NEWSLETTER

November 2019

GOVERNMENT REGULATION ON IMPLEMENTATION OF ELECTRONIC INFORMATION AND TRANSACTION

On 10 October 2019, Government Regulation No. 82 of 2012 on Implementation of Electronic Information and Transaction ("**GR 82/2012**") has been revoked and replaced with Government Regulation No. 71 of 2019 on Implementation of Electronic Information and Transaction ("**GR 71/2019**"). GR 71/19 came into effect on 16 October 2019. There are several provisions of GR 71/2019 that are expected to affect general business activities and ESO in general, which include: (a) a clearer categorization of Electronic System Operator ("**ESO**"); (b) registration requirements of it, (c) expanding obligations for ESO, (d) some changes in personal data protection law, (e) data storage, including (d) electronic certificate requirements and (e) sanctions.

Key contacts:

Eka Wahyuning Siswani
Attorney
ekaws@mkklaw.net

I Gusti Ngurah Oka Anantajaya
Attorney
oka.anantajaya@mkklaw.net

Jonathan Sadikin
Attorney
jonathan.sadikin@mkklaw.net

Definition of Public ESO and Private ESO

Previously GR 82/2012 divided ESO into "public service ESO" and "non-public service ESO". The definition under GR 82/2012 on the public and non-public service ESO was not clear. In the current regulation, the distinction is made clearer between ESO in Public Scope ("**Public ESO**") and ESO in Private Scope ("**Private ESO**"). Public ESO is defined as the implementation of Electronic System by a state institution or institutions appointed by a state institution, with the exception of Public ESO that serves as the managing and supervisory authority in the financial sector. Private ESO refers to implementation of Electronic System by individuals and business entities and is comprised of:

i. Electronic systems which are subject to the regulation or supervision of a ministry or governmental institution in accordance with the law; and
ii. Electronic systems which possess internet-based portals, sites or applications which is used to:
    a. Provide, manage and/or operate the following: (i) offering and/or trading of goods and/or services, (ii) financial transaction services, (iii) communication services (including, but not limited to short text messages, voice calls, video calls, emails, digital chatrooms, networking services and social media);
    b. Deliver material or paid digital content through data networks by way of downloading via websites, sending emails or via applications to customer devices;

c. search engine and electronic information provider services (in the form of text, audiovisual data, animations, music, video, films and games or any part and/or complete combination of the above); and/or
d. Processing of personal data in relation to the organization of public services which address electronic transaction activities.

Registration Requirement

GR 71/2019 requires both Private and Public ESO to register their Electronic System with the Ministry of Communication and Informatics ("**MoCI**"). The registration process is made through an integrated electronic business license service and must be completed before the electronic system can be operated by ESO users. MoCI Regulation Number 36 of 2014 about Registration Procedure of ESO states that an ESO must complete a registration form and provide the supporting documents; for example, if the applicant is a legal entity, it must provide a certificate of company registration, the latest statement of domicile, technical scheme of the Electronic System, *etc.* There will be a verification process of the submitted documents. Based on the completion of administrative requirements, no later than 3 business days, MoCI will issue the certificate of registration, and it shall be extended every 5 years.

Electronic System Requirement

With regard to the operating of the electronic system, the registered ESO must fulfill minimum requirements; namely, it must

be able to re-display information and/or electronic documents in their entirety according to the retention period required by the applicable laws and regulations, and it must be able to protect the availability, integrity, authenticity, confidentiality, accessibility of the electronic information in the administration of the electronic system.

Cooperation with Law Enforcement and Government

ESOs are required to make certain that their electronic systems do not contain or facilitate propagation of prohibited electronic information and/or documents according to the applicable laws and regulations. Information and/or electronic documents considered prohibited are ones that: (a) violate the applicable laws and regulations such as, among others, pornography, gambling, defamation, hate comments and terrorism; (b) unsettle the community and disturb public order and; (c) give way or provide access to electronic information and/or documents that contain prohibited content in accordance with the applicable laws and regulations. The inability to adhere with the above conditions can result in termination of access (access blockage, account closure and/or content removal), either directly by the government and/or by government order to ESOs to terminate access to the electronic information and/or document in violation.

Personal Data Protection

Another change made in GR 71/2019 is personal data protection which is subject to administrative sanctions on failure of compliance. The regulation sets out the provision on the process of acquiring personal data information and the storage and

removal of the related information. GR 71/2019 introduces the right to erasure (deletion) of personal data acquired and processed without the prior consent of the data owner; data with revoked consent; and data that are acquired and processed unlawfully **and** the right to delisting (removal) from search engines based on a court stipulation granted by the local district court. If the local district court grants a request for delisting (removal), ESO must comply with the court order by utilizing a removal mechanism in its electronic system.

