

Client Alert

February 2018

Introducing Data Categorization and Leniency for Electronic System Operators Providing Public Services

For More Information:

Mark Innis
Foreign Legal Consultant
+62 21 2960 8618
mark.innis@bakernet.com

Adhika Wiyoso
Associate
+62 21 2960 8507
adhika.wiyoso@bakernet.com

Denny Ngadimin
Associate
+62 21 2960 8641
denny.ngadimin@bakernet.com

Gabriela Valencia
Associate
+62 21 2960 8560
gabriela.valencia@bakernet.com

Background

The Government (through the Ministry of Communication and Informatics ("**MOCI**")) has issued a draft amendment to Government Regulation No. 82 of 2012 ("**GR 82**") on the Implementation of Electronic Systems and Transactions ("**Draft Amendment**") for public comment and feedback. GR 82 is an implementing regulation of Law No. 11 of 2008 as amended by Law No. 19 of 2016 on Electronic Information and Transactions ("**EIT Law**").

For context, under GR 82, electronic system operators¹ that provide a "public service" were required to have onshore data centers and disaster recovery centers by 15 October 2017.

However, there has never been any clarification on the definition and coverage of "public service", there has been extensive lobbying from cloud providers and the business community (the latter on costs for business) and there have been different approaches taken by sectoral regulators. In October 2017, the MOCI indicated that it would revise GR 82 to introduce data categorization and lessen, where possible, the requirements for data localization.

The Draft Amendment addresses these points and expands on other matters. Unfortunately the Draft Amendment does not differentiate between data controllers and data processors as in other countries.

What are the Amendments?

The Draft Amendment introduces:

- A broad definition of electronic system operators that provide a "public service"

¹ Under the EIT Law and GR 82:

- "Electronic System" is defined as a series of electronic sets and procedures which function to prepare, collect, process, analyze, store, display, announce, send and/or disseminate electronic information.
- "Electronic System Operator" is defined as any person, state entity, business entity and community that provides, manages and/or operates an Electronic System whether independently or collectively to an Electronic System user for its own use and/or another party's use.

Based on the above definitions (which are broad in nature), any person or entity that manages and operates an Electronic System (such as websites, applications, email, and messengers), and provides those systems to other parties, may be considered an Electronic System Operator.





- A brand new concept of data categorization
- Implementing provisions for the registration of electronic system operators
- Implementing provisions for the right to be forgotten
- Implementing provisions for the Government's right to terminate access to electronic information and/or documents (generally in respect of unlawful online content)

Electronic System Operators Providing a Public Service - New Article 5(1a)

The Draft Amendment states that the following electronic system operators are providing a "public service", namely electronic system operators:

1. regulated or monitored by sectoral agencies and regulators
2. for governmental institutions
3. that own electronic systems that:
 - (i) Are an online portal, site or application through the internet (including digital platforms) used to facilitate offers of, and/or trade in, goods and/or services
 - (ii) Have a facility for online payment and/or financial transactions through a data communication network or the internet
 - (iii) Process electronic information containing or requiring a deposit of funds or funds equivalent
 - (iv) Are used to process, manage or store data, including personal data, for operational activities serving the public in connection with electronic transaction activities
 - (v) Are used to deliver paid digital material through a data network either by way of downloading from a portal/site, email delivery, or through any other application to the user's device
 - (vi) Provide, manage, and/or operate a communication service in the form of short message, voice call, video call, electronic mail, and online chat (chatting/instant messaging), search engine, social media and social network, and a service of provision of digital information that may be in the form of text, sound, image, animation, music, video, movie, game or a combination of any and/or all of them, including in the form of streaming or downloading.

So this is still a very broad categorization, and for example will have an impact on all websites that collect or process information, does not distinguish between public facing or non-public facing systems and potentially, given the Data Categorization issues raised below, might still mean that Indonesian citizens' personal data cannot leave Indonesia.

Subject to the Data Categorization section below (and the concern whether all Indonesian citizens' personal data can be categorized as Strategic Electronic Data), this means all the above electronic system operators need to be



registered but may not need to have onshore data centers and disaster recovery centers. The process is meant to be a registration process, although in reality to date this has been an approval process.

