TECHNOLOGY, MEDIA & TELECOMMUNICATIONS

Decoding Indonesia's Latest Online Child Safety Regulations: What Digital Platforms Need to Know

© ASSEGAF HAMZAH & PARTNERS

On 27 March 2025, the Indonesian government enacted a comprehensive online child protection regulation ("**Regulation**") that digital platforms should be aware of.[1] This Regulation, stemming from Articles 16A and 16B of the EIT Law[2] (as previously discussed in our earlier client update, accessible here), introduces a range of important obligations designed to create a safer online environment for children.

This client alert will explore the essential obligations of this new Regulation. We will discuss the scope of its application, the critical process of risk assessment, and the strong emphasis on obtaining parental consent and implementing high privacy by default. We will also examine the specific requirements around minimum age disclosure, age verification processes, and the implementation of age-appropriate access and account management. Ensuring service information is easily understandable and accessible is another key aspect, as well as the responsibility for third-party compliance and the clear prohibition of harmful online practices. Lastly, we will outline the transition timeline and the potential sanctions for failing to comply.

Understanding Who is Affected by the New Rules

The Regulation applies broadly to all electronic system operators ("**ESOs**") – public and private, domestic and foreign – as long as their products, services, or features are specifically intended to be used or accessed by children (defined as anyone under 18 years old) in Indonesia. This means that it includes social media sites, online games, e-commerce platforms, educational apps, smart toys and devices, as well as streaming services for entertainment and other content.

Notably, even if a platform is not specifically aimed at children, it could still fall under these rules if it is likely that children will use it. The government will look at several indicators to determine this, such as whether the platform's own rules (whether published or outlined in its internal documents) suggest it is for kids, if there is a strong evidence of large portion of its regular users are children, if its ads target children, if its design and presentation appeal to children, or if it is very similar to other services known to be popular with kids.

While the specifics of these indicators are not yet crystal clear – for example, what exactly counts as "strong evidence" of a large child user base – the Ministry of Communications and Digital Affairs will provide more detailed guidance on how these indicators will be assessed in a subsequent ministerial decree.

Pending further clarification, even if a website or app's terms of use do not specify that its users are children, it may still be subject to the Regulation as the government will not just rely on such a factor.

The Obligation to Assess Risks to Children

A key part of the Regulation is the requirement for all ESOs to conduct a "risk assessment" on their products, services, and features, based on specific risk indicators that might pose harm to children.

In this risk assessment, ESOs need to specifically evaluate the likelihood of, among other things:

1. Children being contacted by strangers.
2. Children encountering harmful content such as pornography or violence.
3. The presence of design elements that could lead to addictive behaviour in children.
4. Potential negative impacts on children's physical or mental health.

[1] Government Regulation No. 17 of 2025 on Governance of Electronic System Implementation in Child Protection (*Tata Kelola Penyelenggaraan Sistem Elektronik Dalam Pelindungan Anak*).
[2] Law No. 11 of 2008 on Electronic Information and Transaction Law, as lastly amended by Law No. 1 of 2024.

If the assessment reveals a high likelihood of any of these risks, the service will be classified as "high-risk." If there are no high risk identified in all of the prescribed criteria, then the service will be classified as "low-risk."

ESOs are then required to submit the results of their self-assessment to the Ministry of Communications and Digital Affairs for their review and final determination of the service's risk profile. In our view, this risk-based approach allows the Ministry to focus its regulatory efforts on monitoring, and develop stronger protective measures to be applied where they are most needed. However, further guidance on how this assessment must be carried out, including the submission of the assessment to the Ministry, remains unclear for now given all these will only be clarified under a subsequent ministerial regulation.