In terms of data center, GR 71/2019 requires the Public ESO to manage, process, and/or store electronic system and data in the territory of Indonesia. The electronic system and data storage of the Public ESO may be done outside of Indonesian territory in the event that such electronic system and data storage technology is not available in Indonesia. However, an exception to such requirements only applies if the relevant committee has determined so. The restriction is now relaxed for many companies that were previously considered Public ESO (due to the clear differentiation in the present regulation). A private ESO is now allowed to manage, process, and/or store data overseas, provided that it ensures the effectiveness of supervision by MoCI or Institution and law enforcement. Nevertheless, regulatory authorities for certain business sectors may regulate matters differently.

Electronic Certificate

GR 71/19 has clarified that both Public ESO and Private ESO are now required to have an electronic certificate. Failure to comply

may result in administrative sanctions. An electronic certificate is issued by Indonesian Electronic Certificate Operator ("**ECO**") which has been acknowledged by MoCI or a Foreign ECO which has been registered in Indonesia. As far as we are aware, there are only 5 (five) local ECO that may provide an Electronic Certificate, among others (i) PT Privy Identitas Digital, (ii) Perusahaan Umum Percetakan Uang Republik Indonesia, (iii) PT Indonesia Digital Identity, (iv) Badan Pengkajian dan Penerapan Teknologi, and (v) Solusi Net Internusa.

ECO may provide 2 types of certified services: (a) electronic signature services and (b) other services which using e-certificate, consists of electronic stamp, electronic time marker, registered electronic delivery service, website authentication, and/or preservation of e-signature and/or e-stamp. E-stamp has the same purpose as e-signature, except it represents the legal entity (not an individual). Other services mentioned above which use an e-certificate are services providing or guaranteeing accuracy, validity and other similar purposes in electronic system and electronic transactions. The respective services have their own requirements which shall be ECO's obligation to comply with. It should be noted that the Indonesian ECO is liable for any losses that arise in relation to its failure to comply with the obligation under GR 71/2019, unless proven otherwise.

More Powerful Sanction Mechanism

The GR 71/2019 also has affirmed the government's authority in relation to the administration of electronic systems and transactions. Failure to comply with the obligations and/or requirements of ESO or ECO will be subject to administrative sanctions.

MoCI may impose sanctions in the form of a warning letter, fine, temporary suspension, restriction of access, and/or being removed from the list of registered ESO or ECO.

As an implementing regulation of Law No. 19 of 2016, GR 71/2019 extended the scope of restriction of access to include blocking of access, shutting down the relevant account, and/or removing the relevant content. MoCI may conduct and/or order ESO (including the internet access service providers, telecommunications network and service providers, content providers, and link provider) to conduct the termination of access, for the purpose of protecting 'public interest'. Given that provision, the government can now compel all ESO to 'support' a government sanction. Uncooperative ESO will be sanctioned under the applicable law and regulations.

Centralized Data Center

The government also introduced a provision on certain institutions and sectors that are considered to have vital information infrastructure, including: (a) government administration; (b) energy and mineral resources; (c) transportation; (d) financial; (e) health; (f) information and communication technology; (g) agriculture; (h) defense; and (i) other sectors determined by the President. Institutions who possess such strategic electronic data is required to make electronic document and electronic backup, and connect it to the centralized data center for data security purposes. This is a newly introduced requirement and this will be further regulated by the *Badan Sandi dan Siber Negara* ("**BSSN**").

Transitional Period

ESO operated prior to GR 71/2019 must comply with the registration requirements within 1 (one) year period following the enactment of GR 71/2019. In addition, within 2 (two) year, Public ESO must comply with the data center requirement that it shall be within the territory of Indonesia.

If you wish to discuss any issues relating to the information and telecommunications law, please feel free to contact any of the following MKK attorneys:

Attorneys	Telephone	E-mail
Eka Wahyuning Siswani	+62-21-5711130	ekaws@mkklaw.net
I Gusti Ngurah Oka Anantajaya	+62-21-5711130	oka.anantajaya@mkklaw.net
Jonathan Sadikin	+62-21-5711130	jonathan.sadikin@mkklaw.net

www.mkklaw.net

Please do not hesitate to contact us for any additional information you may desire regarding this newsletter or MKK. We will be happy to answer your further questions.

Mochtar Karuwin Komar
14th Floor WTC 6
Jalan Jenderal Sudirman Kav. 31
Jakarta 12820, Indonesia
Tel. +62215711130
Fax. +62215711162, +62215701686
Email: mail@mkklaw.net