However, the Draft Amendment does not specifically elaborate which sectoral agencies and regulators are authorized to determine that an electronic system operator provides a "public service". The Draft Amendment only defines sectoral agencies and regulators in the context of identifying Strategic Electronic Data (see the Data Categorization section below).

In reality though, given the tenor of other amendments in the Draft Amendment, it will be left to Government sectoral agencies and regulators to make a determination in their own sectoral regulations. So in many respects the MOCI is leaving the determination to other sectoral agencies and regulators and, in the Draft Amendment, the MOCI is only focusing on electronic system operators over which it has jurisdiction.

Registration of Electronic System Operators - Articles 5(1), 5(3), 5(4a) and 5(5)

Under the Draft Amendment, there is a requirement for "public service" electronic system operators to register with the MOCI. Further, the MOCI can now coordinate the registration requirements with sectoral agencies and regulators.

The registration requirements for electronic system operators that provide either a public service or a non-public service are regulated under GR 82 and MOCI Regulation No. 36 of 2014 on Procedures for Registration of Electronic System Operators ("**MOCI Regulation 36**"). The Draft Amendment implies that registration may be voluntary for an electronic system operator that provides a non-public service.

However, neither GR 82 nor MOCI Regulation 36 (including the Draft Amendment) addresses how an offshore electronic system operator (eg, an offshore Over-The-Top (OTT) service provider) can register itself as an electronic system operator with the MOCI. The current MOCI online system for the registration of electronic system operators (ie, <https://pse.kominfo.go.id/pendaftaran-pse>) can only accommodate onshore electronic system operators.²

If the Draft Amendment were to be enacted in the current form, MOCI Regulation 36 should be amended to cover the registration of offshore electronic system operators after the Draft Amendment is enacted. This is because Article 5(5) of GR 82 and the Draft Amendment authorize the MOCI to issue a further implementing regulation on the registration of electronic system operators.

² Under the EIT Law, there is an extraterritorial provision that applies to Indonesian and foreign individuals or legal entities and to all electronic transactions conducted (i) inside Indonesia, (ii) outside Indonesia but having legal impacts in Indonesia or (iii) having legal impacts outside Indonesia but detrimental to the interests of Indonesia.



Onshore Data Center and Disaster Recovery Center Requirements - Articles 17(1)-(3)

This section should be read in conjunction with the Data Categorization section below.

Under the Draft Amendment, there is no longer a requirement for electronic system operators that provide a public service to have data centers and disaster recovery centers in Indonesia.

However, electronic system operators that provide a public service must effectively process and store Strategic Electronic Data (if any) in onshore data centers and have onshore disaster recovery centers.

In other words, electronic system operators that provide a public service can process and store any electronic data (other than Strategic Electronic Data) offshore.

Data Categorization - New Articles 83J - 83Q

The Draft Amendment introduces a new concept of data categorization. There are three types of electronic data:

1. **Strategic Electronic Data:** Data that strategically affects public interests, public services, the continuity of the State's administration, or the State's defense and security. For example, intelligence data, population data or Indonesian citizens' data, and state defense and security data. While broad and clarification is required to ensure that there is no misunderstanding, presumably it is not the Government's intention that every online application with an Indonesian citizen's identity card is considered strategic nor should large companies which obtain significant amounts of Indonesian citizens' data be caught; rather what should be caught is the centralization of such data by the Government.

Strategic Electronic Data can be managed, processed and stored through cloud computing (eg, a cloud server), but the cloud network must use electronic system networks in Indonesia (eg, managed, processed and stored in a local cloud server). Also, Strategic Electronic Data must not be delivered, exchanged or copied to overseas locations.

