

TABLE OF CONTENTS :

Table of Contents	
Overview	2
I. New Categorization of ESP.....	3
II. Electronic Systems Organized by Private ESP.....	4
III. Mandatory Registration of ESP	5
IV. Other Requirements in Relation to the Organization of Electronic Systems	6
A. Hardware	6
B. Software.....	6
C. Utilization of Experts.....	7
D. Governance of Electronic Systems .	7
E. Location of Data Management, Processing and/or Storage	8
F. Required Information for Users	8
G. Feasibility Assessments	8
V. The Right to Be Forgotten	9
VI. Electronic Agents	10
VII. Electronic Transactions.....	12
A. Scope of Electronic Transactions..	12
B. Certification of Electronic Transactions.....	12
VIII. Electronic Certification Organizers	14
A. General Requirements.....	14
B. Scope of Services	14
IX. Blocking Authority	17
X. Comparison Matrix	18
Conclusion.....	31

New Regulatory Framework Introduced for the Organization of Electronic Systems and Transactions

Electronic system providers in both public and private sectors must now be registered with the Minister of Communications and Informatics before their electronic systems can be utilized by users.

Overview

While closely monitoring the ongoing rapid growth in information technology, the Indonesian Government ultimately decided to revise Regulation of the Government No. 82 of 2012 on the Organization of Electronic Systems and Transactions (“**Regulation 82/2012**”). This revision sets out an updated regulatory framework for the organization of electronic systems and transactions in Indonesia, thereby supporting the government’s vision of transforming Indonesia into the biggest digital-economy power in Southeast Asia.¹ After a year of preparation, the highly-anticipated regulatory framework was finally rolled out recently through the enactment of Regulation of the Government No. 71 of 2019 on the Organization of Electronic Systems and Transactions (“**Regulation 71/2019**”).

Comprising more than 100 articles, Regulation 71/2019 incorporates a number of new areas into its framework. One of the most notable revisions is the new categorization of electronic system providers (*penyelenggara sistem elektronik* – “**ESP**”) which has resulted in changes being made to their various obligations. In addition, Regulation 71/2019 also attempts to create greater certainty as regards the so-called right to be forgotten, which was initially introduced through Law No. 19 of 2016 on the Amendment to Law No. 11 of 2008 on Electronic Information and Transactions.

This edition of Indonesian Law Digest (ILD) will highlight a number of key aspects of Regulation 71/2019 and compare its various provisions with provisions that were originally set out under Regulation 82/2012, which was repealed and replaced when Regulation 71/2019 officially came into force on 10 October 2019. Our discussion will address the following matters:

- I. New Categorization of ESP;
- II. Electronic Systems Organized by ESP within the Private Sector;
- III. Mandatory Registration of ESP;
- IV. Other Requirements in Relation to the Organization of Electronic Systems:
 - A. Hardware;
 - B. Software;
 - C. Utilization of Experts;
 - D. Governance of Electronic Systems ;
 - E. Location of Data Management, Processing and/or Storage;
 - F. Required Information for Users; and
 - G. Feasibility Assessments;
- V. The Right to Be Forgotten;
- VI. Electronic Agents;
- VII. Electronic Transactions:
 - A. Scope of Electronic Transactions;

¹ Kominfo.go.id, “Revisi PP PSTE Dukung Lajunya Teknologi Digital Indonesia,” as accessed through https://kominfo.go.id/index.php/content/detail/14733/siaran-pers-no-243hmkominfo092018-tentang-revisi-pp-pste-dukung-lajunya-teknologi-digital-indonesia/0/siaran_pers on 28 October 2019.

B. Certification of Electronic Transactions; and

VIII. Electronic Certification Organizers:

A. General Requirements;

B. Scope of Services,

IX. Blocking Authority; and

X. Matrix Comparison.

I. New Categorization of ESP

Electronic systems are to be organized by ESP.² Regulation 71/2019 defines two categories of ESP, as follows:

Categories ³	Subjects
ESP in the public sector ("Public ESP")⁴	Government institutions and other agencies which are appointed by government institutions in order to organize electronic systems for and on behalf of them. However, Public ESP exclude ESP which function as regulatory and supervisory authorities within the financial sector (e.g. Bank Indonesia and the Financial Services Authority).
ESP in the private sector ("Private ESP")	Individuals (Indonesian or foreign citizens), business entities (incorporated or unincorporated), as well as members of the general public which organize electronic systems that meet certain criteria and which will be elaborated upon in the following section.

Previously, Regulation 82/2012 set out a different categorization which was based on the underlying purposes for the organization of electronic systems (instead of being based on ESP type) i.e. public services and non-public services. However, Regulation 82/2012 did not offer any further clarification regarding said services, although it did refer to various criteria for public services, as set out under the relevant applicable laws and regulations, including Law [No. 25 of 2009](#) on Public Services ("**Public Services Law**").

² Art. 2 (1), Regulation 71/2019.

³ Art. 2 (2), Regulation 71/2019.

⁴ Art. 2 (3-4) and its elucidations, Regulation 71/2019.

II. Electronic Systems Organized by Private ESP

Regulation 71/2019 now clarifies that Private ESP comprise any parties which organize any of the following electronic systems:⁵

1. Electronic systems which are subject to the regulation or supervision of a ministry or governmental institution; and
2. Electronic systems which incorporate internet-based portals, sites or applications (whether they are used and/or offered in Indonesia)⁶ and which are organized in order to fulfill the following functions:
 - a. Provision, management and/or operation of the following: i) Offering and/or trading of goods and/or services; ii) Financial transaction services; iii) Communications services (including, but not limited to, short text messages, voice calls, video calls, emails, digital chat rooms, networking services and social media);
 - b. Delivery of materials or paid digital content through data networks, by way of downloading from websites, sending of emails or via application to customers' devices;
 - c. Search engines and electronic information provision services (in the form of texts, audiovisual data, animations, music, videos, films and games or any combination of the above); and/or
 - d. Processing of personal data for the organization of public services that relate to electronic transaction activities.

