service Supports with approval from the Signatory.

- (2) The mechanism used by Electronic Signature Organizers to electronically prove a Signatory's identity should implement the combination of, at a minimum, 2 (two) authentication factors.
- (3) The verification process of signed Electronic Information can be carried out using the verification data of Electronic Signature to track every signed change of data."

15. Between Article 59 and Article 60 is inserted 1 (one) article, namely Article 59A, therefore it reads as follows:

"Article 59A

- (1) Electronic System Users may use a digital identity which is a representation of legal subjects and/or an entity which is unique and a differentiator from other subjects in an Electronic System.
- (2) The digital identity as referred to in paragraph (1) is required to use an Electronic Certificate issued by an electronic certification organizer which is under a parent organization.
- (3) Digital identity is organized by digital identity organizers.
- (4) Digital identity organizers operating in Indonesia are required to secure an acknowledgment from the Minister.
- (5) The acknowledgment of the digital identity organizers as referred to in paragraph (4) is exempted for Electronic Certification Organizers that are under a parent organization, and that become a digital identity organizer.
- (6) Further provisions on the digital identity organization mechanism shall be stipulated under a Regulation of the Minister."

16. The provision of Article 60 letter a has been amended, therefore Article 60 reads as follows:

"Article 60

Electronic certification organizers are authorized to:

- a. inspect the identity of any prospective owner and/or holder of Electronic Certificate;
- b. issue Electronic Certificates;
- c. extend the validity period of Electronic Certificates;
- d. block and revoke Electronic Certificates;
- e. validate Electronic Certificates; and
- f. create a list of Electronic Certificates that are active and that are under suspension."

17. The provision of Article 61 has been amended, therefore Article 61 reads as follows:

"Article 61

- (1) the organization of electronic certification in Indonesia shall adhere to the principle of one parent organization.
- (2) The organization of parent electronic certification is held by the Minister.
- (3) Electronic certification organizers operating in Indonesia are required to secure an acknowledgment on having a parent organization from the Minister."

18. The provisions of paragraph (1) and paragraph (4) of Article 62 has been amended, and paragraph (2) and paragraph (3) of Article 62 has been removed, therefore Article 62 reads as follows:

“Article 62

- (1) The acknowledgment as referred to in Article 61 paragraph (3) shall be granted by the Minister after electronic certification organizers satisfy the requirements for registration and certification processes stipulated under a Regulation of the Minister.
- (2) Removed.
- (3) Removed.
- (4) Further provisions on procedures for the registration and certification of electronic certification organizers as referred to in paragraph (1) shall be stipulated under a Regulation of the Minister.”

19. The provision of paragraph (2) of Article 64 has been amended, therefore Article 64 reads as follows:

“Article 64

- (1) Supervision toward the organization of electronic certification is implemented by the Minister.
- (2) Further provisions on the supervision of organization of electronic certification are stipulated under a Regulation of the Minister.”

20. Between CHAPTER VIII and CHAPTER IX is inserted 1 (one) chapter, namely CHAPTER VIIIA, therefore it reads as follows:

“CHAPTER VIIIA

ROLE OF THE GOVERNMENT

Article 83A

The role of the Government in the organization of Electronic Transactions and systems encompass:

- a. facilitating the use of Information Technology and Electronic Transactions in accordance with provisions of laws and regulations;
- b. protecting public interests from all kinds of interference due to the misappropriation of Electronic Information and Electronic Transactions that disturbs public order, in accordance with provisions of laws and regulations;
- c. undertaking the prevention of dissemination and use of Electronic Information and/or Electronic Documents containing banned contents in accordance with provisions of laws and regulations or unlawful contents; and
- d. determining the Agencies or institutions possessing Strategic Electronic Data that must be protected.

Article 83B

The role of the Government to facilitate the use of Information Technology and Electronic Transaction as referred to in Article 83A letter a encompass:

- a. policy establishment;
- b. policy implementation;
- c. infrastructure facilitation;
- d. promotion and education; and

- e. supervision.

Article 83C

The infrastructure facilitation as referred to in Article 83B letter c encompass:

- a. the development and organization of the national Electronic System gateway;
- b. the development and organization of forensic facilities for Information Technology;
- c. the organization of electronic organization for parent organizations;
- d. the organization of data center and national disaster recovery center in an integrated manner to organize electronic-based administration affairs;
- e. the Electronic System safeguarding facility for preventing attacks toward vital information infrastructure in strategic sectors;
- f. the facility for entrusting or storing source codes and documentation of software for Agencies; and
- g. other means required to facilitate the use of Information Technology and Electronic Transactions in accordance with provisions of laws and regulations.