The Importance of Parental Consent: Getting Consent for Children's Online Access

The Regulation places a strong emphasis on parental consent for children using online services. As part of this, ESOs must implement a clear "opt-in" consent mechanism, meaning they absolutely cannot allow a child to register, access, or interact with their services unless a parent or legal guardian has actively and explicitly given their consent. The Regulation specifically prohibits implied consent – for example, assuming consent has been provided when a parent does not explicitly object. Instead, ESOs must take proactive steps to get a clear "yes" from a parent or guardian.

However, the Regulation acknowledges that older teenagers have a greater level of maturity. For users aged 17, they can give their own consent directly. Notwithstanding, the ESO must immediately notify the parent or guardian and give them a six-hour window to object. If no objection is received within that time, the 17-year-old can proceed.

For all children under 17, the rules are stricter. The Regulation requires ESOs to actively request parental or guardian consent within 24 hours and prohibits them from providing any access to the service until such consent is obtained. During this 24-hour window, the child cannot use any part of the service.

It is important to note that the Regulation does not explicitly say what happens if a parent or guardian does not respond to the consent request within 24 hours. We believe the safest and most consistent interpretation of the Regulation's emphasis on "opt-in" consent is that a lack of response should be treated as a denial of consent. In such situations, the ESO should not grant access and may need to try the consent process again. We anticipate further clarification on this point.

Protecting Children's Personal Data by Default

In terms of data protection, the Regulation adopts a privacy-by-default approach, requiring ESOs to implement "high privacy settings" as the default. This approach means that from the initial design and development of a service, the strongest privacy safeguards must be automatically activated. This includes measures such as limiting data sharing, restricting tracking of online activity, turning off location services, and ensuring that children are automatically opted out of things like profiling.

These default settings are particularly important because children may not have the awareness or skills to manage their privacy settings effectively. Therefore, the Regulation puts the responsibility on the ESOs to proactively minimise privacy risks through these secure default configurations.

This approach reflects the Regulation's aim to prioritise children’s best interests and their right to privacy from the outset, rather than relying on the child's ability to navigate or understand complex privacy options.

Moreover, if ESOs processes children's personal data, they are required to conduct a Data Protection Impact Assessments (DPIA) in accordance with Indonesia's Personal Data Protection Law (Law No. 27 of 2022). This is a process to identify and assess potential risks to personal data. In addition to that, such ESOs are required to appoint a Data Protection Officer (DPO) to oversee data protection activities provided the threshold requirement for such DPO appointment obligation under the Personal Data Protection Law is met.

You can find a more in-depth explanation of DPIA and DPO requirements in our previous client alert, which is available here.

Clearly Stating Age Limits and Verifying Users' Ages

The Regulation requires ESOs to implement measures to protect children right from the start, which includes clearly stating and enforcing age limits for using their services. ESOs must establish and communicate the minimum age required for children to access their platforms. This information must be presented directly within the service itself, for example, when someone signs up. It should also be easily understood by both children and their parents or guardians. For example, a website might display a pop-up message like "This service is designed for users age 13 and older".

To help ensure these age limits are followed, ESOs also need to implement a mechanism to check a user's age when they sign up. These age verification tools should be built into the registration process and designed with children's privacy in mind. Any information to verify age should be limited to what is absolutely necessary, used only to confirm if the user meets the age requirement, and then securely deleted once that is done (unless retaining such information is legally required).

Managing Children's Accounts Based on Age

The Regulation sets the minimum age of three years old for online services and then groups children into five different age categories:

1. 3 to 5 years old;
2. 6 to 9 years old;
3. 10 to 12 years old;
4. 13 to 15 years old; and
5. 16 to 18 years old.

These age groups are designed to ensure that the online services provided are appropriate for the age and developmental stage of the children using or likely to use them.

In line with these groupings, the Regulation also establishes specific rules for children creating and managing online accounts:

Age Group	Permissible Services
Under 13 years old[3]	• Services **specifically** designed for children; • Low-risk profile services, with parental consent.
13 to 16 years old	• **All** services; • Low-risk profile services, with parental consent.
16 to 18 years old	• **All** services (including high-risk profile), with parental consent.