Given the broad scope of the various electronic systems outlined above, many parties may unknowingly be classified as Private ESP. Meanwhile, once classified as Private ESP, said parties must comply with various requirements and obligations which apply to them, otherwise, they may have sanctions imposed upon them.

⁵ Art. 2 (5), Regulation 71/2019.

⁶ Elucidation of Art. 2 (5), Regulation 71/2019.

III. Mandatory Registration of ESP

Under Regulation 82/2012, it was mandatory for all Public ESP to be registered. Meanwhile, the registration of Private ESP was to be undertaken on a voluntary basis.⁷

Regulation 71/2019 now requires both Public ESP and Private ESP to be registered before their electronic systems can be utilized by users. Registration applications should be submitted to the Minister of Communications and Informatics (“**Minister**”) and should be processed via the Online Single Submission system.⁸

It should be noted that existing ESP must comply with this obligation in accordance with the provisions contained under Regulation 71/2019 within one year.⁹ As additional information, the registration procedures for ESP are still currently covered by Regulation of the Minister [No. 36 of 2014](#) on the Registration Procedure for Electronic System Providers.¹⁰ However, this regulation was issued under the framework of Regulation 82/2012 (which only required the registration of ESP which organize electronic systems in relation to public services) prior to the establishment of the Online Single Submission system. Therefore, the Minister is likely to issue an amendment or a new regulation in the near future in order to bring things into line with the various provisions which are set under Regulation 71/2019.

⁷ Art. 5 (1-2), Regulation 82/2012.

⁸ Art. 6 (1-3), Regulation 71/2019.

⁹ Art. 102, Regulation 71/2019.

¹⁰ For more information on this regulation, see ILB [No. 2522](#).

IV. Other Requirements in Relation to the Organization of Electronic Systems

ESP must ensure that the organization of their electronic systems is in compliance with various requirements which relate to a number of different aspects. The following section will elaborate upon these requirements with a specific focus on the differences between Regulation 71/2019 and Regulation 82/2012.

A. Hardware

All devices which are connected to electronic systems (i.e. hardware) must meet the following requirements:¹¹

1. Must meet the various security, interconnectivity and compatibility requirements of the system in question;
2. Must be equipped with technical support, maintenance and/or after-sales services, as provided by their sellers or providers; and
3. Must be equipped with service sustainability guarantees.

The fulfillment of the abovementioned requirements is to be proven through certification or other similar evidence. Certification-related evidence may be provided by any third parties which are accredited in Indonesia, while other evidence may be provided by foreign certification agencies.¹²

By way of comparison, Regulation 71/2019 simplifies these requirements by dispensing with a number of requirements which were originally set out under Regulation 82/2012, including guarantees relating to the availability of spare parts over three years; guarantees relating to defect-free products; and possession of supporting references from other users of the relevant hardware in order to confirm the conformity of its specifications. In addition, Regulation 71/2019 has also now relaxed the certification requirement, as Regulation 82/2012 previously required all hardware to be covered by feasibility certification issued by the Minister.¹³

B. Software

Computer programs, procedures and/or documentation which relate to the operation of electronic systems (i.e. software) must meet the following requirements:¹⁴

1. Must have their security and operational feasibility guaranteed (i.e. the software must be guaranteed to not contain any instructions which do not conform to its purposes, including malicious code, time-bomb instructions and virus programs), which should be guaranteed through source-code checking; and
2. Must have their service sustainability guaranteed.

¹¹ Arts. 1 (12) and 7 (1), Regulation 71/2019.

¹² Art. 7 (2) and its elucidation, Regulation 71/2019.

¹³ Art. 6 (1), Regulation 71/2019.

¹⁴ Arts. 1 (13) and 8 (and its elucidation), Regulation 71/2019.

It is important to note that developers of any software which is specifically developed for Public ESP must provide both the source code and related documentation for said software to the relevant ESP. Meanwhile, recipients must: 1) Secure said source codes and documentation by themselves or through the use of trusted third parties; and 2) Guarantee the confidentiality of source codes and ensure that any source codes are only used in the ESP's interests.¹⁵

By way of comparison, Regulation 71/2019 contained similar provisions to those which are now set out under Regulation 82/2012. However, Regulation 71/2019 no longer requires software to be registered with the Minister, as was the case under Regulation 82/2012.¹⁶

C. Utilization of Experts

Regulation 71/2019 allows for ESP to utilize experts (i.e. persons who possess academically and practically proven expertise relating to electronic systems), provided that any such experts meet relevant provisions which are contained under prevailing laws and regulations.¹⁷

Previously, Regulation 82/2012 required all experts to possess competency certification. In addition, in terms of the organization of strategic electronic systems, all related experts were required to be Indonesian citizens, unless capable Indonesian experts were unavailable.¹⁸ Since these provisions have been repealed, ESP may now utilize foreign experts.

D. Governance of Electronic Systems

Regulation 71/2019 requires all ESP to implement proper and accountable governance in relation to their electronic systems. In order to be deemed proper and accountable, governance must meet the following minimum requirements:¹⁹

1. Must ensure the availability of the following: a) Procedures or guidelines for the organization of electronic systems, which must be documented and/or announced in languages, information or symbols which are comprehensible to the relevant stakeholders; b) Sustainable mechanism aimed at ensuring that electronic systems manuals are both up-to-date and clear; c) Supporting agencies and personnel whose job is to ensure the proper operation of electronic systems;
2. Must implement performance management systems aimed at ensuring that electronic systems operate optimally; and
3. Must formulate plans which address the maintenance of electronic systems.

