DENTONS HPRP

Highlights of The New Government Regulation on Electronic Systems and Transactions

*On 10 October 2019, President Joko Widodo finally issued the long-awaited regulation on the issue of data localization in the new Government Regulation of the Republic of Indonesia No. 71 of 2019 ("**GR 71/2019**") on the Organization of Electronic Systems and Transactions, which revokes the previous regulation that was issued in 2012 as Government Regulation of the Republic of Indonesia No. 82 of 2012 ("**GR 82/2012**"). Apart from provisions on data centres, this client alert highlights other material provisions in this new regulation.*

Objectives of GR 71/2019

Data sovereignty has been one of the main talking points for the Government. The initial intention of the Government was to enforce data localization, mainly aimed at electronic data classified as strategic, by amending GR 82/2012. However, in the development, instead of an amendment, GR 71/2019 was issued to replace GR 82/2012 and provide a more flexible approach to data management.

In addition to data management, GR 71/2019 also emphasizes the Government's role in Electronic Systems and Transactions and the obligation of Electronic System Operators ("ESO") to remove any irrelevant Electronic Information and/or Electronic Documents which are under their control.

Key Points in GR 71/2019

We will elaborate on some of the key points of GR 71/2019 below.

1. New Terms for ESO

In comparison with GR 82/2012, there have been changes in the terms of ESO categorization as incorporated in the GR 71/2019.

GR 82/2012:

a) ESO for Public Services;
b) ESO for Non-Public Services.

GR 71/2019:

a) ESO for Public Scope;
b) ESO for Private Scope.

In GR 71/2019, the term "public service" and "non-public service" are no longer used but instead, GR 71/2019 introduces the new terms "ESO for Public Scope" and "ESO for Private Scope".

GR 71/2019 defines ESO for Public Scope as the provision of electronic systems with the intended subject being State Agencies or institutions appointed by them.

According to the elucidation of Article 2 paragraph 3(b) "Institution appointed by the agency" means an institution operating the electronic system for Public Scope on behalf of the appointing agency.

Meanwhile, ESO for Private Scope is defined as the intended subject being a Person, Business Entity, or community consisting of (i) ESO that are regulated and supervised by the relevant Ministry or Institution based on laws and regulations, and (ii) ESO which own portals, websites, or applications within the internet network, whose electronic system is used in and/or offered in Indonesian territory, and is used, among others, to sell, manage and/or operate offers and/or trade goods and/or services and search engine.

Each ESO is responsible for its operation of the electronic system unless the occurrence of force majeure, or the fault or negligence of the electronic system user, can be proven.

Each ESO must operate an electronic system that meets the following minimum requirements:

a. it can re-display Electronic Information and/or Electronic Documents in their entirety in accordance with the retention period established by legislative regulations;
b. it can protect the availability, integrity, authenticity, confidentiality, and accessibility of Electronic Information in the operation of the Electronic System;
c. it can operate in accordance with the procedures or guidelines in the operation of the Electronic System;
d. it is complete with the procedures or guidelines published in the language or with information or symbols which the parties concerned with the operation of the Electronic System can understand; and
e. it has a continuous mechanism to keep the procedures or guidelines up to date, clear, and responsible.

2. Mandatory Registration of Electronic System Providers

Previously, under GR 82/2012, mandatory registration for electronic systems only applied to ESO for Public Services while ESO for Non-Public Services were open to voluntary registration. In the new regulation GR 71/2019, registration of electronic systems becomes mandatory for both ESO for Public Scope and Private Scope. We expect that the implementing regulations in relation to registration will be further adjusted to align with GR 71/2019.

3. Electronic System Skilled Personnel and Management

The skilled personnel used by an ESO must be competent in the field of electronic systems or information technology.

The ESO must ensure:

a. the availability of service level agreements;
b. the availability of information security agreements for the Information Technology services being used; and
c. the security of the internal information and communications facilities being used.

The ESO must ensure that each component and the integrity of the Electronic System as a whole operates properly. The SEO must apply risk management to any damage or loss incurred and must have management policies, operation working procedures, and carry out periodic audit mechanisms of the electronic system.

