ATD LAW
in association with
MORI HAMADA

Newsletter

June 2, 2025

New and Improved Regulation for Public Electronic Service Operator

Abadi Abi Tisnadisastra
Partner
abadi.t@morihamada.com

Prayoga Mokoginta
Senior Associate
prayoga.m@morihamada.com

Aloysius Andrew Jonathan
Associate
andrew.j@morihamada.com

Introduction

On 18 March 2025, the Ministry of Communication and Digital Affairs ("MOCD") issued MOCD Regulation No. 5 of 2025 on Public Scope Electronic System Operators ("MOCD Reg. 5/2025"). The regulation serves as an implementing regulation of Government Regulation No. 71 of 2019 ("GR 71/2019") and replaces the Ministry of Communication and Informatics Regulation No. 10 of 2015. It updates the regulatory framework applicable to public scope electronic system operators ("Public ESOs").

MOCD Reg. 5/2025 introduces a number of significant changes and enhancements, including: (i) a clearer classification of Public ESOs, (ii) more detailed registration requirements for Public ESOs, (iii) specific requirements for Public ESOs that facilitate user-generated-content, (iv) expanded authority for MOCD to block access and issue content takedown orders, (v) a risk-based approach to data classification, and (vi) specific transitional deadlines for compliance.

A summary of several key provisions of MOCD Reg. 5/2025 is provided below.

I. Classification of Public ESOs

MOCD Reg. 5/2025 finally provides much-needed clarity on the scope of Public ESOs, confirming that the term is not limited to government agencies. In addition to legislative, judicial, and executive bodies established by law, an institution may qualify as a Public ESO if it is appointed by a government agency under a specific law or regulation.[1] To be eligible for such appointment, the institution must (i) be registered as a private scope electronic service operator ("Private ESO"), (ii) be an Indonesian entity, and (iii) have a data centre located in Indonesia. This means that a Private ESO can be appointed as a Public ESO, but only if the appointment is formalized through a specific regulation. MOCD Reg. 5/2025 specifically excludes supervisory and regulatory authorities in the financial sector (e.g., OJK, BI) from being classified as Public ESOs.

Under GR 71/2019, the definition of a Public ESO is relatively broad, covering "government agencies or institutions which are appointed by such government agencies to operate and manage electronic systems on their behalf."[2] This broad framing created lingering uncertainty regarding the boundaries of what constitutes a Public ESO—particularly whether a Private ESO acting as a service provider to government agencies could be deemed a Public ESO by implication. MOCD Reg. 5/2025 resolves this ambiguity by confirming that a Private ESO will only be classified as a Public ESO if it is expressly appointed by laws or regulations.

II. Mandatory Registration Requirements for Public ESOs

MOCD Reg. 5/2025 sets out detailed requirements and procedures for Public ESOs to register with the MOCD. This registration is required to be completed before their systems can be made available for user access. The registration must be carried out by an appointed "registration officer" who must be: (i) a state civil apparatus for a Public ESO that is a government agency; or (ii) a permanent employee for a Public ESO that is an appointed institution.[3] As part of the registration process, Public ESOs must submit the following information:[4]

- general information about the operation of the electronic system;
- confirmation of compliance with information security obligations;
- confirmation of the implementation of a security system, which includes measures to prevent and mitigate risks of system failure, data loss, or interference;

[1]Article 3 of MOCD Reg. 5/2025
[2]Elucidation of Article 2(3) of GR 71/2019
[3]Article 6 of MOCD Reg. 5/2025
[4]Article 11 of MOCD Reg. 5/2025

- confirmation of compliance with personal data protection obligations;
- confirmation of the performance of electronic system due diligence; and
- confirmation of compliance with the central government's and regional government's national electronic-based governance system architecture requirements.

The general information on the operation of the electronic system must include:[5]

- the name of the electronic system;
- the owner of the electronic system;
- the sector/domain of the electronic system;
- contact details of the electronic system's contact person;
- the uniform resource locator (URL) of the website;
- the domain name system and/or server internet protocol (IP) address;
- a brief description of the electronic system's functions and business processes;
- the electronic system's risk-based classification;
- a description of any classified data handled by the electronic system;
- a description of the personal data processed by the electronic system; and
- details on the location where the electronic system and its electronic data are managed, processed, and/or stored.