Previously, under Regulation 82/2012 the above requirements only applied to Public ESP.²⁰

¹⁵ Art. 9, Regulation 71/2019.

¹⁶ Compare Arts. 7-9, Regulation 82/2012 with Arts. 8-9, Regulation 71/2019.

¹⁷ Art. 10 and its elucidation, Regulation 71/2019.

¹⁸ Art. 10-11, Regulation 82/2012.

¹⁹ Art. 19 (1-2), Regulation 71/2019.

²⁰ Art. 16 (1-2), Regulation 82/2012.

E. Location of Data Management, Processing and/or Storage

Regulation 71/2019 outlines different location requirements which relate to the management, processing and/or storage of electronic systems and electronic data based on the relevant ESP categories, as follows:²¹

ESP Category	Location
Public ESP	Must be within Indonesia, unless the relevant storage technology is unavailable domestically (as determined by the government).
Private ESP	Must be within Indonesia and/or overseas. In terms of the latter, the relevant Private ESP must provide access to their electronic systems and electronic data for the purposes of supervision and law enforcement.

Previously, Regulation 82/2012 only required Public ESP to locate their data centers (for the storage and management of electronic systems and their components) and disaster recovery centers (for the recovery of data/information and the strategic functions of electronic systems) within Indonesia.²² Moreover, Regulation 82/2012 was silent regarding location requirements for ESP data centers and/or disaster recovery centers for non-public services.

F. Required Information for Users

All ESP are obliged to disclose the following information to their users:²³

1. Identity of said ESP;
2. Transaction objects;
3. Feasibility or security of the relevant electronic systems;
4. Device utilization manuals;
5. Contract terms and conditions;
6. Procedures for the reaching of agreements;
7. Guarantees relating to privacy and/or personal data protection; and
8. Phone numbers of claim centers.

Previously, under Regulation 82/2012, phone numbers of claim centers were not required to be disclosed to users.²⁴

G. Feasibility Assessments

Both Public ESP and Private ESP must undergo feasibility testing in order to assess whether the components contained within their electronic systems meet with the obligatory protection requirements and strategic characteristics.²⁵ Regulation 71/2019 does not specify the outputs of feasibility testing, in contrast with

²¹ Arts. 20-21, Regulation 71/2019.

²² Art. 17 (2), Regulation 82/2012.

²³ Art. 29, Regulation 71/2019.

²⁴ Compare Art. 25, Regulation 82/2012 with Art. 29, Regulation 71/2019.

²⁵ Art. 34, Regulation 71/2019.

Regulation 82/2012, which directly required all ESP to secure feasibility certificates from the Minister through a feasibility certification process.²⁶

V. The Right to Be Forgotten

As briefly addressed earlier, Regulation 71/2019 attempts to incorporate the so-called “right to be forgotten” concept into its framework. This concept was first introduced in Indonesia through the amendment of Law [No. 11 of 2008](#) on Electronic Information and Transactions by Law [No. 19 of 2016](#) (collectively referred to as the “ITE Law”).

Pursuant to the ITE Law, ESP are required to delete any irrelevant electronic information and/or documents under their control, as requested by the owners of said information and/or documents.²⁷ As an implementing regulation of the ITE Law, Regulation 71/2019 now sets out further details regarding the implementation of the right to be forgotten, as detailed in the table below:

Measure	Details
Deletion (right to erasure)²⁸	<p>Personal data may be deleted if:</p> <ol style="list-style-type: none"> 1. They are acquired and processed without the prior consent of the relevant data owner; 2. Consent relating to said data has been revoked by the data owner; 3. They are acquired and processed unlawfully; 4. They no longer fit their acquisition purposes, as stated under the relevant agreement and/or laws and regulations; 5. Their utilization period has exceeded the period stipulated under the relevant agreement and/or laws and regulations; and/or 6. They are disclosed by ESP in a way that disadvantages the data owner; <p>It should be noted that the obligation to delete personal data does not apply if said data is required to be preserved under relevant laws and regulations.</p>
Removal (right to delisting)²⁹	<p>Personal data may only be removed from search engines based on a court stipulation.</p> <p>In order to obtain such a stipulation, data owners must submit their application for removal to the relevant local district court. All such applications must include the following information:</p> <ol style="list-style-type: none"> 1. Identities of data owners; 2. Identities of ESP and/or addresses of the relevant electronic systems; 3. Irrelevant personal data which is under the control of the ESP; and 4. Reasons for the removal request.

²⁶ Arts. 30 (1) and 31, Regulation 82/2012.

²⁷ Art. 26 (3), ITE Law.

²⁸ Art. 16, Regulation 71/2019.

²⁹ Art. 17 (1-3), Regulation 71/2019.

Regulation 71/2019 further requires ESP to provide mechanisms for the implementation of the various measures which are outlined above. These mechanisms must at least include information on the following:³⁰

1. Communication channel between ESP and data owners;
2. Deletion or removal features; and
3. Recordation of deletion or removal requests.

VI. Electronic Agents

In addition to being organized by ESP, electronic systems may also be organized by electronic agents.³¹ An electronic agent refers to electronic system devices that are specifically created (as visual, audio and electronic data or in other possible forms) in order to automatically perform certain actions in relation to electronic information which is organized by persons (“Agent”).³²

Since an Agent is part of an electronic system, the relevant Agent organizer is subject to the same obligations which apply to ESP.³³ For example, Agent organizers are required to disclose any information which must be disclosed by ESP (as discussed in Section IV, Part F of this edition of ILD). In addition, Agent organizers must also provide certain features which are also required of ESP in relation to the following functions:³⁴

1. Corrections;
2. Cancellations;
3. Confirmations or reconfirmations;
4. Options relating to the continuation or termination of subsequent activities;
5. Provision of access to information in the form of contracts or advertisements;
6. Checking of status in order to ascertain success or failure; and
7. Reading of agreements prior to the execution of transactions.

