DENTONS HPRP

Highlights in 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 previous regulation that were issued in 2012 under 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 new 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, it 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. Unfortunately, the term "institution" is not clearly defined in GR 71/2019 leading to possible differences in interpretation as to whether private companies are included in this category.

Meanwhile, ESO for Private Scope is defined as the intended subject being a Person, Business Entity, or the community consists 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 offer and/or trade goods and/or services and search engine. Please contact us for more details on the criteria for ESO for Private Scope

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. 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 for 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 for 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 centers 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.

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

Unfortunately, the terms “institution” and ”strategic” are not clearly defined in GR 71/2019 leading to, different possible interpretations of this category.

4. 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.

5. Software & Hardware Reliability and Security

Certain hardware requirements which were previously mentioned in GR 82/2012 such as among others certificate of worthiness (*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 certificate of worthiness 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.

Whereas, ESO must use a Software that:
a. guarantee the security and reliability of operations accordingly; and
b. ensure 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.

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 easier electronic data storage, further clarification is still needed by the Government 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), Giani Virginia Rajab (Associate), and Widiarahmi Afiandari (Professional Support Lawyer).***