These rules are part of a "safety by design" approach, meaning that ESOs need to build in features, such as parental controls, that allow parents to monitor and manage their child's use of the service.

Making Information Easy to Understand

The Regulation emphasises that information about an online service must be presented in a way that children can easily understand, using language and formats that are suitable for their different age groups. For example, a platform might use short, simple videos with pictures to explain how to use the service safely. This ensures that kids of all ages can get a clear guidance.

The Regulation also recognises that children have the right to know if they are being monitored online. So, if a service allows parents, guardians, or other users to monitor a child's activity or see their location, the system must clearly display clear and visible notification—which could be a symbol, an alert, or even a pop-up notification—to inform the child that they are being monitored. This requirement reinforces transparency and explicitly prohibits silent or undisclosed forms of monitoring.

In line with the broader aim of empowering child users, the Regulation also requires ESOs to offer easy-to-use tools that allow both children and their parents or guardians to exercise their rights or make complaints about how the service is being used. One example is a "mute words" feature, where users can block certain words, phrases, hashtags, or usernames from appearing in their feeds, search results, or notifications. Besides making these tools easy to access, ESOs also need to have clear steps for how these tools work, including responding quickly to issues and taking appropriate action to fix problems.

Extension of Child Protection Obligations to Third Parties

The Regulation does not just apply to the main ESO providing the online service. It also extends to any other company or individual that the main ESO hires or partners with to help develop, operate, or support the service. This means that if an ESO appoints or partners with another entity (whether through outsourcing, subcontracting, or other commercial arrangements), that third party also needs to follow the child protection rules set in the Regulation.

Importantly, the main ESO is still fully responsible for ensuring that these third parties meet all the requirements under the Regulation. This includes verifying user's age, getting proper consent, being transparent about monitoring, and handling children's personal data safely.

[3] This includes e-learning platforms developed by schools and used solely to distribute assignments or learning materials from teachers to students, without any communication features between students.

Prohibiting Practices That Could Harm Children

Beyond requiring proactive safety measures, the Regulation also establishes clear prohibitions of certain practices that are considered harmful to children online. In this regard, ESOs are not allowed to:

1. Use tricky or misleading design features—often called "dark patterns"—that pressure or deceive children into revealing more personal information than needed, changing their privacy settings, or engaging in activities that could harm their physical or mental well-being.

2. Collect a child's location data automatically, unless it is absolutely necessary and for a limited time. If this type of data is processed, it must be based on explicit consent. Additionally, strong measures must be in place, including technical safeguards like encryption and access control, as well as organisational measures such as regular security audits and staff training to ensure the data is protected appropriately.

3. Create profiles of children, unless it can be clearly shown that doing so is actually in the child's best interests. This means that at every stage of the development and operation of the service, the ESO must prioritise the child's rights, including their safety, health, development, well-being, privacy, and the protection of their personal data.

The Transition Period and Sanctions for Non-Compliance

The Regulation gives ESOs a two-year period, until 27 March 2027, to make sure their services fully comply with all the child protection requirements. During this time, the Ministry of Communications and Digital Affairs will not impose administrative penalties for not meeting the new rules.

However, it is important to note that even during this transition period, affected parties like parents, guardians, or child protection groups can still take private legal action, such as filing civil lawsuits, if they believe a service is harming children or not complying with the Regulation.

Additionally, while the Regulation itself does not stipulate criminal penalties, other laws in Indonesia, like the Child Protection Law (Law No. 23 of 2002, as amended), do have criminal consequences for actions that harm children. For instance, Article 76I of the Child Protection Law prohibits the economic and/or sexual exploitation of a child. Violating this law can lead to imprisonment for up to 10 years and/or a fine of up to IDR200 million (approximately US$11,872, based on a rough exchange rate).

