ALTA Advocates

ALTA Regulation Alert

PP TUNAS: Indonesia's New Regulation on Child Protection in Digital Space

WWW.ALTAADVOCATES.COM

Overview

On March 27, 2025, the Indonesian government officially enacted Government Regulation Number 17 of 2025 on the Governance of Electronic System Implementation in Child Protection or *Tata Kelola Penyelenggaraan Sistem Elektronik dalam Pelindungan Anak* (**PP TUNAS**).

This regulation builds upon the second amendment to the Electronic Information and Transactions Law (**UU ITE**), which introduced the obligation to protect children in digital environments. The Personal Data Protection Law (**UU PDP**) also intersects significantly with PP TUNAS, as it classifies children's data as specific personal data, subject to distinct processing rules.

Under PP TUNAS, a child is defined as any individual under the age of 18. The regulation imposes a broad range of obligations on Electronic System Operators or *Penyelenggara Sistem Elektronik*, including prioritizing the best interests of the child over commercial interests, and classifying access based on age groups, potential risk, and self-assessments.

Key Takeaways

Who Does PP TUNAS Apply to?

PP TUNAS applies to all Electronic System Operators or *Penyelenggara Sistem Elektronik* (**PSE**), both public (i.e., government institutions or the appointed entities) and private[1], whose products, services, or features are either intended for use by children or are likely to be accessed by them.[2] It is important to note that the regulation does not limit its scope to systems explicitly designed for children but also includes those that may be potentially accessed by them.

As a result, a broad range of business actors operating in the digital space may fall under the scope of this regulation, including edutech platforms, game developers, and photo/video sharing platforms. Regardless of industry, any entity whose systems interact with children in the digital environment must assess its obligations under this regulation.

Recognizing the broad nature of the "potential use" criteria, PP TUNAS sets out certain indicators to help determine whether a system is deemed to fall within scope (e.g., any published terms, policies, or internal documents indicating child-directed intent, a user base that predominantly consists of children, child-friendly design elements, and other relevant factors).[3] More detailed assessment criteria are expected to be outlined in a forthcoming ministerial regulation.[4]

The Obligations and Prohibitions

PP TUNAS introduces a series of key obligations for PSE. For ease of reference, below is a simplified breakdown of the key obligations imposed under PP TUNAS. A more detailed explanation of each obligation is provided in the section that follows[5]:

a. **Parental Consent & Notification:** PSE must obtain consent from parents or guardians;
b. **Privacy Settings:** All products, services, and features must be configured with high default privacy settings to minimize data risks from the outset;
c. **Clear and Non-misleading Information:** PSE must ensure that the information provided is complete, accurate, and non-misleading information;
d. **Education and Awareness:** PSE are expected to promote awareness, education, and responsible digital use;
e. **Geo-location Notification:** PSE must provide notifications in the form of signs or signals when monitoring the activities or tracking the location of children;
f. **Age-based Features:** PSE must provide features that are suitable for different age groups, taking into account the development stage and capacity of the child;
g. **Third-Party Compliance:** PSE must clearly designate the party responsible for processing children's personal data in relation to internet-connected toys or devices, and ensure third-party compliance with this regulation; and
h. **PDP Related Requirements:** PSE are required to conduct a Personal Data Protection Impact Assessment (**DPIA**) and appoint for a Data Protection Officer (**DPO**), in accordance with the UU PDP.

In addition to these obligations, PP TUNAS also sets out a number of prohibitions[6]:

a. **Profiling Restriction:** PSE are prohibited from profiling children by default. Profiling is only allowed if it is clearly in the child's best interest, forms an essential part of the product, service, or feature, and/or is explicitly requested by the child.
b. **Geolocation Tracking Restriction:** Precise geolocation tracking is also prohibited unless necessary for the service and must be time-limited; and
c. **Prohibition on Manipulative Practices:** Any methods, techniques, or non-transparent practices that can encourage children to overshare data, disable privacy settings, or engage in harmful behaviour, are strictly forbidden.