Further, sectoral agencies and regulators can identify which data should be categorized as Strategic Electronic Data. The "sectoral agencies and regulators" in this context include government agencies and regulators having jurisdiction over the following sectors:

- (i) Public administration sector
- (ii) Energy and mineral resources sector
- (iii) Transportation sector
- (iv) Finance sector
- (v) Health sector



- (vi) Information technology and communication sector
- (vii) Food sector
- (viii) Security sector
- (ix) Defense and defense industry sector

However, the data identified by sectoral agencies and regulators is only strategic if the following conditions are met:

- (i) If the data were to be disrupted, the data could have an effect on or otherwise cause:
 - (a) Humanity and development disasters
 - (b) Chaos in transportation and/or national communications
 - (c) Disruption in the implementation of state governance
 - (d) Disruption in the law enforcement process
 - (e) Disruption in state defense and security
 - (f) Disruption in national economic resilience

Also, sectoral agencies and regulators can identify which data should be categorized as Strategic Electronic Data based on "other criteria" under the prevailing laws and regulations.

- (ii) The data must also be confirmed by the MOCI as being Strategic Electronic Data.

While it seems that the Draft Amendment gives sectoral agencies and regulators broad authority to identify (not determine) what data should be categorized as Strategic Electronic Data under their sectoral authorities, the relevant sectoral agencies and regulators must request the MOCI to determine (read confirm) the identified data as Strategic Electronic Data.

2. *High Electronic Data*: Data that has a limited impact on the interests of electronic data owners and their sectors. For example, data related to a company's financial records or business data.

High Electronic Data can be processed and stored offshore, but must be made accessible and must be able to be processed in Indonesia for supervision and law enforcement purposes.

Further, we should note that sectoral agencies and regulators can directly determine (not identify only) what data should be categorized as High Electronic Data under their sectoral authorities.

The determination of High Electronic Data would be regulated in future sectoral regulations.



3. Low Electronic Data: Electronic data that is not categorized as Strategic Electronic Data and High Electronic Data. For example, a company's human resources or manpower administration, and public information.

Low Electronic Data can be processed and stored offshore, but must be made accessible and must be able to be processed in Indonesia for supervision and law enforcement purposes.

As with the High Electronic Data, sectoral agencies and regulators can directly determine (not identify only) what data should be categorized as Low Electronic Data under their sectoral authorities.

The determination of Low Electronic Data would be regulated in future sectoral regulations.

Government Role - New Articles 83A - 83E

The Draft Amendment outlines in very broad terms the proposed role of the Government. These provisions are principles only and include an intention:

- (i) To have an integrated national data center and national disaster recovery center for Strategic Electronic Data. This is perhaps unduly broad and centralizes data. These centers themselves could be a high risk if there were cyber attacks
- (ii) To protect critical infrastructure
- (iii) To adopt certified electronic signatures (as contemplated by the EIT Law)
- (iv) To have a national electronic system gateway, however there are no details provided.

Other Provisions

Right to be Forgotten - Articles 15A - 15D

Under the Draft Amendment, electronic system operators must delete irrelevant electronic information and/or documents within their control at the request of the relevant data owner. This right is commonly known as the right to be forgotten.

The right to be forgotten can only be exercised based on a court decision. Further, electronic system operators must have a deletion mechanism for electronic information and/or documents. Also, the Draft Amendment now specifically provides that an electronic system operator that operates a search engine must delete irrelevant electronic information and/or documents, such as deleting the display of and/or terminating access to irrelevant electronic information and/or documents based on a court decision.

The right to be forgotten was previously introduced in 2016 in an amendment to the EIT Law. The Draft Amendment deals in more detail with the processes to be undertaken in deleting irrelevant electronic information and/or documents.

Although the EIT Law (including GR 82 and the Draft Amendment, which is an implementing regulation of the EIT Law) has extraterritorial reach against



offshore electronic system operators, it remains to be seen how an Indonesian court decision could be enforced against offshore electronic system operators.

If an offshore electronic system operator did not comply with a court decision, we suspect that the Government would ultimately block access to the relevant electronic system based on its authority under the EIT Law (see the Termination of Access section below).

Termination of Access to Electronic Information or Documents with Unlawful Content - Articles 83F - 83I

Principally, Articles 83F-83I emphasize the Government's authority to terminate access to electronic information and/or documents with unlawful content (which power is granted under the EIT Law).

