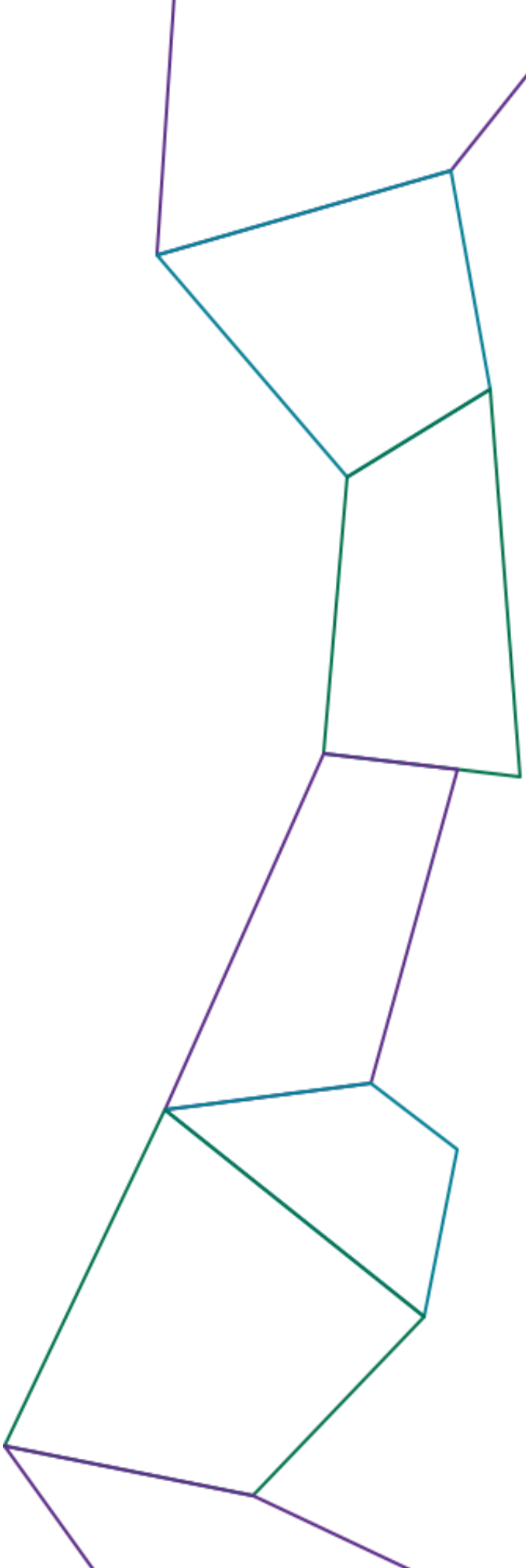

ROUSE

Digital Services Regulations Guide

Indonesia

TABLE OF CONTENTS

DIGITAL SERVICES REGULATIONS: INDONESIA

The myriad of laws and regulations (at the Government and Ministerial level) on digital service/electronic transactions makes it difficult to navigate the Indonesian regulatory framework. This note is an update of a previous note on applicable regulations.

Regulatory regime of electronic system operator (ESO)

The principal legislation/regulations relevant to Electronic System Operators ("**ESO**") are:

- Law No. 11 of 2008 on Electronic Information and Transaction Law as amended by Law No. 19 of 2016 ("**EIT Law**")
- Government Regulation No. 71 of 2019 on Organization of Electronic system and Transactions ("**GR 71**")
- Law No. 27 of 2022 concerning Personal Data Protection Law (the "**PDPA**")
- Government Regulation No. 80 of 2019 on Trade Through Electronic Systems ("**GR 80**")
- Ministry of Communication and Informatics Regulation No. 5 of 2020 on Electronic System Operator Private Scope ("**MOCI 5/2020**")
- Ministry of Communication and Informatics Regulation No. 20 of 2016 on the Protection of Personal Data Protection in Electronic Systems ("**MOCI 20/2016**")
- Ministry of Trade Regulation No. 50 of 2020 on Provisions of Business Licensing, Advertising, Counting, and Supervision of Business Acceptors in Trade Through Electronic Systems ("**MOT 50/2020**")
- Law No. 8 of 1999 on Consumer Protection ("**Consumer Protection Law**")

This note is applicable to ESOs in the private sector which is defined in Article 1(6) of GR 71/2019 (read with Article 1(1) GR 71/2019) and Article 1(6) of MOCI 5/2020.