Risk Classification & Self-assessment

PSE are required to conduct a self-assessment to classify their platforms as high-risk or low-risk to children, based on exposure to the following risk factors[7]:

a. possibility of children interacting with strangers;
b. exposure to pornographic, violent, life-threatening or other inappropriate content;
c. the exploitation of children as consumers;
d. threats to the security of children's personal data;
e. potential for addiction;
f. psychological harm; and
g. physiological harm

If one or more of the above risk factors are rated as high, the platform is classified as high-risk. If all factors are low, it is considered low-risk. The results of this assessment must be submitted to the ministry for verification and final determination.[8] Further technical guidelines will be outlined in a forthcoming ministerial regulation.[9]

Age Range Classifications & Feature

PSE are required to tailor their products, services, and features in line with children's developmental stages, and to clearly display the permitted age range classifications as specified in PP TUNAS[10]:

- 3 – 5 years
- 6 – 9 years
- 10 – 12 years
- 13 – 15 years
- 16 – under 18 years

PSE must also take appropriate steps to verify that users meet the platform's age requirements. This includes confirming that the child is above the minimum age (3 years) and falls within the correct age range. The level of assurance in age verification must be proportionate to the risk posed to the child's rights by the specific product, service, or feature.[11]

If a platform requires account registration, it may only be permitted with the following provisions[12]:

- For children under 13 years old: May create an account related to products, services or features that are specifically designed for children and classified as low-risk with obtaining parental consent.
- For children between 13 – 16 years old: May create an account related to products, services or features classified as low-risk with obtaining parental consent.
- For children between 16 – 18 years old: May create an account related to all products, services or features with obtaining parental consent.

Parental Consent and Notification

The requirement for parental or guardian consent is one of the most highly emphasized aspects of PP TUNAS. PSE must establish a mechanism for obtaining consent from the children's parent or guardian before granting the children access to their platforms.[13]

As a general rule, parental consent operates on an *opt-in* basis, meaning access may only be granted once the parent or guardian has provided their approval. The regulation further mandates that PSE allow a reasonable window of time for consent to be obtained, specifically within 24 hours.[14]

For children aged 17 years and above, the rule shifts to an *opt-out* mechanism. In this case, the child may provide initial consent, but the PSE is required to notify the parent or guardian. If no objection is received within 6 hours of notification, the consent is deemed valid and the service may proceed.[15]

Crucially, if parental consent is explicitly denied, or if consent is only provided by the child without the parental consent, the PSE must refrain from offering the service and delete any data collected. In such case, the consent given by the child is considered legally void, reinforcing the central role of parents or guardians in overseeing children's digital access.[16]

Privacy Settings

Under PP TUNAS, PSE are required to implement a Privacy by Default approach, where high privacy settings must be the default configuration for any product, service, or feature accessible to children.[17] These settings cannot be altered or downgraded unless the change is supported by DPIA and involves clear, active user input.[18] This ensures that children's rights and data is protected from the outset and any exceptions are carefully justified and transparent.

This requirement underscores the government's strong stance on child-focused data protection. Given children's heightened vulnerability online, the regulation places the responsibility on PSE, not to the users, to ensure that high privacy settings are the default standard. Any deviation from this standard must be clearly justified through a DPIA, particularly when privacy settings are configurable. This approach aligns with global best practices and ensures that safety and privacy are built into platform design from the start.

PDP Related Requirements

Based on the elucidation of PP TUNAS, the scope of child personal data may include[19]:

a. **Identifiers**, such as full name, alias, postal address, unique personal identifiers, IP address, email address, account name, social security number, driver's license number, passport number, or similar identifiers;
b. **Commercial information**, including records of personal property, products or services purchased, obtained, or considered, as well as other purchasing or consumption history and trends;
c. **Biometric** data;
d. **Internet or electronic network activity**, including browsing history, search history, and information related to the child's interaction with applications, websites, or online advertisements;
e. **Geolocation** data;
f. **Audio, visual, or similar** information;
g. **Professional or employment-related** information;
h. **Educational** information;
i. **Information or insight generated from any of the above or a combination thereof to create a profile of the child**, including preferences, characteristics, psychological tendencies, behaviour, attitudes, intelligence, abilities, or aptitudes;
j. **Other personal data**, such as financial data, personal security codes, passwords or access credentials, content of private communications (e.g., emails, messages), health data, and information regarding racial or ethnic origin, or religious or philosophical beliefs.