Access to electronic information and/or documents can be terminated if the electronic information and/or a document fulfills any of the following conditions:

- (i) It violates the prevailing laws and regulations (eg, electronic information and/or a document contains material relating to pornography, terrorism, separatism, gambling, hate speech and intellectual property infringements).
- (ii) It disturbs the public and/or public order.
- (iii) It can lead to or provides access to electronic information and/or documents with unlawful content.

The Draft Amendment further provides that government institutions, law enforcement authorities and judicial authorities (eg, courts) can request the MOCI to terminate access to unlawful content. This provision gives the MOCI a firmer legal basis to do so (in addition to MOCI Regulation No. 9 of 2014 on Negative Internet Content ("**MOCI Regulation 9**")).

In addition, the obligation to terminate access to electronic information and/or documents with unlawful content applies not only to electronic system operators, but also to telecommunication network operators and telecommunication service providers (including internet service providers, content service providers, and link operators providing a traffic network to the electronic information and/or documents with unlawful content).

Otherwise, the Government (through the MOCI) could ultimately block access to the relevant electronic system on the basis that the relevant electronic system contains unlawful content.

While there is a safe harbor provision under MOCI Circular Letter No. 5 of 2016 on Limitation and Responsibility of Platform Providers and Merchants through Electronic System (Electronic Commerce) in the Form of User Generated Content ("**MOCI Circular Letter**"), the MOCI has blocked some offshore electronic system operators in the past (eg, chat messaging services and picture hosting platforms) until the offshore electronic system operators removed the unlawful content from their user-generated content platforms.



It remains to be seen how the Draft Amendment would affect MOCI Regulation 9 and the MOCI Circular Letter. Perhaps after the Draft Amendment is issued the MOCI would (i) amend MOCI Regulation 9 and the MOCI Circular Letter or (ii) combine MOCI Regulation 9 and the MOCI Circular Letter into a new MOCI regulation.

Sanctions

The Draft Amendment provides that many of its provisions are subject to administrative sanctions (namely warning letters, fines, temporary suspension of operations and ultimately termination of access). However, it does not preclude civil and criminal liability provided for in other regulations, including the EIT and GR 82.

Transitional Period

The Draft Amendment will become effective when the Draft Amendment is enacted. However, there is a one-year transitional period for existing electronic system operators to comply with the Draft Amendment.

Conclusion

The Government intends to relax the onshore data center and disaster recovery center requirements for electronic system operators that provide a "public service" through the concept of data categorization.

However the MOCI should further clarify the Draft Amendment to ensure that:

- the concept of "public service" is further narrowed
- there is a clear position on the registration of offshore electronic system operators
- Indonesian citizens' personal data can be collected and transferred offshore and is not caught by the definition of Strategic Electronic Data
- the private sector is not required to use an integrated national data center and national disaster recovery center or a national electronic system gateway, nor is source code required to be provided to government agencies.

Electronic system operators should do the following:

- (i) Consider how the Draft Amendment will impact them
- (ii) Lobby the relevant sectoral agencies and regulators on what will be considered Strategic Electronic Data under their sectoral authorities
- (iii) Ascertain from the MOCI how the right to be forgotten can be enforced against offshore electronic system operators (particularly offshore electronic system operators that operate a search engine)
- (iv) If the Draft Amendment were to be substantially enacted in the current form, consider what approach will be taken to comply with the Draft Amendment.

www.hhp.co.id

Hadiputranto, Hadinoto & Partners
The Indonesia Stock Exchange
Building, Tower II, 21st Floor
Sudirman Central Business District
Jl. Jenderal Sudirman Kav. 52-53
Jakarta 12190
Indonesia

Tel: +62 21 2960 8888
Fax: +62 21 2960 8999

©2018 Hadiputranto, Hadinoto & Partners is a member firm of Baker & McKenzie International, a global law firm with member law firms around the world. In accordance with the common terminology used in professional service organizations, reference to a "partner" means a person who is a partner or equivalent in such a law firm. Similarly, reference to an "office" means an office of any such law firm.

This may qualify as "Attorney Advertising" requiring notice in some jurisdictions. Prior results do not guarantee similar outcomes.