Moreover, Agent organizers must also allow users to alter any information while a given transaction is still processing.³⁵

It should be noted that a given Agent may be organized in the interests of more than one ESP based on an agreement which addresses the following aspects at the least:³⁶

1. Rights and obligations;
2. Responsibilities;
3. Claim and dispute resolution mechanisms;

³⁰ Art. 18, Regulation 71/2019.

³¹ One example of an Agent is Hukumonline’s own [Legal Intelligent Assistant \(LIA\)](#).

³² Art. 1 (3); and Art. 36 (1) and (4), Regulation 71/2019.

³³ Art. 36 (2-3), Regulation 71/2019.

³⁴ Arts. 29, 30 and 37, Regulation 71/2019.

³⁵ Art. 37 (4), Regulation 71/2019.

³⁶ Art. 38, Regulation 71/2019.

- 4. Validity periods;
- 5. Costs;
- 6. Scope of services; and
- 7. Choice of law.

By way of comparison, generally speaking, Regulation 82/2012 encompassed similar provisions as those set out under Regulation 71/2019. However, Regulation 71/2019 now requires that the following information also be disclosed to users: contract terms and conditions, procedures for the reaching of agreements and guarantees of privacy and/or personal data protection. Furthermore, Regulation 71/2019 also requires all Agents to now add features that enable users to: 1) Read transaction agreements prior to their execution; and 2) Change their information while a transaction is still processing.³⁷

³⁷ Compare Art. 35, Regulation 82/2012 with Art. 37, Regulation 71/2019.

VII. Electronic Transactions

In general, Regulation 71/2019 and Regulation 82/2019 outline similar provisions regarding electronic transactions. However, there are several differences between the two regulations, specifically in terms of the scope of and the required certification for electronic transactions.

A. Scope of Electronic Transactions

Electronic transactions refer to all legal actions which are conducted through the use of computers, computer networks and/or other electronic media.³⁸ Such transactions may be conducted within both the private and public sectors by the following parties:³⁹

Parties to Electronic Transactions	
Public Sector	Private Sector
<ol style="list-style-type: none"> 1. Government institutions ("Institutions"); 2. Organizations which are appointed by Institutions ("Organizations"); 3. Intra-institution; 4. Intra-Organization; 5. Between Institutions and Organizations; and 6. Between Institutions or Organizations and businesses. 	<ol style="list-style-type: none"> 1. Intra-business; 2. Between businesses and consumers; and 3. Intra-personal.

This classification is slightly different to that originally set out under Regulation 82/2012, which classified transactions in the public sector, as described under points (3) and (6) above,⁴⁰ as private sector transactions.⁴¹

B. Certification of Electronic Transactions

Electronic transactions must be accompanied by the electronic certificates of the parties to the relevant transactions and these electronic certificates should contain their digital signatures and identities. These certificates are issued by Indonesian certification organizers (e.g. PrivyID, PERURI, Vida, Govca and Digisign).⁴²

Electronic transactions may also be accompanied by the reliability certificates (*sertifikat keandalan*) of electronic transaction organizers in order to confirm that said organizers have passed the auditing and conformity testing process, as implemented by reliability certification agencies which are registered in

³⁸ Art. 1 (2), Regulation 71/2019.

³⁹ Art. 41, Regulation 71/2019.

⁴⁰ Specifically for transactions which take place between Institutions and businesses.

⁴¹ Art. 40, Regulation 82/2012.

⁴² Kominfo, "Status Pengakuan Penyelenggara Sertifikasi Elektronik", as accessed through <https://psre.rootca.or.id/#?hash=1&page=0> on 29 October 2019.

Indonesia. In contrast with electronic certificates, these certificates are to be provided on a voluntary basis only.⁴³

Regulation 81/2012 previously allowed for electronic transactions to be accompanied by either electronic certificates and/or reliability certificates.⁴⁴ This means that electronic certificates were not previously mandatory for electronic transactions.

⁴³ Art. 42, Regulation 71/2019.

⁴⁴ Art. 41, Regulation 82/2012.

VIII. Electronic Certification Organizers

Regulation 71/2019 requires all ESP to possess electronic certificates. Users of electronic systems may subsequently obtain these for use in electronic transactions. When required by the government under certain circumstances, possession of said certificates may even become mandatory for electronic system users. In order to obtain an electronic certificate, both ESP and electronic systems users are required to submit their applications to Indonesian electronic certification organizers.⁴⁵

It should be noted, however, that two types of electronic certification organizers are now available (“**Certification Organizers**”), specifically: Indonesian Certification Organizers and foreign Certification Organizers.⁴⁶ The following section will outline the general requirements and scope of services for these Certification Organizers.

A. General Requirements

As mentioned above, Certification Organizers may take the form of either Indonesian or foreign entities. In general, Indonesian Certification Organizers must be acknowledged by the Minister and are to be routed (*berinduk*) under the main Certification Organizer which is recognized by the Minister.⁴⁷ Meanwhile, all foreign Certification Organizers must be registered with the Minister.⁴⁸

In contrast with Regulation 71/2019, Regulation 82/2012 did not specifically categorize two types of Certification Organizers. Nevertheless, Regulation 82/2012 required all Certification Organizers operating within Indonesia to be acknowledged by the Minister at the following levels: registered, certified and routed (*berinduk*).⁴⁹

B. Scope of Services

Regulation 71/2019 has now broadened the scope of the various services which may be provided by Certification Organizers, as elaborated upon in the table below:

Services ⁵⁰		Remarks ⁵¹
Type	Definition	
Digital signature	A signature that contains electronic information which is affixed, associated or related to other electronic information and which is to be used as a	<ul style="list-style-type: none">Function as authentication and verification tools in relation to:<ol style="list-style-type: none">Identities of the relevant signatories; and

⁴⁵ Art. 51 (1-4), Regulation 71/2019.