> *Article 1(6) GR 71/2019*
> *Electronic System Provider in the Private Sector is the organization of Electronic System by a Person, Business Entity, and public.*
>
> *Article 1(6) of MOCI 5/2020*
> *Electronic System Provider (Penyelenggara Sistem Elektronik) in the Private Sector, from this point onward is referred to as PSE in the Private Sector, is the organization of Electronic System by a person, business entity, and the community.*
>
> *Article 1(1) GR 71/2019*
> *Electronic System is a series of devices and electronic procedures which function to prepare, collect, process, analyze, store, display, announce, transmit, and/or disseminate Electronic Information.*

Reference to ESOs includes digital services such as social media platforms , electronic commerce provider and OTT (i.e., over-the-top media) services.

The key requirements are:

- Registration of ESO with the Ministry of Communication and Information under Article 2 of MOCI 5/2020;
- Setting up of representative office in Indonesia where the transactions exceed 1000 a year or has delivered 1000 packages to consumers a year under Article 15 of Trade Regulation 50/2020 (MOT 50/2020);
- Terms of use and privacy policy to be in Indonesian language under Article 47(1) of GR 71;

- Provide contact information for directing consumer complaints in the case where trade is being provided by the ESO under Article 26 (3)(f) of MOT 50/2020; and
- Collection and use of personal information should be based on one of the following legal bases : consent; contract; legal obligation; vital interests; public task; or legitimate interests. See this page for detailed discussion of the 2022 Personal Data Protection Act.

Registration of ESO with Ministry of Communication and Informatics ("MOCI")

ESOs, including foreign based ones, that provides web services in Indonesia are required to register with the MOCI. (Article 4(1) of MOCI 5/2020)

This Ministerial Regulation is meant to implement GR71.

Sanctions for failing to register is provided in Article 7(2) of MOCI 5/2020 which includes access blocking:

> *"In the event that PSE in the Private Sector do not register as referred to in paragraph (1)(a), the Minister shall impose an administrative sanction in the form of Electronic System Access Blocking."*

Setting up a local representative office

Where the number of trade transactions exceed 1000 per year or more than 1000 deliveries have been made per year, the Foreign Trade Operators through Electronic Systems ("**PPMSE**") must set up a local representative office.

This is based on Article 15 (1) and (2) of MOT 50/2020 which states:

(1) The foreign PPMSEs (as referred to in Article 2(1)(b) that meets certain criteria are required to appoint a representative domiciled within the jurisdiction of the Unified State of the Republic of Indonesia which may act as and on behalf of the PPMSE concerned.

(2) The 'certain criteria' for foreign PPMSEs as referred to in (1) consists of:
   a. already made transactions with more than 1.000 (one thousand) Consumers within a one-year period; and/or
   b. already deliver more than 1.000 (one thousand) packages to Consumers within a one-year period.

Other pertinent regulatory requirements to meet consumer protection laws under MOT 50/2020:

Article 26 (3)(f) on provisions to forward contact details to representatives of foreign electronictrade operators:

(1) The representative of foreign Trade Operators through electronic systems/PPMSE should make available contact numbers and/or email addresses of the consumer complaint services provided by the represented foreign PPMSE; and
(2) The representative office is to fulfill consumer protection obligation on behalf of the foreign PPMSE.

Article 26 (5) explains the purpose of above requirements - for the foreign trader to::

- fulfilling its consumer protection obligation;
- performing guidance to increase competitiveness; and
- settling disputes.

In the event of termination of an existing representative office, a replacement should be appointed within 14 days. Article 30 of MOT 50/2020 stipulates:

> *"In the event of a unilateral termination of representation, foreign PPMSEs are required to appoint a new representative within a maximum period of 14 (fourteen) calendar days after one of the parties declared the termination concerned in writing".*

Sanction for failing to appoint representative office.
Article 46 of MOT 50/2020 stipulates sanctions that shall be imposed on foreign PPMSEs which fulfil the criteria stipulated in Article 15 but do not appoint its representative in Indonesia. The sanction will be in the form of written warnings that will be given up to 3 (three) times with a maximum of 14 (fourteen) calendar days grace period between each warning. Failure to comply within the period will result in the foreign PPMSE being put on a blacklist and temporary suspension of the foreign PPMSE's services by the authorized relevant agency.

Data Protection

The personal data protection legislation (**PDPA**) was passed on 17 October 2022. Please refer to this page for an overview of the PDPA.