What This Means for Digital Platforms

The Regulation represents a major shift in how Indonesia protects children online, moving from general guidelines to clear and enforceable rules. Although there is a two-year transition period, ESOs should not adopt a passive "wait and see" approach. Several important requirements – like conducting a Data Protection Impact Assessments (DPIA), setting up strong default privacy settings, implementing age verification processes, and providing easy-to-use reporting tools for children – are existing measures that ESOs should carry-out under other laws, such as the Personal Data Protection Law.

Getting started early will help reduce the risk of penalties once the transition period ends. ESOs that proactively adapt to these new requirements will not only be better protected legally but will also build stronger trust with their users, parents, and the government.

Contacts

TECHNOLOGY, MEDIA & TELECOMMUNICATIONS

Zacky Zainal Husein

PARTNER

D +62 21 2555 9956
zacky.husein@ahp.id

Muhammad Iqsan Sirie

PARTNER

D +62 21 2555 7805
iqsan.sirie@ahp.id

Contribution Note

This Legal Update is contributed by the Contact Partners listed above, with the assistance of **Daniar Supriyadi** (Associate, Assegaf Hamzah & Partners).

Please feel free to also contact Knowledge Management at RTApublications@rajahtann.com.

Regional Contacts

Cambodia
Rajah & Tann Sok & Heng Law Office

T +855 23 963 112 | +855 23 963 113
kh.rajahtannasia.com

China
Rajah & Tann Singapore LLP
Representative Offices

Shanghai Representative Office
T +86 21 6120 8818
F +86 21 6120 8820

Shenzhen Representative Office
T +86 755 8898 0230
cn.rajahtannasia.com

Indonesia
Assegaf Hamzah & Partners

Jakarta Office
T +62 21 2555 7800
F +62 21 2555 7899

Surabaya Office
T +62 31 5116 4550
F +62 31 5116 4560
www.ahp.co.id

Lao PDR
Rajah & Tann (Laos) Co., Ltd.

T +856 21 454 239
F +856 21 285 261
la.rajahtannasia.com

Malaysia
Christopher & Lee Ong

T +603 2273 1919
F +603 2273 8310
www.christopherleeong.com

Myanmar
Rajah & Tann Myanmar Company Limited

T +951 9253750
mm.rajahtannasia.com

Philippines
Gatmaytan Yap Patacsil Gutierrez & Protacio
(C&G Law)