Article 83D

- (1) The promotion and education as referred to in Article 83B letter d shall be carried out by Agencies in accordance with their authorities in based on provisions of laws and regulations to realize the use of Information Technology and Electronic Transactions that are safe, ethical, clever, creative, productive and innovative.
- (2) The implementation of promotion and education may involve stakeholders, including communities and/or Information Technology and Electronic Transaction practitioners.

Article 83E

- (1) The role of the Government to protect public interests from all kinds of interference due to the misappropriation of Electronic Information and Electronic Transactions which disturbs public order as referred to in Article 83A letter b encompass:
 - a. establishment of a national cybersecurity strategy which a part of the national security strategy, including the development of cybersecurity culture;
 - b. regulation of information security standards;
 - c. regulation of the organization of vital information infrastructure protection;
 - d. regulation of risk management for the organization of Electronic Systems;
 - e. regulation of human resources in the organization of Electronic System protection;
 - f. development and supervision of the organization of vital information infrastructure protection;
 - g. development and supervision of risk management for the organization of Electronic Systems;
 - h. development and supervision of human resources in the organization of Electronic System protection;
 - i. organization of Electronic Information safeguarding;
 - j. organization of the handling of information security incidents;

- k. organization of emergency response handling; and
 - l. other functions necessary to protect public interests from all kinds of interference.
- (2) The provisions as referred to in paragraph (1) are the authority of the Government.
 - (3) The authority as referred to in paragraph (2) can be implemented in cooperation with other parties.

Article 83F

The role of the Government to undertake the prevention of dissemination and use of Electronic Information and/or Electronic Documents containing banned contents in accordance with provisions of laws and regulations or unlawful contents as referred to in Article 83A letter c takes the form of termination of Access and/or ordering Electronic System Providers to terminate Access toward said Electronic Information and/or Electronic Documents.

Article 83G

The termination of Access is carried out toward Electronic Information and/or Electronic Documents as referred to in Article 83F with the following classification:

- a. violating provisions of Laws and Regulations;
- b. disturbing the community and/or disrupting public order; and
- c. informing the method to or providing Access toward Electronic Information and/or Electronic Documents containing banned contents in accordance with provisions of laws and regulations or unlawful contents.

Article 83H

- (1) Communities, Sectoral Regulatory and Supervisory Agencies, law enforcement officers, and judiciary bodies can apply to the termination of Access to the Electronic Information and/or Electronic Documents as referred to in Article 83G to the Minister.
- (2) The provisions on the procedures for applying the termination of Access as referred to in paragraph (1) shall be regulated under a Regulation of the Minister.

Article 83I

- (1) Electronic System Providers are required to perform the termination of Access toward the Electronic Information and/or Electronic Documents as referred to in Article 83G.
- (2) The Electronic System Providers as referred to in paragraph (1) includes internet Access service providers, telecommunication network and service providers, content providers, and link providers that provide traffic networks for Electronic Information and/or Electronic Document.
- (3) Electronic System Providers that does not perform the termination of Access may subject to legal liability in accordance with provisions of laws and regulations.
- (4) Further provisions on the implementation of the mandatory termination of Access as referred to in paragraph (1) shall be regulated under a Regulation of the Minister.

Article 83J

- (1) Aside from determining the Agencies or institutions that own the Strategic Electronic Data that must be protected as referred to in Article 83A letter d, the also set out the classification of

Electronic Data.

- (2) The Electronic Data as referred to in paragraph (1) consists of Strategic Electronic Data, High-Risk Electronic Data, and low-risk Electronic Data.

Article 83K

- (1) The Strategic Electronic Data that must be protected as referred to in Article 83J are data that satisfies the following criteria:
 - a. any threat and/or interference towards them disrupts state administration;
 - b. any threat and/or interference towards them disrupts security and defense;
 - c. other criteria in accordance with the provisions of Laws and Regulations.
- (2) The Strategic Electronic Data that must be protected as referred to in paragraph (1) shall be determined by the President.
- (3) The Strategic Electronic Data as referred to in paragraph (2) shall be identified and proposed by Sectoral Regulatory and Supervisory Agencies through the coordinating minister whose scope of coordination relates with the sector concerned.
- (4) The Strategic Electronic Data as referred to in paragraph (1) are required to be managed, processed, and stored within Indonesian territory.
- (5) The management, processing, and storage of the Strategic Electronic Data as referred to in paragraph (3) are required to use Indonesian networks and Electronic Systems.
- (6) The Strategic Electronic Data as referred to in paragraph (1) are prohibited to be transmitted, exchanged, and/or copied outside Indonesian territory.
- (7) The provision as referred to in paragraph (5) may be exempted with approval from the President.
- (8) Further provisions on the management, processing, storage, transmission, exchange, and/or copying of Strategic Electronic Data shall be regulated under a Regulation of the President.

