



July 2022 – Issue 3

ABOUT M&T ADVISORY

M&T Advisory is a digital publication prepared by the Indonesian law firm, Makarim & Taira S.

It informs generally on the topics covered and should not be treated as legal advice or relied upon when making investment or business decisions.

Should you have any questions on any matter contained in M&T Advisory, or other comments in general, please contact us at the emails provided at the end of this article.

ADDRESS

Summitmas I, 16th & 17th Floors
Jl. Jend. Sudirman Kav. 61-62
Jakarta 12190

PHONE

+6221 5080 8300 | +6221 252 1272

FAX

+6221 252 2750/51

 makarim.com  Makarim & Taira S.

Registered Foreign Electronic System Organizers (ESOs) in Indonesia. What to do next?

Electronic System Organizers (“**ESO**”) in the private sector, that include foreign private ESOs, which have been registered with the Minister of Communication and Informatics Regulation (“**MOCI**”) are subject to a number of obligations under MOCI Regulation No. 5 of 2020 on ESOs in the Private Sector as amended by MOCI Regulation No. 10 of 2021 (“**MOCI Regulation 5/2020**”), as the implementing regulation of Government Regulation No. 71 of 2019 on the Organization of Electronic Systems and Transactions (as summarized below).

Foreign private ESOs referred above mean private ESO operators that are established under the laws of another country or permanently domiciled in another country and meet the following criteria (i) they provide services within the territory of Indonesia; (ii) they do business in Indonesia, and/or (iii) their electronic systems are used or offered in Indonesia.

A foreign private ESO that has successfully registered with the MOCI will be listed in the MOCI’s official website (<https://pse.kominfo.go.id/home/pse-asing>).

Handling Prohibited Electronic Information or Documents

Under MOCI Regulation 5/2020, foreign private ESOs are responsible for the organization of their electronic systems and the management of electronic information and electronic documents in their electronic systems in a manner that is reliable, safe and responsible.

Further, foreign private ESOs must ensure that their electronic systems do not contain or facilitate the dissemination of prohibited electronic information or documents. Prohibited electronic information or documents are classified as electronic information or documents that:

1. violate the prevailing laws and regulations;
2. are unsettling for the public or threaten public order; or
3. provides ways or access to distribute illegal electronic information or documents.

If a foreign private ESO does not comply with the above obligations, its access to the electronic system in Indonesia will be blocked by the MOCI.

Private User Generated Content ESOs

A private user generated content ESO (that is, a foreign private ESO in which the provision, broadcasting, uploading and/or exchange of electronic information or documents is conducted by the electronic system users, eg applications such as *Twitter*, *TikTok* and *Instagram*), must ensure that their electronic systems do not contain or facilitate the dissemination of prohibited electronic information or documents. To do so, private user generated content ESOs must:

1. have procedures in place regarding electronic information or documents that cover the following:
 - a. the obligations and rights of electronic system users regarding the use of the electronic system's services;
 - b. the obligations and rights of the foreign private ESO regarding the operation of the electronic system;
 - c. liability related to the electronic information or documents uploaded by the electronic system's users; and
 - d. the availability of facilities and services and the settlement of complaints;
2. provide a reporting mechanism accessible to the public and foreign private ESOs must:
 - a. respond to any complaint/report;
 - b. conduct an independent examination of a complaint/report or request the verification of the complaint/report it to the MOCI or the related ministry or institution;
 - c. notify its electronic system's users of the complaint/report about electronic information or documents uploaded by an electronic system user; and
 - d. reject any complaint/report if the reported electronic information or document is not prohibited.

If a foreign private ESO does not comply with the above obligations, its access to the electronic system in Indonesia will be blocked by the MOCI.

A private user generated content ESO may be exempted from legal liability regarding electronic information and documents that are prohibited from being transmitted and distributed through its electronic system if the private user generated content ESO:

1. has complied with all its obligations explained above;
2. provides information about the subscriber (whose electronic data is controlled or managed by the foreign private ESO) that uploaded the prohibited electronic information or document; and
3. blocks access to the prohibited electronic information or document.

Cloud Computing Organizers

A cloud computing organizer is a foreign private ESO that provides, organizes, manages and/or operates cloud computing. For example, parties that can be categorized as cloud computing organizers may include *Dropbox* and *Google Drive*.

Cloud computing organizers must ensure that their electronic systems do not contain or facilitate the dissemination of prohibited electronic information or documents. To do so, cloud computing organizers must have procedures in place regarding electronic information and documents, that cover the following:

1. the obligations and rights of cloud computing organizer users that are using their cloud computing;
2. the obligations and rights of cloud computing organizers regarding the operation of their cloud computing; and
3. the liability of the cloud computing organizer's users regarding storing electronic information and documents in their cloud computing.

Cloud computing organizers must also provide electronic information and documents regarding their cloud computing organizer users that they own for the purpose of supervision and law enforcement.

Access to Electronic Systems and Electronic Data for Government Authorities

For the purpose of supervision and law enforcement, Indonesian ministries, institutions and law enforcement agencies can request access to a foreign private ESOs' electronic system and electronic data, and the foreign private ESO must provide them access upon receipt of a request from the government authority.

For this, foreign private ESOs must appoint at least one liaison officer (an individual) who is domiciled in Indonesia to be in charge of handling requests for access from the Indonesian government authorities.