In addition to complying with the PDPA, operators of web services also need to comply with pre-PDPA regulations that are specifically directed at electric systems. The source of law/regulations on protection of personal data in electronic system is found in the following:

- EIT Law, in particular Article 26;
- GR 71 Articles 14, 15, 16, 17, and 18; and
- MOCI 20/2016.

These pre-PDPA regulations applies where personal data is collected in electronic systems. The following discusses protection of personal data which is collected in such environment. Where applicable, these pre-PDPA requirements will be contrasted with those under the PDPA.

Definition of "Personal Data"
Article 1(29) of GR 71 defines 'Personal Data' as:

> "*All data related to a person, whether identified or capable of being identified using that data or in combination with other information, whether directly or indirectly, through the use of an electronic system and/or non-electronic means*."

The local data protection regime in the context of electronic system are:

When collecting, processing, analysing, retaining, displaying, announcing, sending and publishing personal data of its users, ESOs must obtain the *consent of the personal data owner* in respect of the aforesaid activities including the purpose for which the data is collected, processed and stored (Article 14(3) GR 71). For example, if the personal data is analysed, and used for marketing purposes, such purposes must be informed to the users.

Retention of data
Data and information relating to financial transactions to be retained for a minimum period of 10 (ten) years from

when data and information were obtained, while PMSE data and information not relating to non-financial transactions for a minimum period of 5 (five) years from when data and information were obtained (Article 25(1) GR 80).

Personal data must be stored in encrypted form (Article 15(2) MOCI 20/2016) and minimum period for 5 years (Article 15(3)(b) MOCI 20/2016).

Electronic system operator must provide access for lawful interceptions and permit the gathering of evidence for criminal investigations if requested by law enforcement agencies under the following provisions:

Article 32 of MOCI 5/2020:

(1) PSE in the Private Sector shall grant access to Electronic Data to Law Enforcement Apparatus for investigation, prosecution, or trial of criminal acts within the jurisdiction of the Republic of Indonesia.

(2) Criminal acts as referred to in paragraph (1) are criminal acts in which the criminal punishment is in the form of imprisonment for a minimum of 2 (two) years.

Article 33 of MOCI 5/2020:

(1) PSE in the Private Sector shall grant access to Electronic System to Law Enforcement Apparatus for investigation, prosecution, or trial of criminal acts within the jurisdiction of the Republic of Indonesia.

(2) Criminal acts as referred to in paragraph (1) are criminal acts in which the criminal punishment is in the form of imprisonment:

a. for a minimum of 5 (five) years;

b. below 5 (five) years but must not be below 2 (two) years as long as it has obtained a ruling from the district court within the jurisdiction where the Law Enforcement Apparatus has jurisdiction.

Cross border transfer of data

In addition to securing consent from the users, when a cross-border transfer of the customers' personal data from Indonesia occurs, ESOs must submit to MOCI pre and post notification of such transfer (Article 22 of MOCI 20/2016).

The above is in addition to the requirement under the PDPA provisions:

- data Controller to ensure that the receiving party's country has the same level of or better personal data protection standard.
- If not, data Controller to ensure adequate and binding effort for personal data protection.
- where both of the above conditions cannot be met, data controller must obtain consent from the relevant personal data subjects.

Deleting or erasing data

ESOs are to delete data on request pursuant to Article 26 of Regulation 20/201, Article 15(2) read with Article 16(1) of GR 71/2019 - when the data is no longer relevant and upon request.

Contrast with PDPA - Controllers are to end processing of data in one of these circumstances (Article 42) :

- the processing has reached the retention period;
- the purposes have been achieved; or
- at the request of the data subject

The obligation to delete data is in article 43 PDPA. Data subject to be notified of deletion (article 45)

Data breach
Under Article 28(c)(4) of MOCI 20/2016, ESO is obliged to issue notification of data breach to the relevant personal data owner within 14 days from the leak occurrence.

Under the PDPA, the time for notification is shortened to 3x24 hours from breach under the PDPA.

See this link for an overview of the PDPA.

Location of Data

ESOs in the private sector may locate their data outside Indonesia (Article 21 of GR 71). However, this allowance might be impinged upon by regulations applicable to specific sectors such as Ministry of Finance.

Further, additional measures are required to protect data of a strategic nature. Although ESOs may locate their data outside Indonesia, they must ensure that their electronic systems and data are accessible to the Indonesian authority for supervision and law enforcement.