Article 83L

- (1) High-Risk Electronic Data is data that satisfy the criteria that any threat and/or interference toward them causes or have impacts that are limited to the interests of electronic data owners and their sector.
- (2) Sectoral Regulatory and Supervisory Agencies shall identify and propose High-Risk Electronic Data to the Minister to be determined.
- (3) Electronic System Providers may manage, process, and store High-Risk Electronic Data inside Indonesian territory and/or outside Indonesian territory.
- (4) In the case of the management, processing, and storage of the High-Risk Electronic Data as referred to in paragraph (3) is undertaken outside Indonesian territory, then Electronic System Providers are required to ensure the effectiveness of supervision and enforcement of Indonesian laws.
- (5) Technical provisions on the management, processing, and storage of High-Risk Electronic Data shall be further regulated by Sectoral Regulatory and Supervisory Agencies.

Article 83M

Electronic Data that does not fulfill the criteria for Strategic Electronic Data and High-Risk Electronic Data constitutes low-risk Electronic Data.

Article 83N

Strategic Electronic Data, High-Risk Electronic Data, and low-risk Electronic Data are required to be stored within Electronic Systems in accordance with provisions of laws and regulation that regulates the mandatory data storage period at the respective Sectoral Regulatory and Supervisory Agency.

Article 83O

- (1) Strategic Electronic Data, High-Risk Electronic Data, low-risk Electronic Data are required to be managed, processed, and stored while satisfying the provisions on the protection of the organization of Electronic Data, Personal Data protection guarantee, and enforcement of state sovereignty.
- (2) Electronic System Providers are required to provide Access to and/or handover Strategic Electronic Data, High-Risk Electronic Data, and/or low-risk Electronic Data for supervision and law enforcement in accordance with provisions of Laws and Regulations.

Article 83P

Agencies and/or institution that owns Strategic Electronic Data is required to make electronic backups (rekam cadang elektronik) as well as connect them to the data center and disaster recovery center in an integrated manner for data safeguarding purposes.

Article 83Q

- (1) In organizing the protection of vital information infrastructures as referred to in Article 83E paragraph (1) letter c, the Government shall determine the sectors that have vital information infrastructures.
- (2) The sectors that have vital information infrastructures as referred to in paragraph (1) encompass:
 - a. the government administration sector;
 - b. the energy and mineral resources sector;
 - c. the transportation sector;
 - d. the finance sector;
 - e. the health sector;
 - f. the information technology and communication sector;
 - g. the food (security) sector; and
 - h. the security and defense sector.
- (3) Further provisions on the stipulation and regulation on the sectors that have vital information infrastructures as referred to in paragraph (1) and paragraph (2) shall be regulated under a Regulation of the President.

Article 83R

- (1) Sectoral Regulatory and Supervisory Agencies are domiciled at the ministry and/or agency at the sector in question in accordance with provisions of Laws and Regulations.
- (2) Further provisions on the establishment, authorities, and mechanisms for the implementation of the duties of Sectoral Regulatory and Supervisory Agencies shall be regulated under a

Regulation of the President.”

21. The provisions of paragraph (1), paragraph (2), and paragraph (4) of Article 84 have been amended, as well as the elucidation of Article 84 paragraph (1) has been amended, therefore Article 84 reads as follows:

“Article 84

- (1) Violations toward the provisions of Article 5 paragraph (1) and paragraph (3), Article 7 paragraph (1), Article 8 paragraph (1) and paragraph (3), Article 12 paragraph (1) and paragraph (2), Article 13, Article 14 paragraph (1), Article 15 paragraph (1) and paragraph (2), Article 15A paragraph (1) and paragraph (2), Article 15C paragraph (4), Article 15D paragraph (1), Article 16 paragraph (1), Article 17 paragraph and paragraph (2), Article 18 paragraph (1), Article 21, Article 22 paragraph (1), Article 25, Article 27, Article 29, Article 30 paragraph (1), Article 37 paragraph (1), Article 39 paragraph (1), Article 41 paragraph (1), paragraph (2), and paragraph (3), Article 44 paragraph (1), Article 58 paragraph (1) and paragraph (2), Article 59 paragraph (1), Article 59A paragraph (2) and paragraph (4), Article 61 paragraph (3), and Article 78 paragraph (1) and paragraph (2), Article 81 paragraph (2), Article 83I paragraph (1), Article 83K paragraph (4), paragraph (5), and paragraph (6), Article 83L paragraph (4), Article 83N, Article 83O paragraph (1) and paragraph (2), and Article 83P shall be subject to administrative sanctions.
- (2) The administrative sanction as referred to in paragraph (1) may take the form of:
 - a. written warning;
 - b. administrative fine;
 - c. temporary deactivation;
 - d. termination of Access;
 - e. exclusion from the list as referred to in Article 5 paragraph (4b), Article 37 paragraph (2), Article 62 paragraph (1), and Article 65 paragraph (4).
- (3) The administrative sanction is rendered by the Minister in accordance with provisions of laws and regulations.
- (4) The imposition of the administrative sanctions as referred to in paragraph (2) letter c and letter d shall be carried out through coordination with the head of Sectoral Regulatory and Supervisory Agency.
- (5) (5) The imposition of the administrative sanctions as referred to in paragraph (2) and paragraph (3) does not abolish criminal and civil liabilities.

Article II

- (1) Electronic System Providers that already operates before this Regulation of the Government comes into force are required to conform to the provisions of this Regulation of the Government by no later than 1 (one) year after this Regulation of the Government is promulgated.
- (2) This Regulation of the Government comes into force from the date of its promulgation.

For public cognizance, it is hereby ordered that this Regulation of the Government be promulgated in the State Gazette of the Republic of Indonesia.

Established in Jakarta,

On

THE PRESIDENT OF THE REPUBLIC OF INDONESIA,

Signed.

JOKO WIDODO

Promulgated in Jakarta,

On

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

Signed.

YASONNA H. LAOLY

STATE GAZETTE OF THE REPUBLIC OF INDONESIA OF NUMBER

**DRAFT OF
ELUCIDATION OF
REGULATION OF THE GOVERNMENT OF THE REPUBLIC OF INDONESIA
NUMBER OF
ON
THE AMENDMENT TO REGULATION OF THE GOVERNMENT NUMBER 82 OF 2012 ON THE
ORGANIZATION OF ELECTRONIC SYSTEMS AND TRANSACTIONS**

I. General

Law Number 19 of 2016 on the Amendment to Law Number 11 of 2008 on Electronic Information and Transactions was established to ensure acknowledgment, as well as respect, toward the rights and freedom of other people and to fulfill fair demands in accordance with the consideration of public order and security in a democratic community. Based on the said matter, then there is a need to amend Regulation of the Government Number 82 of 2012 on the Organization of Electronic Systems and Transactions as the implementing regulations of the said Law.

This Regulation of the Government is established to implement several provisions in Law Number 19 of 2016 on the Amendment to Law Number 11 of 2008 on Electronic Information and Transactions, such as the provision of Article 26 paragraph (5) on the obligation of every Electronic System Provider to erase irrelevant Electronic Information and/or Electronic Documents under its control upon request from the Person concerned based on a court decree, and the provision of Article 40 on the role of the Government in facilitating the use of Information Technology and Electronic Transaction, protecting public interests from all kinds of interference due to the misappropriation of Electronic Information and Electronic Transactions that disturbs public order, and prevent the dissemination and use of Electronic Information and/or Electronic Documents containing banned contents in accordance with provisions of Laws and Regulations.

Moreover, this Regulation of the Government is established for the purpose of enforcing state sovereignty over Electronic Information in the territory of the Unified Nation of the Republic of Indonesia which is realized in the form of the regulation that strategic data in the organization of Electronic Systems in several sectors are required to be managed and stored in Electronic Systems in the territory of the State of the Republic of Indonesia. Those sectors are, among others, the government administration sector, the energy and mineral resources sector, the transportation sector, the finance sector, the health sector, the information technology and communication sector, the food sector, and the security and defense sector.