Personal Data

Foreign private ESOs must comply with the relevant personal data regulations, including to protect against personal data if they wish to process the personal data (which includes acquiring, collecting, processing, analysing, storing, displaying, publishing, transmitting, distributing or deleting personal data). In brief, according to MOCI Regulation No. 20 of 2016 on Personal Data Protection in Electronic Systems (“**MOCI Regulation 20/2016**”), any personal data can only be processed after a prior consent of the data owner has been obtained and that must be in the Indonesian language.

MOCI Regulation 5/2020 defines personal data as certain individual data (whether identified or identifiable or combined with other information directly or indirectly through an electronic system or non-electronic system). Meanwhile, according to MOCI Regulation 20/2016, it is defined as certain individual data that is stored, maintained, the veracity of which is sustained, and the confidentiality of which must be protected.

Further, MOCI Regulation 5/2020 also defines specific personal data, which is health data and information, biometric data, genetic data, sexual life or orientation, political views, child data, personal financial data and other data according to the prevailing laws and regulations. This specific personal data must be provided to law enforcement agencies (as explained above) upon their request for law enforcement purposes for crimes committed in Indonesia for which the prison sentence is at least 2 years.

Other obligations

Foreign private ESOs must also comply with the following obligations, among others:

1. to provide an audit trail of the electronic system’s activities;
2. in the event of a system failure or disruption that may seriously impact the electronic system:
 - a. to secure all electronic information and documents;
 - b. at the earliest opportunity, to report the failure or disruption to the relevant law enforcement agencies and ministries/agencies;
 - c. to install prevention and mitigation measures such as an antivirus, antispam, firewall or intrusion detection system in the electronic system;
3. to provide users guidelines in the Indonesian language;
4. to ensure that their information security complies with the prevailing laws and regulations;
5. to conduct an electronic system feasibility test in accordance with the prevailing laws and regulations; and
6. to provide access to the electronic system and electronic data to ensure the effectiveness of supervision and law enforcement in accordance with the prevailing laws and regulations.

MOCI Regulation 5/2020 also requires a foreign private ESO that has obtained an ESO Registration Certificate and made changes to, among other things, its general overview of the electronic system's operation, its commitment to protect personal data or the details of the system's owner, the person in charge, the number of users or the transaction value in Indonesia etc., to inform the MOCI of the amendments. Failure by an ESO to comply with this requirement will be subject to progressive sanctions starting with written warnings, followed by a temporary blocking of access, and finally, permanent blocking of access together with the revocation of the ESO Registration Certificate.

Overseas E-commerce Organizers

Private foreign ESOs that provide electronic systems to be used for e-commerce business activities may fall under the definition of overseas e-commerce organizers ("**Overseas E-commerce Organizers**") and therefore, subject to Minister of Trade Regulation No. 50 of 2020 on Provisions on Business Licensing, Advertising, Guidance and the Supervision of Business Actors in Trading through Electronic Systems ("**MOT Regulation 50/2020**").

Under MOT Regulation 50/2020, Overseas E-commerce Organizers must establish an Indonesian Trading Representative Office (*Kantor Perwakilan Perusahaan Perdagangan Asing di bidang Perdagangan melalui Sistem Elektronik – KP3A Bidang PMSE*) if they meet the following criteria:

1. they have facilitated transactions with more than 1,000 consumers in Indonesia within 1 year;
or
2. they have delivered more than 1,000 packages to consumers in Indonesia within 1 year.

One Trading Representative Office can only represent one Overseas E-commerce Organizer.

Although strictly reading the regulation, the obligation to establish a Trading Representative Office only applies to foreign ESOs that provide electronic systems to be used for e-commerce businesses, currently, the Online Single Submission ("**OSS**") system does not differentiate between the requirements for electronic systems for trading and for non-trading activities. As a result, after the ESO registration has been completed, the OSS automatically generates a reminder that all foreign private ESOs that meet the threshold in 1. or 2. above must establish a Trading Representative Office.

Sanctions

If a foreign private ESO fails to comply with MOCI Regulation 5/2020, it may have the following administrative sanctions imposed on it:

- a. a written warning (through electronic mail/other electronic media);
- b. a fine;
- c. a temporary suspension of its business (which we believe would be more relevant to local ESOs);

- d. the revocation of its evidence of the organizer's registration (through electronic mail/other electronic media); and
- e. the termination of access to its electronic system.

The MOCI can impose all the above administrative sanctions regardless of what legal jurisdiction the private ESO falls under.

Further, in relation to prohibited content, the public, ministries, institutions, law enforcement agencies and the courts can submit requests to the relevant ministries or the MOCI for the termination (taking down) of access to prohibited electronic information and documents. Requests can be submitted through the following media:

1. the website or application;
2. non-electronic mail; and
3. electronic mail,

Accompanied by certain information including, at least, the following:

1. the applicant's identity;
2. an image or screen capture that displays the prohibited electronic information or document;
3. a link or URL that links to the prohibited content to which the termination of access is being applied for; and
4. the reason for the application.

Upon instructions from the MOCI, the foreign private ESO in question must process the termination of access order within 1x24 hours of receiving the instruction, or if the content requires urgent action (eg materials related to child pornography or terrorism, or materials likely to threaten public order), within 4 hours of receiving the instruction from the MOCI. If a private ESO fails to terminate access or takes too long to do so, the MOCI may block the private ESO's access to its electronic system or instruct internet service providers to block access to it through the foreign private ESO's electronic system.

If a foreign private ESO's access to the electronic system is blocked it can submit a request for normalization/the restoration of its access to the MOCI.



Fanissa Runalita

Associate

fanissa.runalita@makarim.com



Maria Sagrado

Partner

maria.sagrado@makarim.com