⁴⁶ Art. 53 (1), Regulation 71/2019.

⁴⁷ Due to the single parent principle (*prinsip satu induk*), electronic certificates which are issued by Indonesian Certification Organizers will be signed based on a certificate issued by the main Certification Organizer hosted by the Minister. (Elucidation, Art. 53 [2], Regulation 71/2019)

⁴⁸ Art. 53 (1), (3) and (5), Regulation 71/2019.

⁴⁹ Art. 61, Regulation 82/2012.

⁵⁰ Arts. 57 and its elucidation, Regulation 71/2019.

⁵¹ Arts. 60, 65-72, Regulation 71/2019.

	verification and authentication tool	2. The wholeness and authenticity of electronic information
Electronic seal	A digital signature which is used by business entities or Institutions in order to guarantee the originality and integrity of electronic information and/or documents	<ul style="list-style-type: none"> May be certified or uncertified, on condition that any certified item meets the following requirements: <ol style="list-style-type: none"> Must meet the criteria for lawful digital signatures (e.g. data for the establishment of digital signatures must specifically relate to the relevant signatory, any modification which is made to any digital signature must be able to be detected, while there must be a method in place in order to identify signatories); Must utilize electronic certificates which are issued by Indonesian Certification Organizers; and Must be created through the use of certified digital signature producing devices
Electronic timer	A binding signature which sets the time and date of electronic information and/or documents	<ul style="list-style-type: none"> May be certified or uncertified, on condition that any certified item meets the following requirements: <ol style="list-style-type: none"> Must be a binding signature which addresses both time and date in order to eradicate the possibility of any electronic information and/or documents being modified undetectably; Must refer to accurate time which relates to coordinated universal timing; Must utilize electronic certificates which are produced by the Certification Organizer; and Must be signed with a digital signature which is produced by the Certification Organizer, Certified electronic timers are obliged to encompass: <ol style="list-style-type: none"> Accurate times and dates; and The integrity of electronic information and/or documents within the stipulated time.

Recorded electronic delivery services	A service which is used in order to deliver electronic information and/or documents, as well as to provide evidence regarding said delivery while simultaneously protecting all delivered electronic information and/or documents from certain risks (e.g. risk of being lost, stolen or damaged)	<ul style="list-style-type: none"> • May be certified or uncertified, on condition that any certified service meets the following requirements: <ol style="list-style-type: none"> 1. Must be organized by one or more Certification Organizer; 2. Must accurately identify senders; 3. Must identify receivers' addresses prior to delivery and so forth, • Certified delivery services must ensure the following: <ol style="list-style-type: none"> 1. The integrity of all transmitted data; 2. Identities of senders; 3. Identities of receivers; and 4. Accuracy of delivery times.
Website authentication	A service aimed at identifying websites and associating them with individuals or business entities which obtain electronic certificates from said websites	<ul style="list-style-type: none"> • May be certified or uncertified. • Whether certified or not, electronic certificates which will be used as web authentication may comprise the following information: <ol style="list-style-type: none"> 1. Identity of web organizers, including addresses where the relevant organizers are domiciled or where Institutions are operating; 2. Domain names; 3. Validity periods of electronic certificates and so forth.
Preservation of digital signatures and/or electronic seals	A service aimed at ensuring that any expired digital signature and electronic seal may still be validated	<ul style="list-style-type: none"> • May be certified or uncertified, provided that any certified service meets the following requirements: <ol style="list-style-type: none"> 1. Must utilize electronic certificates which are produced by the Certification Organizer; and 2. Any digital signature and/or electronic seal which is contained as part of electronic information and/or documents must remain valid if the relevant electronic certificate has expired.

Previously, Regulation 82/2012 only allowed for Certification Organizers to issue electronic certificates, while digital signatures fell under the authority of digital signature organizers.⁵² Meanwhile, the other services outlined above were not previously addressed under Regulation 82/2012.

IX. Blocking Authority

Regulation 71/2019 introduces a number of new provisions which address the government's various authorities in relation to the organization of electronic systems and transactions, as follows:⁵³

1. Facilitating the utilization of information technology and electronic transactions;
2. Protecting the public interest from any disturbances that may result from the misuse of electronic information and transactions;
3. Implementing preventive actions aimed at stopping the dissemination of any electronic information and/or documents which are prohibited under laws and regulations; and
4. Determining the Institutions or Organizations that possess strategic electronic data that must be protected.

In implementing any preventive actions, as outlined in number (3) above, the government may terminate access to and/or order an ESP to terminate access to the prohibited electronic information and/or documents.⁵⁴

⁵² Arts. 1 (21) and 60, Regulation 82/2012.

⁵³ Art. 90, Regulation 71/2019.

⁵⁴ Art. 95, Regulation 71/2019.

X. Comparison Matrix

The main differences between Regulation 71/2019 and Regulation 82/2012 are summarized in the comparison matrix below:

No.	Aspects	Remarks	
		Regulation 71/2019	Regulation 82/2012
1.	ESP categorization	<ul style="list-style-type: none"> Public ESP comprise electronic systems organized by government institutions and other organizations which are appointed by government institutions to organize electronic systems for and on behalf of them; (Art. 1 [5]) It should be noted that public sector ESP exclude ESP which function as regulatory and supervisory authorities within the financial sectors (e.g. Bank Indonesia and the Financial Services Authority); (Art. 2 [4]) Private ESP comprise individuals (Indonesian or foreign citizens), business entities (either incorporated or unincorporated), as well as the general public; (Art. 1 [6]) Private ESP organizes the following electronic systems: (Art. 2 [5]) <ul style="list-style-type: none"> Electronic systems which are subject to the regulation or supervision of a ministry or governmental institution; and 	<ul style="list-style-type: none"> Criteria for ESP for public services refer to the Public Services Law (Art. 3 [2]); Criteria for public services under the Public Services Law are as follows (Art. 5, Public Services Law): <ul style="list-style-type: none"> Public services activity covers the procurement of public goods and public services, as well as administrative services; and The procurement of public goods and public services can be implemented by government institutions, business entities whose capital derives from separated state assets or regional assets and business entities whose capital does not derive from state assets or regional assets, while the objectives of procurement are to fulfill state missions; No criteria for Private ESP were specifically regulated