The ESO must implement personal data protection principles in processing personal data, including:

a. the collection of Personal Data must be limited and specific, legally valid, fair, and with the knowledge and consent of the owner of the Personal Data;
b. Personal Data must be processed in accordance with its purpose;
c. Personal Data must be processed guaranteeing the rights of the owner of the Personal Data;
d. Personal Data must be processed accurately, and be complete, not misleading, up to date, accountable, and with due attention to the purpose of processing the Personal Data;
e. Personal Data must be processed with the Personal Data protected from loss, misuse, illegitimate Access and disclosure, and any change or damage to the Personal Data;
f. Personal Data must be processed informing the purpose of collection, the processing activities, and any failure to protect the Personal Data; and
g. processed Personal Data must be destroyed and/or deleted except within the retention period in accordance with need pursuant to the provisions of legislative regulations.

If any failure in the protection of Personal Data managed by the ESO occurs, the ESO must inform the owner of the Personal Data in writing.

The ESO must apply good, accountable electronic system management which meets at least the following requirements:

a. the availability of procedures or guidelines in the operation of the Electronic System which are documented and/or published in the language or with information or symbols which can be understood by the parties related to the operation of the Electronic System;
b. there must be a continuous mechanism to keep the procedures and guidelines for implementation up to date and clear;

c. there must be institutional support with complete support personnel for the proper operation of the Electronic System;
d. performance management must be applied to the Electronic System being operated to ensure that the Electronic System is operating properly; and
e. there are plans to safeguard the continuity of operation of the Electronic System it manages.

4. Location of Electronic Data Storage

Significant changes may be seen in the provision on the location of data storage which has been a topic of a long debate among stakeholders.

Under the previous regulation, ESO for Public Services had to establish a data centre in Indonesia resulting in many private sector companies being subject to the requirement to place a data center within Indonesia.

In GR 71/2019, more flexible provision on data management is directed to both ESO for Public Scope and ESO for Private Scope. Unless the technology needed is unavailable in Indonesia, an ESO for Public Scope must store its electronic system in Indonesia. Meanwhile companies that fall under the criteria of ESO for Private Scope are allowed to do management, processing, and/or storage of electronic systems outside of Indonesia while ensuring effective supervision by the relevant Ministry and certain regulatory bodies.

However, while the ESO for Private Scope may enjoy the flexibility of data centres being located outside Indonesia, the companies must ensure that their electronic systems and data are accessible to the Indonesian authority for supervision and law enforcement.

Furthermore, for the financial sector, GR 71/2019 states that the relevant authorities governing this sector may regulate separate provisions on data management.

In addition, while GR 71/2019 provides flexibility on data centres for ESO, it also provides flexibility for the Government to further determine whether State Agencies and institutions possessing data viewed as strategic which need to be protected and must be made into Electronic Documents and backups should be connected to certain data centres which will be further regulated in a separate regulation by the cyber security agency.

According to the elucidation of Article 99 paragraph 1 “Institution which has Strategic Electronic Data” means an institution which has vital information infrastructure in a sector determined under Article 99 paragraph 2 of GR 71/2019.

5. Security of Electronic System Operations

An ESO must make available audit tracking of all electronic system operations which can be used for the purpose of supervision, law enforcement, dispute settlement, verification, testing, and other investigations.

The ESO must make the electronic system components secure.

The ESO must provide a security system which covers procedures and systems for preventing and handling threats and attacks which would give rise to disruption, failures, and losses. If system failures or disruptions which have a serious impact do occur as a result of another party’s actions against the Electronic System, the ESO must secure the Electronic Information and/or Electronic Documents and immediately report such actions to law enforcement and the relevant Ministry or Institution at the first opportunity.

The ESO must deliver information to the Electronic System Users with regard to at least:
a. the identity of the Electronic System Operator;
b. the object of the transaction;
c. the fitness or security of the Electronic System;
d. the procedures for use of the equipment;
e. the terms of the contract;
f. the procedures to reach an agreement;
g. warranties of privacy and/or protection of Personal Data; and
h. the telephone number of the complaints centre.

The ESO must provide features in accordance with the characteristics of the Electronic System it uses. The features must take form of at least features to:
a. make corrections;
b. cancel orders;
c. provide confirmation or reconfirmation;

d. choose to continue or discontinue the implementation of the next activity;
e. see information delivered in the form of an Electronic Contract offer or advertisement;
f. check whether the Electronic Transaction was successful or failed; and
g. read the contract before performing the Electronic Transaction.

The ESO must protect its users and the public at large from losses caused by the Electronic System it operates. The ESO must provide, educate, and train personnel assigned to and responsible for the security and protection of the Electronic System facilities and infrastructure.

