



MAGNUS
LAW OFFICES

BEYOND LEGAL SOLUTIONS

KEY TAKEAWAYS:

**GOVERNMENT REGULATION NO. 17 OF 2025 ON GOVERNANCE
OF ELECTRONIC SYSTEMS FOR CHILD PROTECTION**

MAGNUS LAW OFFICES

CONTACT DETAILS



+62 21 29398927



info@magnuslaw.co.id



www.magnuslaw.co.id



Magnus Law Offices

Overview & Introduction

Pursuant to the mandate established by Law No. 35 of 2014 concerning Child Protection and Law No. 11 of 2008 concerning Electronic Information and Transactions as amended, the Government has issued Government Regulation No. 17 of 2025 on the Governance of Electronic Systems for Child Protection (“**Government Regulation No. 17/2025**”). This regulation institutes comprehensive and binding obligations upon all Electronic System Operators (ESOs) whose services are directed toward, or foreseeably accessed by, minors residing within the jurisdiction of the Republic of Indonesia. Its primary objective is to delineate duties of care, safeguard the privacy rights of children in the digital domain, and establish a robust enforcement framework to ensure the creation and maintenance of a secure, ethical, and developmentally appropriate digital ecosystem, thereby actualizing the state’s constitutional responsibility toward its younger generation.

Key Takeaways from Government Regulation No. 17/2025

1. **Mandatory Protection Duties for Children**

Government Regulation No. 17/2025 establishes a clear and non-delegable duty of protection for all Electronic System Operators (“**ESOs**”), both public and private, toward users under the age of eighteen. This duty requires ESOs to design their services with a heightened level of care, ensuring that minors are not only granted access to safe digital environments but also shielded from any exposure that could endanger their development. By codifying this protection mandate in Article 2, 3, and 4 Government Regulation No. 17/2025, the regulation places the responsibility directly on operators, recognizing that children are uniquely vulnerable in the digital domain.

To operationalize this mandate, ESOs must implement technical measures such as minimum age thresholds and verifiable age-assurance mechanisms. These requirements are intended to prevent unlawful or inappropriate access to systems by minors, particularly in cases where digital services are designed for general audiences but are foreseeably accessed by children. By establishing these

safeguards, the regulation moves beyond aspirational principles and requires enforceable compliance measures that protect the best interests of minors.

In addition, ESOs are expected to ensure that all available content is appropriate to the user's age group. This obligation goes beyond merely filtering harmful material; it requires the proactive curation and structuring of services so that children are not inadvertently exposed to inappropriate content. Collectively, these duties reflect a regulatory philosophy that treats child protection as a central obligation rather than a discretionary choice for digital platforms.

2. Content Moderation and Reporting Mechanisms

The Article 5 and 6 of Government Regulation No. 17/2025 introduce explicit obligations on ESOs to actively moderate and regulate the content available on their platforms. These provisions address the need to safeguard children from harmful or illicit material, particularly content related to sexual exploitation, violence, and self-harm. The regulation requires platforms to adopt filtering technologies, moderation protocols, and preventive safeguards that are both technical and organizational in nature, thereby elevating content moderation from a best practice to a statutory duty.

Equally important is the establishment of reporting channels that are easy to find and simple to use. ESOs must ensure that parents, guardians, and even children themselves are empowered to flag unsafe or illegal content through accessible mechanisms. Reports must be acted upon within a defined period, ensuring timely intervention that prevents prolonged exposure to harmful materials. The law thereby seeks to transform reporting systems from symbolic features into enforceable compliance tools with clear accountability.

By combining proactive moderation with responsive reporting, Government Regulation No. 17/2025 builds a holistic framework where safety is embedded into the system design, and accountability is reinforced by law. This marks a significant departure from a purely voluntary approach, ensuring that service providers are legally compelled to place child protection at the forefront of their operations.