T +632 8248 5250
www.cagatlaw.com

Singapore
Rajah & Tann Singapore LLP

T +65 6535 3600
sg.rajahtannasia.com

Thailand
Rajah & Tann (Thailand) Limited

T +66 2656 1991
F +66 2656 0833
th.rajahtannasia.com

Vietnam
Rajah & Tann LCT Lawyers

Ho Chi Minh City Office
T +84 28 3821 2382
F +84 28 3520 8206

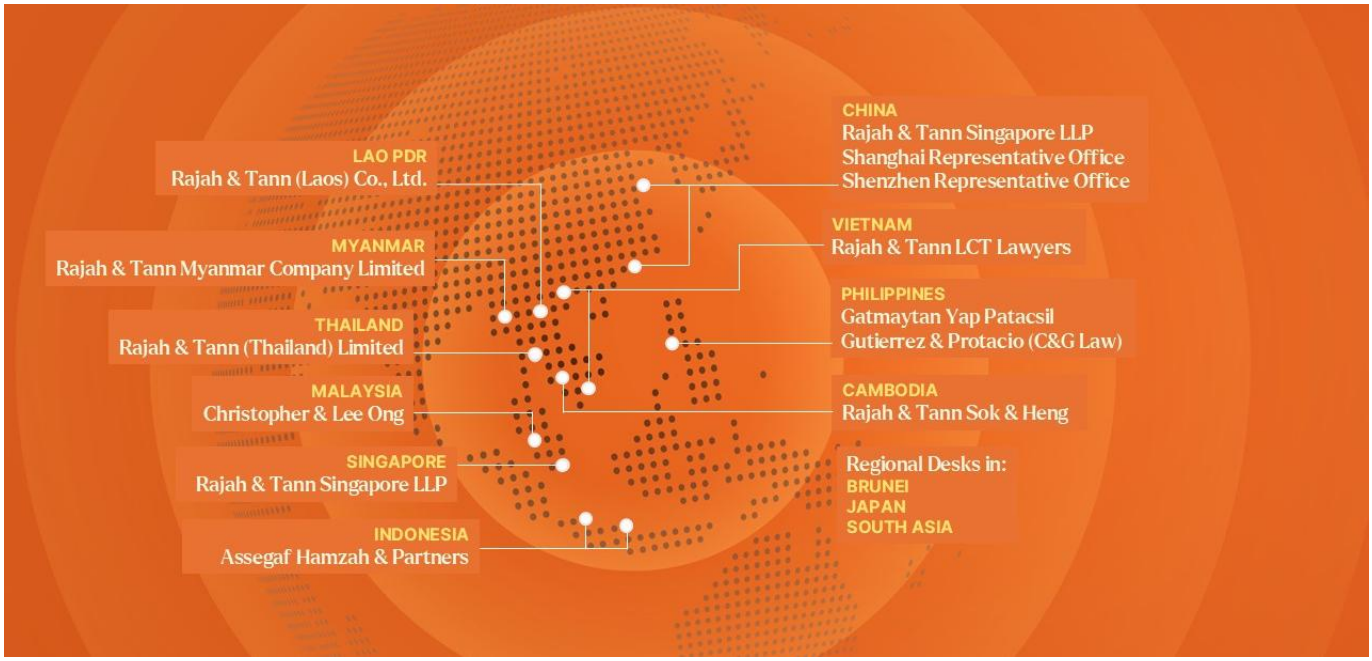
Hanoi Office
T +84 24 3267 6127 | +84 24 3267 6128
vn.rajahtannasia.com

Rajah & Tann Asia is a network of legal practices based in Asia.

Member firms are independently constituted and regulated in accordance with relevant local legal requirements. Services provided by a member firm are governed by the terms of engagement between the member firm and the client.

This update is solely intended to provide general information and does not provide any advice or create any relationship, whether legally binding or otherwise. Rajah & Tann Asia and its member firms do not accept, and fully disclaim, responsibility for any loss or damage which may result from accessing or relying on this update.

Our Regional Presence



Based in Indonesia, and consistently gaining recognition from independent observers, Assegaf Hamzah & Partners has established itself as a major force locally and regionally, and is ranked as a top-tier firm in many practice areas. Founded in 2001, it has a reputation for providing advice of the highest quality to a wide variety of blue-chip corporate clients, high net worth individuals, and government institutions.

Assegaf Hamzah & Partners is part of Rajah & Tann Asia, a network of local law firms in Cambodia, China, Indonesia, Lao PDR, Malaysia, Myanmar, the Philippines, Singapore, Thailand and Vietnam. Our Asian network also includes regional desks focused on Japan and South Asia.

The contents of this Update are owned by Assegaf Hamzah & Partners and subject to copyright protection under the laws of Indonesia and, through international treaties, other countries. No part of this Update may be reproduced, licensed, sold, published, transmitted, modified, adapted, publicly displayed, broadcast (including storage in any medium by electronic means whether or not transiently for any purpose save as permitted herein) without the prior written permission of Assegaf Hamzah & Partners.

Please note also that whilst the information in this Update is correct to the best of our knowledge and belief at the time of writing, it is only intended to provide a general guide to the subject matter and should not be treated as a substitute for specific professional advice for any particular course of action as such information may not suit your specific business and operational requirements. It is to your advantage to seek legal advice for your specific situation. In this regard, you may contact the lawyer you normally deal with in Assegaf Hamzah & Partners.