Content related obligations of ESOs

PSE in the Private Sector are to provide user guidelines in Indonesian language in accordance with the provisions of laws and regulations (Article 9(2) MOCI 5/2020) and any electronic contract addressed to Indonesian citizen shall be in Indonesian language (Article 47(1) GR 71).

ESOs are required to ensure that their electronic system does not (Article 5 of GR 71):

- contains the electronic information and/or electronic documents that contravenes existing law/regulation; and
- facilitates the distribution of the prohibited electronic information and/or electronic documents.

Under Article 9(2) and (3) of MOCI 5/2020, Private ESPs are required to comply with several content moderation obligations, particularly to:

- provide guidelines for the electronic system in the Indonesian language;
- ensure that no prohibited information or documents exist within the electronic system; and
- ensure that the electronic system does not facilitate the spread of prohibited information or documents.

Article 9(4) of MOCI 5/2020 has expanded the scope of prohibited electronic information and documents to now cover any electronic information/document (Prohibited Content) that:

- violates the prevailing laws and regulations;
- causes disturbances to society and public order; and/or
- provides methods or access to prohibited information or documents.

User Generated Content ("UGC")

The following discusses safe harbor provisions relating to UGC.

User Generated Content ESO is defined under Article 1(7) of MOCI 5/2020 as:

> *"ESO in the Private Sector of which the provision, presentation, uploading, and/or exchange of Electronic*

Information and/or Electronic Document is conducted by Users."

ESO offering platforms for UGC should stipulate governance terms and conditions in respect of obligations for posting UGCs (Article 10(1)(a) and (2) of MOCI 5/2020). In particular, ESOs are to provide procedure for dealing with complaints against legality of UGC and facility for settlement of complaints (Article 10 (1)(b), (3) and (4) of MOCI 5/2020).

Article 11 of MOCI 5/2020 exempts online intermediaries that provide UGC from being liable for hosting prohibited content if they maintain the above-mentioned facility for complaint reporting and settlement. UGCs are additionally defined under MOCI 5/2020 as Electronic Information provided, presented, uploaded by subscribers. Private ESPs provides platforms where subscribers can provide, present, upload and/or exchange electronic information and/or documents.

UGCs are required to exercise governance on the use of their information technology by establishing procedures (Procedural Governance) and reporting tools for the public to report or submit complaints about any Prohibited Content (Reporting Tools).

UGCs will be exempted from Prohibited Content violations under MOCI 5/2020 if the UGC:

- complies with the obligation to ensure that the electronic system neither contains nor facilitates the spread of Prohibited Content;
- complies with the obligation to provide Procedural Governance and Reporting Tools;
- provides the relevant subscriber information of the user that has uploaded Prohibited;
- content in the context of law enforcement/supervision; and
- takes down the Prohibited Content.

Marketing activities/advertisements

Consent is required in the use of personal contact information for marketing activities. In the case of financial service provider, OJK prohibits any financial service provider from making direct marketing communications without prior customers' consent (Article 19 of OJK Regulation 1/POJK.07/2013).

In particular, the sender of electronic information (which includes marketing material) should ensure that this does not cause disturbance to the recipient (Article 44 GR 71)

Furthermore, Article 19(2) of MOT Reg 50/2020 requires all electronic advertisement to fulfil the following:

- not deceive consumers on quality, quantity material, utility and price of goods and/or fee of services, as well as the expected time of arrival;
- not mislead in respect of warranty of goods and/or services;
- not contain untrue, false, or inaccurate information; and
- provide clear exit function (e.g., terminate or skip button) on the displayed electronic advertisement.

Also note the requirement under Article 17 of Consumer Protection Law, which requires all advertisers to comply with the advertisement code of ethics as issued by the Indonesian Advertising Council.

Sanctions

Article 95 of GR 71 provides that the Government is authorized to prevent the dissemination and use of electronic

information and/or an electronic document by means of: blocking of access; and/or an instruction to an ESO to block access.

Under Article 96 of GR 71, these measures may be taken in respect of electronic information and/or an electronic document that:

- violates the provisions of the laws and regulations;
- causes public disquiet and disturbs public order; or
- provides know-how to access, or provides access to, electronic information and/or an electronic document that contains content that is prohibited by law.