3. Data Protection and Privacy Obligations

Article 7 and 8 Government Regulation No. 17/2025 establish rigorous standards for the protection of minors' personal data, embedding the principle of "Privacy by Design and Default" into the regulatory architecture. ESOs must minimize data collection, process only what is strictly necessary, and design systems that automatically adopt the highest privacy settings for accounts used by children. This obligation reflects a recognition that children, by virtue of their age, cannot be expected to fully understand the implications of data processing and therefore require heightened safeguards.

The regulation mandates explicit and verifiable parental or guardian consent for any processing beyond the essential operation of the service. This means that data processing for targeted advertising, behavioral tracking, or commercial exploitation is generally prohibited unless specific consent is obtained through transparent and secure procedures. Importantly, the regulation also prohibits the use of manipulative designs, often referred to as “dark patterns,” that may mislead children or guardians into granting consent.

In addition, children and their legal guardians are granted enforceable rights to access, rectify, and request deletion of personal data, reinforcing the “Right to Be Forgotten” principle. This ensures that the processing of minors’ data is not only compliant with parental consent but also subject to ongoing oversight and correction, thereby prioritizing the child’s right to privacy and protection above commercial interests.

4. Oversight, Enforcement, and Sanctions

The Supervision of ESOs under Government Regulation No. 17/2025 is entrusted primarily to the Ministry of Communication and Digital Affaris, which is empowered to conduct both scheduled audits and ad hoc investigations. ESOs must submit self-assessments regarding the risks associated with their services and cooperate fully with audits. This oversight model combines self-regulation with state authority, creating a dual system that emphasizes both corporate accountability and government enforcement.

Where breaches occur, the regulation introduces a structured and escalating sanctions framework pursuant to Article 38 Government Regulation No. 17/2025. Violations may trigger written warnings, financial penalties, temporary suspension of specific services, or in severe cases, the permanent blocking of access within Indonesian jurisdiction. The proportionality principle is embedded into this regime, ensuring that the severity of the sanction reflects the seriousness of the breach and its impact on child protection.

In addition, sanctions are not limited to punitive measures but also serve corrective and preventive functions. Operators that receive warnings are typically required to implement remedial action plans within a specified timeframe, demonstrating that their internal systems and procedures have been adjusted to align with the regulatory requirements. Failure to comply with such corrective measures can escalate the penalties imposed, reinforcing the expectation that compliance must be continuous and demonstrable.

The regulation further clarifies that the imposition of administrative sanctions does not preclude criminal liability where violations intersect with broader statutory prohibitions, such as offenses under the Child Protection Law or the Electronic Information and Transactions Law (ITE Law). This dual exposure underscores the seriousness of non-compliance, signaling to ESOs that negligence in safeguarding children online may carry both regulatory and criminal repercussions.

By introducing this comprehensive sanctioning regime, Government Regulation No. 17/2025 firmly establishes that child protection in the digital sphere is a matter of legal obligation, not corporate discretion. ESOs are expected to embed compliance into their governance structures, ensuring that their platforms contribute to a safe, ethical, and developmentally sound digital ecosystem for children.

Jakarta, 15 October 2025

MAGNUS LAW OFFICES

For further information please contact Pascal A. Hutasoit (pascal@magnuslaw.co.id) or Gilang Mursito Aji (aji@magnuslaw.co.id).

Disclaimer:

This publication is the property of Magnus Law Offices and may not be used by any other party for any purpose whatsoever without first obtaining prior written consent from Magnus Law Offices.

The information contained herein is for general purposes only and is not offered as legal or any other advice on any particular matter, whether it be legal, procedural or otherwise. It is not intended to be a substitute for reference to the detailed provisions of applicable laws, rules, regulations or forms. Legal advice should always be sought before taking any action or refraining from taking any action based on any information provided. Accordingly, Magnus Law Offices accepts no liability of any kind in respect of any statement, opinion, view, error, or omission that may be contained in this legal update.