PP TUNAS requires PSE to conduct a DPIA for any products, services, or features that are designed for or may be accessed by children.[20] This requirement aligns with the UU PDP, which classifies children's personal data as specific data, thereby triggering the obligation to carry out a DPIA prior to any data processing activity involving children. Additionally, if the platform allows configurable privacy settings beyond the default high-privacy standard, such configurations must be explicitly justified through the DPIA.[21]

In addition, PSE are obligated to appoint a DPO or designate a responsible official to oversee compliance with personal data protection obligations related to children. This appointment must be made in accordance with the UU PDP.[22]

Third-Party Compliance

PSE must ensure that all third-party partners, vendors, or affiliates comply with the same child protection and personal data standards as set out in the regulation. This can include, among others, data processors, and/or generally partners, content providers, and analytics services.[23]

PSE must clearly determine and document the roles and responsibilities of each party involved in the processing of children's personal data,[24] specifically identifying who acts as the data controller, data processor, or others. This role clarity is essential to ensure legal accountability, liability, transparency in processing activities, and effective implementation of data protection principles. An internal assessment and appropriate contractual arrangements should be put in place to reflect these roles and safeguard compliance throughout the data lifecycle.

Sanction & Transition Period

PP TUNAS imposes administrative sanctions for non-compliance, including written warnings, fines, temporary suspension, or even access blocking.[25] These sanctions are applied following a formal investigation if a PSE is found to have breached its child protection obligations.[26]

The regulation provides a 2-year transition period for PSE to adjust.[27] During this time, PSE are encouraged to proactively prepare the necessary technical systems, operational procedures, and internal policies to ensure compliance. Early planning is essential, especially for obligations that require careful design and coordination, such as determining the most practical and business-friendly methods for obtaining parental consent or implementing proportionate and effective age verification.

Conclusion

The PP TUNAS marks a significant step forward in child protection within digital environments. It establishes clearer obligations for PSE regarding age-based access, parental consent, privacy, and the protection of children's data. While the regulation offers greater clarity, several aspects remain subject to upcoming implementing regulations.

PSE should begin early assessments to ensure compliance during the transition period, including planning the necessary technical and organizational measures for implementation. By preparing proactively, PSE can navigate these requirements and help create a safer digital space for children.

You can access and download the PDF version of the PP TUNAS here.

Contact Us

Raditya Kosasih

Partner
kosasih.raditya@altaadvocates.com

Nabila Oktavia Annyndira

Associate
oktavia@altaadvocates.com

Disclaimer: *This publication is intended for general information purposes only and should not be construed as legal advice. It is not intended to create, and receipt of it does not constitute, an attorney-client relationship. Readers should not act upon this information without seeking professional counsel. While we strive to provide accurate and up-to-date information, the law is constantly changing, and individual circumstances may vary. Therefore, the information contained in this publication should not be relied upon as a substitute for obtaining legal advice from a qualified attorney regarding your specific situation. ALTA Advocates and its authors expressly disclaim all liability to any person with respect to the contents of this publication, and with respect to any act or failure to act made in reliance on any information contained herein. We shall not be held liable for any loss, damage, or inconvenience resulting from reliance on the information presented in this publication. By accessing and reading our news articles, readers acknowledge and accept the terms outlined in this disclaimer. We encourage readers to contact us with any concerns or feedback regarding our publication.*

[1] Article 3 paragraph (1) and paragraph (2)
[2] Article 3 paragraph (3) and Article 4 paragraph (1)
[3] Article 4 paragraph (2)
[4] Article 4 paragraph (3)
[5] Article 7 paragraph (1) letter a until j
[6] Article 7 paragraph (2) *jo.* Article 17, Article 18, and Article 19
[7] Article 5 paragraph (1) until paragraph (9)
[8] Article 5 paragraph (4), paragraph (7), and paragraph (8)
[9] Article 6
[10] Article 20 paragraph (1) and paragraph (2)
[11] Article 22 paragraph (1) and paragraph (2)
[12] Article 21 paragraph (1)
[13] Article 9 paragraph (1)
[14] Article 9 paragraph (3) and its elucidation
[15] Article 9 paragraph (2)
[16] Article 9 paragraph (5)
[17] Article 10 paragraph (1)
[18] Article 10 paragraph (2)
[19] Elucidation of Article 9 paragraph (5) letter b
[20] Article 7 paragraph (1) letter b and Article 7 paragraph (3)
[21] Article 10 paragraph (2)
[22] Article 7 paragraph (1) letter j and Article 7 paragraph (3)
[23] Article 16
[24] Article 15
[25] Article 38 paragraph (2)
[26] Article 26 paragraph (1) to paragraph (4)
[27] Article 49