The Elucidation of Article 96 of GR 71 explains that prohibited content includes electronic information and/or an electronic document that contains or promotes any of the following elements:

> *"Pornography, slander, fraud, hatred against a particular ethnic group, religion, race or group, violence/violence against children; infringement of intellectual property rights; trading of prohibited goods/services; terrorism and/or radicalism; separatism and/or dangerous prohibited organizations; violations of data security; violations of consumer protection; violations in the health field; and violations related to food and drug supervision."*

Validity of Click Wrap Agreement

The validity of click wrap agreement is unclear. Although the current legislation recognises electronic contract and electronic signature[1], it is unclear how the court will accept as proof of execution. This is because the same legislation also provides for the use of electronic signature (which can be certified or uncertified - Article 60(2) of GR 71).

In the event of dispute, Indonesian courts might expect to see contract in the traditional form with signatures in order for the contract's existence to be proved. But this problem might be ameliorated by providing governing law with a stronger framework supporting electronic transaction and also providing for arbitration as means of dispute resolution.

Language of Terms of Use and Privacy Policy

Indonesian language is to be used for contractual terms, terms of use and privacy police. This is based on the following legislations/regulations:

Article 31 of Law No. 24 of 2009 on Official Flag, Language and Emblem, and Official Anthem ("**Law 24/2009**"):

> *"Indonesian Language must be used in a memorandum of understanding or agreement involving state institutions, government agencies of the Republic of Indonesia, Indonesian private entities or Indonesian citizens.*
>
> *The memorandum of understanding or agreement as referred to in paragraph (1) which involves a foreign party shall also be written in the national language of the foreign party and/or in English."*

[1] Article 1 (17) of EIT Law defines electronic contract as agreement that is made via electronic system. Also refer to Article 1 (3) of EIT Law: "*An electronic transaction is a legal action that is performed using the Computer, network Computer, and/or other electronic media*."

Article 47(1) of GR 71:

> *"The Electronic Contract and other contractual forms as referred to in Article 46(1) which is addressed to Indonesian citizens shall be drafted in Bahasa Indonesia."*

Article 9(2) MOCI 5/2020:

> "*PSE in the Private Sector must provide user guidelines in Indonesian language in accordance with the provisions of laws and regulations*."

English language version can be agreed to be the prevailing version as stipulated in Article 26 (3) and (4) of President Regulation No. 63 of 2019 on Usage of Indonesian Language (**PR 63/2019**):

> *"The national language of the foreign party and/or English as referred to in paragraph (2) shall be used as the equivalent or translation of the Indonesian Language to unify the understandings upon the memorandum of understanding or agreements with foreign parties.*
>
> *In the event that there is a difference in interpretation toward the equivalent or translation as referred to in paragraph (3), then the language to be used shall be the language agreed upon in the memorandum of understanding or agreements."*

Content Management

In GR 71/2019, more flexible provision on data management is directed to both ESO for Public Scope and ESO for Private Scope.

Public 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.

Private Scope

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.

MOT Reg 50/2020 does not differentiate between domestic and foreign PSPs and both must secure a SIUPMSE license from the OSS Agency.

Online Advertisements

E-commerce businesses are permitted to distribute online advertisements provided they comply to applicable laws and regulations in Indonesia.

Article 19(2) of MOT 50/2020 does state several requirements online advertisements should satisfy. These include:

- Must not deceive consumers on the quality, prices, materials, and quantity, or other false and incorrect information for the goods/service being provided;
- Must not provide false claims with regards to warranties or guarantees;
- The company must provide the usage risks for the said goods/services being advertised
- All electronic advertisements should have an exit function, such as through a 'skip' or 'close' button to close the advertisement; and
- Consumers can make complaints for ads that are not incompliance with the relevant laws and regulations through the Director-General of Consumer Protection and Trade Compliance.

Cloud Computing Private ESO

Cloud ESPs are defined under MOCI 5/2020 as Private ESPs that provide, organise, manage and/or operate cloud computing services. To comply with the requirement for an electronic system to neither store nor spread Prohibited Content, Cloud ESO must also exercise Procedural Governance, which must include at least having in place guidance on:

- users' rights and obligations to use the relevant cloud computing services;
- the cloud computing provider's rights and obligations; and
- users' accountability if the user stores Prohibited Content.

The requirements for transferring personal data out of Indonesia is not being enforced for now. The requirements under MOCI 20/2016 (Article 22) on delivery of personal data managed by ESO's domiciled in Indonesia to outside of Indonesia are as follows:

- Coordinate with the Minister or officials/institutions given the authority to do so; and
- Apply the provisions of laws and regulations regarding the exchange of Personal Data across national borders

However, the MOCI has not begun to enforce this and businesses file volunteer reporting of such transfer as attempts to comply with the above.