

Indonesia: Regulation on Online Child Safety Issued! New Obligations to Protect the Younger Generation

In brief

The Indonesian Government has just issued a much-anticipated regulations that is closely connected with two important elements in society: children and technology. This new regulation introduces new obligations and prohibitions for electronic system operators in relation to the access and use of electronic systems by children.

In this issue

Key Takeaway

Actions to Consider

Key takeaways

Government Regulation No. 17 of 2025 on the Governance of Electronic System Implementation in Child Protection (*Peraturan Pemerintah No. 17 Tahun 2025 tentang Tata Kelola Penyelenggaraan Sistem Elektronik Dalam Pelindungan Anak* ("GR 17")) is effective as of 27 March 2025. There is a two-year transitional period for Electronic System Operators ("ESO") to conform with GR 17, and there are indications that one or more ministerial regulations will be issued to add more details. As with the 2022 Personal Data Protection Law, which has a similar transitional period, the expectation is that full implementation and enforcement will be conducted after the transitional period.

General requirement

GR 17 regulates that ESOs are obligated to provide protection for children (i.e., those who are under 18 years of age) who use or access electronic systems, by providing:

- a. Information on the minimum age limit for children who can use their products and services (i.e., grouping of (i) 3-5 years, (ii) 6-9 years, (iii) 10-12 years, (iv) 13-15 years, and (v) 16-before 18 years)
- b. A verification mechanism for child users
- c. A reporting mechanism for misuse of products, services, and features that violate or have the potential to violate children's rights

Who are the ESOs

The term ESO in GR 17 covers both public ESOs and private ESOs. For private ESOs, it covers those that develop and/or operate online products, services and features that are either (i) specifically designed to be used or accessed by children, or (ii) may be used or accessed by children.

Risk level and notification requirement

Online products, services and features will be accessed based on their risk level for children, i.e., either low risk or high risk.

The risk level assessment is done based on the following aspects:

- a. Contracting with unknown people
- b. Exposure to pornographic content, violent content, content that can endanger life, and other content that is not appropriate for children

- c. Exploitation of children as consumers
- d. Threat to children's psychological wellness
- e. Possible physiological disorders in children

If an online product, service or feature has a high risk level in one of the aspects above, it will be considered as high risk.

If an online product, service or feature has a low risk level in all of the aspects above, it will be considered as low risk.

The risk level assessment is a self-assessment done by the relevant ESO. That said, the relevant ESO must report the result of the self-assessment to the Ministry of Communication and Digital ("**Komdigi**"). The Ministry will verify the submitted result, and then stipulate the risk profile of the online product, service or feature.

GR 17 mandates the preparation and issuance of a ministerial regulation to provide further provisions on the self-assessment mentioned above. As such, this self-assessment and notification requirement may not be implemented and enforced immediately.

Obligations of ESOs

ESOs are also required to meet the following obligations:

- a. Obtain consent from child users' parents or guardians
- b. Conduct a personal data protection impact assessment
- c. Configure product, service and feature settings that are specifically designed to be used or accessed by children or that may be used or accessed by children in a high level of privacy by default
- d. Provide information that is complete, correct, accurate and not misleading that allows users to understand the products, services and features
- e. Provide education and empowerment on the digital ecosystem
- f. Provide notifications in the form of signs or signals in monitoring children's activities or tracking children's locations from product, service and features
- g. Provide a choice of functions that are suitable for the child's capacity and age
- h. Firmly determine the party responsible for processing children's personal data for toys or devices that can be connected to the internet
- i. Ensure that parties appointed by or collaborating with the ESO meet the requirements of child protection
- j. Appoint an official or officer who carries out the function of personal data protection

Prohibitions

ESOs are also prohibited from carrying out activities such as:

- a. Using or implementing means, techniques or practices that are hidden or non-transparent in the development or use of the products, services and features
- b. Collecting accurate geolocation information of children
- c. Carrying out profiling of children.

Actions to Consider

While there is a two-year transitional period before GR 17 will be fully implemented and enforced, ESOs may need to start familiarizing themselves with the provisions in the regulation and identifying a plan to comply with the regulation.

Do bear in mind the need for ESOs to conduct a risk level self-assessment of their platforms (which then needs to be reported to Komdigi), as well as the age categories that are appropriate to use and access the products, services and features.

Komdigi will be the government agency in charge of the implementation of GR17 (with the possibility of cooperation with other government agencies and law enforcement agencies), which includes the authority to perform the following actions:

- a. Monitoring and/or tracing of child protection obligations in electronic systems operated by ESOs
- b. Receiving reports or complaints on alleged violations by ESOs regarding child protection obligations
- c. Carrying out examinations to follow up on the monitoring and/or tracing
- d. Taking actions to establish control (such as imposing administrative sanctions, giving orders to ESOs, or making violations by ESOs public) based on the results of the examinations

From the public perspective, GR 17 provides the opportunity for the public/community in general to take active roles in child protection in electronic systems, by providing education to children, parents or guardians regarding the benefits and negative impacts of the use of products, services and features. GR 17 also provides opportunities for the public/community to report or make complaints if they suspect ESOs are not meeting their obligations to protect children in electronic systems.

Contact Us



Daniel Pardede

Senior Partner

daniel.pardede@hhplawfirm.com



Daru Lukiantono

Senior Partner

daru.lukiantono@hhplawfirm.com



Harry Kuswara

Associate Partner

harry.kuswara@hhplawfirm.com



Adhika Wiyoso

Associate Partner

adhika.wiyoso@hhplawfirm.com



Bratara Damanik

Associate

bratara.damanik@hhplawfirm.com

© 2025 HHP Law Firm. All rights reserved. In accordance with a 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 the office of any such law firm. This may qualify as 'Attorney Advertising' requiring notice in some jurisdictions. Prior results do not guarantee a similar outcome