For the purpose of criminal proceedings, the Electronic System Operator must provide Electronic Information and/or Electronic Data found in the Electronic System or Electronic Information and/or Electronic Data produced by the Electronic System on a lawful request from an investigator of certain crimes in accordance with the authority provided by statute.

6. Removal of Certain Electronic Data

In GR 71/2019 adds provisions regarding the removal of Electronic Information and Electronic Documents deemed irrelevant. The removal was briefly mentioned in the regulation of the Minister of Communications and Informatics of the Republic of Indonesia No. 20 of 2016 on Privacy Data Protection in Electronic Systems ("MCI Reg 20/2016"), but now in GR 71/2019, the mandatory right to removal, consists of the right of erasure and right to delisting (from search engines).

The right of erasure excludes certain data which must be stored and which it is prohibited to erase as determined by the prevailing regulations.

The right to delisting can be exercised by submitting a petition to the relevant district court to request removal of electronic information and/or Electronic Documents.

Further, each ESO must provide a mechanism for removal of irrelevant Electronic Information and/or Electronic Documents including at least communication channels between the ESO and the personal data owner, removal features and data collection on the removal request. Further provisions on such mechanism will be regulated in a Ministerial Regulation.

7. Software & Hardware Reliability and Security

Certain hardware requirements which were previously mentioned in GR 82/2012 such as among others certificate of fitness (*sertifikasi kelaikan*) issued by the Minister of Communication and Informatics, having supporting references from other users that the hardware is functioning according to specifications, having guaranteed availability of spare parts for at least 3 (three) years, clarity on new conditions and guarantees of freedom from defects are not mentioned in GR 71/2019. Instead, the requirements are replaced with a requirement which the ESO must use a Hardware that:

a. fulfill the aspects of security, interconnectivity and compatibility with the systems used;
b. have a technical support service, maintenance, and/or after-sale services from the seller or provider; and
c. have a guaranteed service continuity.

Despite the removal of the certificate of fitness issued by the Minister of Communication and Informatics, it is further stated that the fulfillment of these requirements must be done through certification by an accredited third party or other similar evidence by certification agencies from outside Indonesia.

ESO must use software that:

a. guarantees the security and reliability of operations accordingly; and
b. ensures the sustainability of services.

Following the provision on software in GR 82/2012, in GR 71/2019, developers providing software specifically developed for the ESO for Public Scope must submit the source code and documentation for the software to the state agencies or institutions concerned.

8. Electronic Transactions

Electronic Transactions performed by parties have legal consequences for the parties. An Electronic Contract will be considered valid if:

a. there is a consensus between the parties;
b. it is made by legal subjects with capacity or authority to represent in accordance with the provisions of legislative regulations;
c. there is a certain object; and
d. the object of the transaction must not be contrary to legislative regulations, morality, and public order.

An Electronic Contract and other contractual forms directed to the population of Indonesia must be made in Bahasa Indonesia.

Electronic Contracts must contain at least:
a. the identity data of the parties;
b. the object and specifications;
c. the terms of the Electronic Transaction;
d. costs and fees;
e. procedures in the event of cancellation by the parties;
f. provisions which entitle harmed parties to return goods and/or request replacement of any products if there are hidden defects; and
g. the governing law for completion of the Electronic Transaction.

Electronic Transactions occur when an agreement is reached by the parties. The agreement may be by means of:
a. an action of acceptance which states consent; or
b. an action of acceptance and/or use of the object by the Electronic System User.

6. Sanction

Administrative sanctions will be imposed for certain violation of GR 71/2019, in the form of:

a. Warning letters;
b. Administrative fines;
c. Temporary suspension;
d. Blocking of access;
e. Removal from the list of registered ESO.

The imposition of the administrative sanctions above does not eliminate any civil or criminal responsibility.

For more information on the violations, please contact us.

Conclusion

While GR 71/2019 provides for easier electronic data storage, further clarification by the Government is still needed through implementing regulations that distinctively separate ESO for Public Scope and ESO for Private Scope. In addition, we should expect a number of existing implementing regulations following GR 82/2012 to be adjusted to GR 71/2019.

-o0o-

*The article above was prepared **Fabiola Hutagalung (Partner), Mika Isac Kriyasa (Senior Associate), Giani Virginia Rajab (Associate), and Widiarahmi Afiandari (Professional Support Lawyer).***