The contents in this Regulation of the Government are, among others:

- a. the mandatory registration for Providers of Electronic System for public services;
- b. the use of Indonesian expert staffs for Electronic System Providers that manage Strategic Electronic Data;
- c. the mandatory undertaking of Electronic System Feasibility Test for Providers of Electronic System for public services;
- d. the mandatory erasure of irrelevant Electronic Information and/or Electronic Documents for Electronic System Providers;
- e. the criteria of irrelevant Electronic Information and/or Electronic Documents;
- f. the mechanism for the erasure and/or blocking of Access toward irrelevant Electronic Information and/or Electronic Documents;
- g. the mandatory placement and processing Strategic Electronic Data at the data center and disaster recovery center in Indonesian territory for Electronic System Providers;

- h. the organization of Electronic Transactions using Electronic System for public service purposes is required to use a Certificate of Reliability and Electronic Certificate;
- i. the role of the Government in the organization of Electronic Transactions and Systems;
- j. the use of digital identity is required to use an Electronic Certificate issued by an Electronic Certification Organizer which is Under a Parent Organization;
- k. the organization of electronic certification adheres to the principle of one parent organization;
- l. the criteria of Strategic Electronic Data that must be protected; and
- m. the obligation relating to Strategic Electronic Data that must be protected to be managed, processed, and stored in Indonesian territory.

II. ARTICLE BY ARTICLE

Article I

Number 1

Article 1

Self-explanatory.

Number 2

Article 4

Self-explanatory.

Number 3

Article 5

Self-explanatory.

Number 4

Article 11

Removed.

Number 5

Article 15A

Paragraph (1)

“Electronic System Provider which is required to erase irrelevant Electronic Information and/or Electronic Documents that are under its control” includes Electronic System Providers that operate search engines. The mandatory erasure for Electronic System Providers that operate the said search engine is, among others erasing the display and/or blocking Access toward the said irrelevant Electronic Information and/or Electronic Documents based on a court decree.

Paragraph (2)

Self-explanatory.

Paragraph (3)

Self-explanatory.

Article 15B

Self-explanatory.

Article 15C

Self-explanatory.

Article 15D

Paragraph (1)

Self-explanatory.

Paragraph (2)

Self-explanatory.

Paragraph (3)

Letter a

Self-explanatory.

Letter b

"Electronic System address" takes the form of, among others, internet address or other forms which indicates the location of display of irrelevant Electronic Information and/or Electronic Documents.

Letter c

Self-explanatory.

Letter d

Self-explanatory.

Paragraph (4)

Self-explanatory.

Paragraph (5)

Self-explanatory.

Number 6

Article 17

Paragraph (1)

“plan on the continuity of activities” is a set of the process undertaken to ensure continuous activities in conditions of interference or disaster.

Paragraph (2)

“data center” is a facility used for placing Electronic Systems and their related components that may take the form of cloud computing service for data placement, storage, and processing.

“disaster recovery center” is a facility which may take the form of cloud computing services which is used for restore data or information, as well as important functions, of Electronic Systems that are disrupted or damaged due to the occurrence of disasters caused by nature or human.

Paragraph (3)

Self-explanatory.

Number 7

Self-explanatory.

Number 8

Article 30

Paragraph (1)

Self-explanatory

Paragraph (2)

Removed.

Paragraph (3)

Electronic System components include, among others, Hardware, Software, expert staffs, governance, and safeguarding.

Paragraph (4)

Self-explanatory.

Number 9

Article 31

Removed.

Number 10

Article 32

Removed.



Number 11

Article 41

Self-explanatory.

Number 12

Article 42

Self-explanatory.

Number 13

Article 43

Paragraph (1)

Letter a

Self-explanatory.

Letter b

Removed.

Letter c

Self-explanatory.

Letter d

“Electronic System Networks” is the connection of two or more Electronic Systems, which is closed or open.

Paragraph (2)

Self-explanatory.

Paragraph (3)

Self-explanatory.

Number 14

Article 58

Paragraph (1)

Self-explanatory.

Paragraph (2)

The authentication factors that may be selected to be combined can be differentiated in 3 (three) types, namely:

- a. what you have (sesuatu yang dimiliki secara individu), such as an ATM card or a smart card;

- b. what you know (sesuatu yang diketahui secara individu), such as a PIN/password or cryptographic key; and
- c. what you are (sesuatu yang merupakan ciri/karakteristik seorang individu), such as voice patterns, handwriting dynamics, or fingerprints.

Paragraph (3)

Self-explanatory.

Number 15

Article 59A

Paragraph (1)

“unique” is have to refer only to one legal subject or one entity which represents one identity.

Paragraph (2)

Self-explanatory.

Paragraph (3)

Self-explanatory.

Paragraph (4)

Self-explanatory.

Paragraph (5)

Self-explanatory.