No.	Aspects	Remarks	
		Regulation 71/2019	Regulation 82/2012
		<ul style="list-style-type: none"> Electronic systems which possess internet-based portals, sites or applications which are organized in order to fulfill the following functions: <ul style="list-style-type: none"> a) Provision, management and/or operation of the following: i) Offering and/or trading of goods and/or services; ii) Financial transaction services; iii) Communications services (including, but not limited to, short text messages, voice calls, video calls, emails, digital chat rooms, networking services and social media); b) Delivery of materials or paid digital content through data networks by way of downloading from websites, sending of emails or via application to customers' devices; c) Search engines and electronic information provider services (in the form of texts, audiovisual data, animations, music, videos, films and games or any combination of the above); and/or d) Processing of personal data for the organization of 	

No.	Aspects	Remarks	
		Regulation 71/2019	Regulation 82/2012
		public services that relate to electronic transaction activities	
2.	ESP registration obligations	<ul style="list-style-type: none"> Both Public ESP and Private ESP must comply with the same registration obligations. (Art. 6 [1]) 	<ul style="list-style-type: none"> ESP for public services are obliged to register with the Minister while ESP for non-public services are not required to comply with this obligation (Art. 5 [1] and [2])
3.	Hardware requirements	<ul style="list-style-type: none"> ESP hardware must meet the following requirements (which have been simplified from Regulation 82/2012): (Art. 7 [1]) <ul style="list-style-type: none"> Comply with various security, interconnectivity and compatibility criteria which are aligned to the relevant system; Operate technical support maintenance services and/or after-sales services; and Maintain the sustainability of services. The fulfillment of the above must be proven through certification or other similar proof (i.e. certification issued by foreign agencies) (Art. 7 [2] and its elucidation) 	<ul style="list-style-type: none"> ESP hardware must meet the following requirements: <ul style="list-style-type: none"> Comply with various security, interconnectivity and compatibility criteria which are aligned to the relevant system; Secure certification from the Minister; Operate technical support maintenance services and/or after-sales services; Maintain supporting references from other users which address fully functional hardware; Maintain the availability of spare parts for three years at the minimum; Maintain clarity assurances with regard to updates; and Maintain product defect assurances; Technical standards relating to hardware requirements are

No.	Aspects	Remarks	
		Regulation 71/2019	Regulation 82/2012
			further determined by the Minister (Art. 6 [2])
4.	Software requirements	<ul style="list-style-type: none"> – ESP software must meet the following criteria: (Art. 8) <ul style="list-style-type: none"> • Security and operational feasibility must be guaranteed (i.e. the software must be guaranteed to not contain any instructions which do not conform to its purposes, including malicious code, time-bomb instructions and virus programs); and • Assurances relating to service continuity must be guaranteed; – Assurances relating to the security and operational feasibility above may be backed up by source-code checking (Elucidation, Art. 8) 	<ul style="list-style-type: none"> – ESP software for the public sector must meet the following criteria: (Art. 7) <ul style="list-style-type: none"> • Must be registered with the Minister; • Security and operational feasibility must be guaranteed; and • Software must operate in accordance with prevailing laws and regulations
5.	Experts requirements	<ul style="list-style-type: none"> – The utilization of experts in relation to electronic systems must involve parties who are competent in relation to the relevant electronic system or information technology and who also meet provisions which are set out under the prevailing laws and regulations (Art. 10) 	<ul style="list-style-type: none"> – Experts must be competent and must be in possession of competency certification; (Art. 10) – In terms of ESP within strategic sectors specifically, Indonesian experts must be utilized, except in cases where capable Indonesian workers are not available (Art. 11)
6.	The right to be forgotten	<ul style="list-style-type: none"> – ESP who obtain or process any personal data under their control are obliged to delete any irrelevant electronic information and/or electronic documents as 	<ul style="list-style-type: none"> – Not Regulated

No.	Aspects	Remarks	
		Regulation 71/2019	Regulation 82/2012
		<p>requested by data owners; (Art. 15 [1])</p> <ul style="list-style-type: none"> – Data deletion measures comprise the following: 1) The right to erasure; and 2) The right to delisting; (Art. 15 [2]) – The right to private data erasure may be performed in relation to the following: (Art. 16 [1]) <ul style="list-style-type: none"> • Data which is acquired and processed without the prior consent of the data owner; • Consent relating to said data has been withdrawn by the data owner; • Data which is acquired and processed unlawfully; • Data which no longer fits the stated acquisition purposes as set out under the relevant agreements and/or laws and regulations; • Data for which the utilization period has exceeded the period stipulated under the relevant agreement and/or laws and regulations; and/or • Data which is disclosed by ESP in a way that places the data owner at a disadvantage; 	

No.	Aspects	Remarks	
		Regulation 71/2019	Regulation 82/2012
		<ul style="list-style-type: none"> – The above requirements may be exempted under certain circumstances, specifically, if the relevant electronic information and/or electronic documents must be preserved in accordance with prevailing laws and regulations; (Art. 16 [2]) – Meanwhile, the right to delisting may only be performed in relation to a court stipulation that is secured by a data owner after they have first submitted an application to a court. The application must encompass the following: (Art. 17) <ul style="list-style-type: none"> • Identities of data owners; • Identities of ESP and/or addresses of the relevant electronic systems; • Irrelevant personal data which are being controlled by the relevant ESP; and • Reasons for the removal request; – The stated right to be forgotten mechanism must be provided by the relevant ESP (Art. 18 [1]) 	
7.	Location of data management, processing and/or storage	<ul style="list-style-type: none"> – Public ESP must implement data management, processing and/or storage within Indonesian territory unless Indonesia does not yet possess adequate technology, in which case these 	<ul style="list-style-type: none"> – ESP for public services must operate data center and data recovery centers within Indonesian territory (Art. 17 [2])