Upon approval of the registration by the MOCD, a registration mark will be issued to the Public ESO.[6]

Failure to complete the registration may result in the MOCD, in coordination with the relevant ministerial authorities, blocking the electronic system.[7]

III. Governance of User Generated Content by Public ESOs

MOCD Reg. 5/2025 requires any Public ESO that provide, host, display or exchange content uploaded by users ("UGC Public ESO") to implement mechanisms for user reporting and to establish an electronic information governance policy, which must include:[8]

- the rights and obligations of users;
- the rights and obligations of the Public ESO in operating the electronic system;

[5]Article 12 of MOCD Reg. 5/2025
[6]Article 13 of MOCD Reg. 5/2025
[7]Article 16 of MOCD Reg. 5/2025
[8]Article 19 of MOCD Reg. 5/2025

- responsibilities concerning uploaded electronic information; and
- the availability of service and mechanisms handling for user complaints.

Public ESOs must make available a reporting system that allows the public to report unlawful electronic information.

A UGC Public ESO will not be held responsible for unlawful electronic content uploaded by users, provided it can demonstrate that it has (i) ensured its electronic system does not contain or facilitate the dissemination of unlawful electronic information, (ii) responded adequately to reports of such unlawful electronic information, (iii) provided relevant information about the upload of such unlawful content, and (iv) taken down such unlawful content.[9]

IV. MOCD Authority on Access Blocking and Content Takedown

MOCD Reg. 5/2025 grants the MOCD the authority to instruct Public ESOs to take down unlawful electronic information.[10] Public ESOs are required to comply with such takedown orders within 24 hours or within 4 hours for urgent unlawful content, such as material related to terrorism or child pornography.[11] If a Public ESO fails to comply with the takedown order, the MOCD has the authority to direct internet service providers to block access to the electronic system of that Public ESO.

V. Risk-based Data Classification

MOCD Reg. 5/2025 introduces a risk-based data classification framework comprising three categories: open electronic data (for low risk data), limited electronic data (for medium risk data), and closed electronic data (for high risk data). Public ESOs are required to classify their data according to their risk categories, which in turn determine how the data must be managed, processed, and stored.[12] For example, while open and limited electronic data may be processed and stored in national data centers operated by appointed third party providers, closed electronic data must be stored and processed in data center facilities owned by the government.[13] Limited and closed electronic data must be stored while at rest in an encrypted form.[14] Closed electronic data cannot be transmitted via networks.[15] While access to limited electronic data requires approval from the data guardian, access to closed electronic data requires approval from the head of the relevant government agency that owns the data.[16]

[9]Article 20 of MOCD Reg. 5/2025
[10]Article 21 of MOCD Reg. 5/2025
[11]Article 26 of MOCD Reg. 5/2025
[12]Article 62 of MOCD Reg. 5/2025
[13]Article 87 of MOCD Reg. 5/2025
[14]Article 90 of MOCD Reg. 5/2025
[15]Article 91(3)of MOCD Reg. 5/2025
[16]Article 93 of MOCD Reg. 5/2025

VI. Transitional Deadline

The MOCD Reg. 5/2025 provides that Public ESOs are granted a one-year transitional period, ending on 25 March 2026, to bring their operations into full compliance with its provisions. In addition, Public ESOs that have already completed registration under the previous framework are still required to re-register in accordance with MOCD Reg. 5/2025 within the same one-year period.

Key Takeaways

MOCD Reg. 5/2025 generally provides much-needed clarity on the regulatory framework governing Public ESOs and imposes obligations that are aligned with those applicable to Private ESOs, particularly with respect to responsibility for unlawful electronic information. The one-year transitional period provides sufficient time for Public ESOs (including those newly appointed) to make the necessary adjustments and prepare for compliance and registration with the MOCD. During this period, Public ESOs should take proactive steps to ensure compliance, including conducting internal audits and legal reviews to assess current practices, identify any compliance gaps, and implement measures to meet the new regulatory standards.