Paragraph (6)

Self-explanatory.

Number 16

Article 60

Letter a

“inspect the identity of any candidate owner and/or holder of Electronic Certificate” are, among others, inspection relating to the identity, physical existence of any candidate owner and/or holder of Electronic Certificate.

Letter b

Self-explanatory.

Letter c

Self-explanatory.

Letter d

Self-explanatory.

Letter e

Self-explanatory.

Letter f

Self-explanatory.

Number 17

Article 61

Paragraph (1)

“one parent organization” is that electronic certification organizers in Indonesia stem from the parent electronic certification organizer held by the Minister.

Paragraph (2)

Self-explanatory.

Paragraph (3)

“Electronic certification organizers that secure an acknowledgment of having a parent organization” are electronic certification organizers that are under a parent organization whose certificate is signed using the certificate of the parent electronic certification organizer.

Number 18

Article 62

Self-explanatory.

Number 19

Article 64

Self-explanatory.

Number 20

Article 83A

Self-explanatory.

Article 83B

Self-explanatory.

Article 83C

Letter a

“national Electronic System gateway” are, among others, the Indonesia National Single Window (INSW) and the online single submission.

Letter b

Self-explanatory.

Letter c

Self-explanatory.

Letter d

The organization of data center and national disaster recovery center in an integrated manner is aimed at general applications and Strategic Electronic Data.

Letter e

Self-explanatory.

Letter f

Self-explanatory.

Letter g

Self-explanatory.

Article 83D

Self-explanatory.

Article 83E

Self-explanatory.

Article 83F

Self-explanatory.

Article 83G

Letter a

“violating provisions of Laws and Regulations” are, among others, Electronic Information and/or Electronic Document containing elements of pornography, gambling, slander and/or defamation, fraud, animosity toward ethnicity, religion, race, and inter-group relations (suku, agama, ras, dan antargolongan - SARA), violence and/or violence against children, intellectual property infringement, violation of trade in goods and services with specific rules, terrorism and/or radicalism, separatism and/or forbidden harmful organization, information security violation, consumer protection violation, violation in the health sector, food and drug control violation.

Letter b

“disturbing the community and/or disrupting public order” are, among others, falsified information and/or facts.

Letter c

Self-explanatory.

Article 83H

Self-explanatory.

Article 83I

Paragraph (1)

“termination of Access” are, among others, Access blocking, account shut down, and/or content removal.

Paragraph (2)

Self-explanatory.

Paragraph (3)

Self-explanatory.

Paragraph (4)

Self-explanatory.

Article 83J

Self-explanatory.

Article 83K

Self-explanatory.

Article 83L

Paragraph (1)

Example of “High-Risk Electronic Data” are, among others, data relating to digital platform-based services.

Paragraph (2)

Self-explanatory.

Paragraph (3)

Self-explanatory.

Paragraph (4)

Self-explanatory.

Paragraph (5)

Self-explanatory.

Article 83M

Self-explanatory.

Article 83N

Self-explanatory.

Article 83O

Self-explanatory.

Article 83P

Self-explanatory.

Article 83Q

Paragraph (1)

Vital information infrastructures are a series of electronic system components that process, manage, and store Strategic Electronic Data and/or High-Risk Electronic Data, as well as constitute an essential part in the organization of vital infrastructures.

Paragraph (2)

Self-explanatory.

Paragraph (3)

Self-explanatory.

Article 83R

Self-explanatory.

Number 21

Article 84

Paragraph (1)

Self-explanatory.

Paragraph (2)

Letter a

Self-explanatory.

Letter b

Self-explanatory.

Letter c

“temporary deactivation” takes the form of the deactivation of a part of or all components or services on the Electronic System concerned for a certain period.

Letter d

Self-explanatory.

Letter e

Self-explanatory.

Paragraph (3)

Self-explanatory.

Paragraph (4)

Self-explanatory.

Paragraph (5)

Self-explanatory.

Article II

Self-explanatory.

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

DISCLAIMER

"This translation was produced by Hukumonline for the purpose of understanding Indonesian law only and does not constitute an official translation published by the Indonesian Government. Hukumonline has made every effort to ensure the accuracy and completeness of the information that is contained within this translation, however, we are not responsible for any errors, omissions and/or mistakes that occur in the source text. Hukumonline reserves the right to change, modify, add or remove any errors or omissions without any prior notification being given. These services are not intended to be used as legal references, advice and/or opinions and no action should be taken as regards the reliability of any of the information contained herein without first seeking guidance from professional services."