No.	Aspects	Remarks	
		Regulation 71/2019	Regulation 82/2012
		<p>activities may be implemented outside of Indonesia. Technological adequacy criteria are to be determined by the Minister (Art. 20)</p> <ul style="list-style-type: none"> – Meanwhile, data management, processing and/or storage by Private ESP may be performed both within Indonesia and/or outside Indonesia. Provided that the government has access to any such data; (Art. 21) – However, the placement of data centers and data disaster recovery centers which specifically relate to the electronic provision of government services must be organized by the Indonesian Government (Art. 92.d) 	
8.	Required information to be disclosed by ESP to users	<ul style="list-style-type: none"> – ESP must disclose the following information to their users: (Art. 29) <ul style="list-style-type: none"> • Identity of said ESP; • Transaction objects; • Feasibility or security of electronic systems; • Utilization manuals for devices; • Contract terms and conditions; • Procedure for consensual agreements; 	<ul style="list-style-type: none"> – ESP must disclose the following information to their users: (Art. 25) <ul style="list-style-type: none"> • Identity of said ESP; • Transaction objects; • Feasibility or security of electronic systems; • Utilization manuals for devices; • Contract terms and conditions; • Procedure for consensual agreements; and • Privacy guarantees and/or personal data protection

No.	Aspects	Remarks	
		Regulation 71/2019	Regulation 82/2012
		<ul style="list-style-type: none"> • Privacy guarantees and/or personal data protection; and • Phone numbers for claim centers 	
9.	Feasibility assessments of electronic systems	<ul style="list-style-type: none"> – All ESP, whether public or private, must undergo feasibility testing in terms of their electronic systems; (Art. 34) – Feasibility testing (<i>uji kelaikan</i>) comprises tests that have been designed to objectively assess the components of electronic systems. These tests may be conducted on a partial basis that covers the protection of the strategic nature of electronic systems organizations (Arts. 1 and 34 [2]) 	<ul style="list-style-type: none"> – ESP for public services must secure Electronic System Feasibility Certificates, as issued by the Minister or by recognized certification centers (Arts. 30 [1] and 31)
10.	Treatment of Agents	<ul style="list-style-type: none"> – The provisions which apply to ESP also apply mutatis mutandis to Agents 	<ul style="list-style-type: none"> – Specifically stipulates that Agents must complete a registration process through the Minister (Art. 37)
11.	Disclosures by Agents to users	<ul style="list-style-type: none"> – Information which must be disclosed by ESP also applies to disclosures which are made by Agents (Art. 37) 	<ul style="list-style-type: none"> – Information which must be disclosed by ESP also applies to disclosures which are made by Agents, with the exclusion of disclosures of the phone numbers of the claim centers (Art. 35)
12.	Features of Agents	<ul style="list-style-type: none"> – Agents must have features that are similar to those which are set out under Regulation 82/2012 with the addition of a single extra feature, specifically readings of agreements prior to transactions proceeding (Art. 37 [3]) 	<ul style="list-style-type: none"> – Agents must provide the following features in order to ensure the protection of customer rights: (Art. 35) <ul style="list-style-type: none"> • Corrections; • Cancellations;

No.	Aspects	Remarks	
		Regulation 71/2019	Regulation 82/2012
			<ul style="list-style-type: none"> • Confirmations and reconfirmations; • Options to proceed with or terminate subsequent activities; • Access to information in the form of contracts or advertisements; and/or • Checking of statuses: success or failure
13.	Categorization of electronic transactions	<ul style="list-style-type: none"> – Electronic transactions which are undertaken within the public sector encompass transactions which involve the following: (Art. 41) <ul style="list-style-type: none"> • Institutions; • Organizations; • Intra-Institution; • Intra-Organization; • Between Institutions and Organizations; and • Between Institutions or Organizations and business entities; – Electronic transactions which are undertaken within the private sector encompass transactions which involve the following: (Art. 41) <ul style="list-style-type: none"> • Intra-business; • Between businesses and consumers; and • Intra-personal 	<ul style="list-style-type: none"> – Electronic transactions which are undertaken within the public sector encompass transactions which involve the following: (Art. 40) <ul style="list-style-type: none"> • Transactions between institutions or other parties who provide public services are accommodated under the ITE Law; and • Other services within the public sector, as regulated under the relevant laws and regulations; – Electronic transactions which are undertaken within the private sector encompass transactions which involve the following: (Art. 40) <ul style="list-style-type: none"> • Intra-business; • Between businesses and consumers; • Intra-personal; • Intra-Institution; and • Between Institutions and businesses

No.	Aspects	Remarks	
		Regulation 71/2019	Regulation 82/2012
14.	Certification of electronic transaction organizer	<ul style="list-style-type: none"> Organizers of electronic transactions must possess electronic certificates and may also secure reliability certificates on a voluntary basis (Art. 42) 	<ul style="list-style-type: none"> Organizers of electronic transactions within the public sector must secure either electronic certificates and/or reliability certificates. (Art. 41) Organizers of electronic transactions within the private sector may secure either electronic certificates and/or reliability certificates on a voluntary basis. (Art. 42)
15.	Requirements for electronic certification organizers	<ul style="list-style-type: none"> Electronic certification organizers may take the following forms: (Art. 53 [1]) <ul style="list-style-type: none"> Indonesian organizers; and Foreign organizers who are registered in Indonesia. Electronic organizers must be acknowledged by the Minister through single parent (<i>berinduk</i>) principle, as implemented by the Minister. (Art. 53 [3]) 	<ul style="list-style-type: none"> Electronic certification organizers must secure leveling acknowledgments which comprise: registration, accreditation and routed (<i>berinduk</i>) (Art. 61)
16.	Scope of services offered by electronic certification organizers	<ul style="list-style-type: none"> May provided certificates services which comprise: (Art. 57) <ul style="list-style-type: none"> Digital signatures; and/or Other services, as follows: <ul style="list-style-type: none"> a) Electronic seals; b) Electronic timers; c) Recorded electronic delivery services; d) Website authentications; and/or 	<ul style="list-style-type: none"> Issuance of electronic certificates (Art. 60)

No.	Aspects	Remarks	
		Regulation 71/2019	Regulation 82/2012
		e) Preservation of digital signatures and/or electronic seals	
17.	Reliability certification agencies	<ul style="list-style-type: none"> – Reliability certification agencies must be domiciled within Indonesia. Regulation 71/2019 no longer specifies whether said agencies may take the form of foreign entities (Art. 73) 	<ul style="list-style-type: none"> – Reliability certification agencies comprise the following entities, which should be listed by the Minister: (Art. 65) <ul style="list-style-type: none"> • Indonesian agencies which must be domiciled within Indonesia; and • Foreign agencies
18.	Categorization of reliability certificates	<ul style="list-style-type: none"> – Reliability certificates encompass the following categories: (Art. 76) <ul style="list-style-type: none"> • Identity registrations; • Electronic systems security; and • Privacy policies 	<ul style="list-style-type: none"> – Reliability certificates encompass the following security-related categories: (Art. 68) <ul style="list-style-type: none"> • Identities; • Data exchanges; • Vulnerabilities; • Consumer ratings; and • Personal data protection
19.	Establishers of reliability certification agencies	<ul style="list-style-type: none"> – Must be established by the following professionals: (Art. 73) <ul style="list-style-type: none"> • Information technology consultants; • Information technology auditors; and • Legal counsels working within the area of information and technology 	<ul style="list-style-type: none"> – Must be established by the following professionals at the minimum: (Art. 69 (2)) <ul style="list-style-type: none"> • Information technology consultants; • Information technology auditors; and • Legal counsels working within the area of information and technology. – However, in addition to the above, other professionals may involve themselves in such

No.	Aspects	Remarks	
		Regulation 71/2019	Regulation 82/2012
			<p>establishments, as follows: (Art. 69 [3])</p> <ul style="list-style-type: none"> • Accountants; • Management counsels working within the area of information and technology; • Appraisers; • Notaries; and • Other professionals working within the area of information and technology, as determined by the Minister
20.	Government authorities	<p>– In essence, the government's authorities as regards electronic systems and transactions encompass: (Art. 90)</p> <ul style="list-style-type: none"> •Facilitating the utilization of information technology and electronic transactions; •Protecting the public interest from any disturbances which may arise as a result of the misuse of electronic information; •Implementing preventive actions in order to stop the spread of any information which is prohibited under the relevant laws and regulations; and •Determining Institutions or Organizations who are in possession of strategic electronic data which must be protected 	<p>– Not regulated</p>

No.	Aspects	Remarks	
		Regulation 71/2019	Regulation 82/2012
21.	Blocking authority	<ul style="list-style-type: none"> – As the government attempts to prevent the spread of prohibited information, it may implement the following measures: (Art. 95) <ul style="list-style-type: none"> • Termination of access; and/or • Ordering ESP to terminate access 	<ul style="list-style-type: none"> – Not regulated

Conclusion

Regulation 71/2019 has been introduced in an attempt to accommodate recent developments in the organization of electronic systems and transactions. Expanding the previous framework which covered this area to more than a hundred articles, Regulation 71/2019 not only revises the previous framework but also codifies various new aspects that were not previously addressed.

Some of these new provisions represent a regulatory tightening aimed at the protection of the relevant stakeholders. Said new provisions include the mandatory registration of electronic systems by all ESP and the mandatory deletion or removal of electronic information and/or documents, as requested by their owners. Meanwhile, the government now has the authority to block access to prohibited electronic information and/or documents.

On the other hand, a number of other provisions have now been relaxed in order to encourage more activities relating to electronic systems and transactions. These include the possibility of storing Private ESP data overseas, the removal of the requirement for software to be certified, as well as the possibility of utilizing experts who do not possess competency certificates or who are not Indonesian citizens.^{VN}

Indonesian Law Digest is a service of
PT Justika Siar Publika owner and operator of www.hukumonline.com
and pro.hukumonline.com

PT Justika Siar Publika, AD Premier 9th floor
Jl TB. Simatupang No.5 Ragunan,
Pasar Minggu, Jakarta Selatan 12550

to subscribe, call +62-21-2270 8910 or
fax to +62-21 2270 8909 or email
marketing@hukumonline.com

for feedback email rna@hukumonline.com

Head of Legal Research and Analysis: **Christina Desy** | Editors: **Simon Pitchforth, Ricky Pratomo** | Analyst: **Sinatrya Prima, Phalita Gatra, Vania Natalie** | Librarian Manager: **Dedi Rosyadi**

Disclaimer: All data and information contain in this service is compiled from various reliable sources. We have taken every effort to ensure the accuracy and completeness of data and information in these services; however, we are not responsible for any errors or omissions as well as translation mistakes from the source language. Hukumonline Pro may change, modify, add or remove any errors or omissions on pro.hukumonline.com without notification. These services are not intended and should not be taken as legal advice or opinion. No action should be taken in reliance of information contained in these services without first seeking professional services. PT JUSTIKA SIAR PUBLIKA 2019, All Rights Reserved.