International Journal of Sociology of Religion (IJSR)
Volume 04, Number 02, December 2026, Pages: 178-187
Website: https://www.journals.asteec.com/index.php/ijsr/index
E-ISSN: 3064-0482
DOI: https://doi.org/10.70687/3w89ka30

From Age Limits to Accountable Design: A Risk-Based Framework to Protect Children on Social Media in Indonesia

Hilman Jayadi
Hilmanjayadi26@gmail.com
STIS Harsy Lombok Tengah

ARTICEL INFO

Articel history:
Received 29, 06, 2026
Revised 04, 08, 2026
Accepted 05, 09, 2026
Available online December 12, 2026

Keywords*: child online safety; age assurance; social media governance; personal data protection; platform accountability*

This is an open-access article under the CC BY-SA license.

Copyright © 2026

Abstract

Children's participation in social media creates opportunities for communication, learning, and self-expression, but it also exposes them to risks associated with unwanted contact, harmful content, exploitation, and extensive personal-data processing. This article examines whether Indonesia's child-protection framework has translated general legal duties into workable governance standards for social media. It employs doctrinal legal research using statutory, conceptual, and comparative approaches. Primary legal materials include Law No. 35 of 2014 on amendments to the Child Protection Law, Law No. 1 of 2024 amending the Electronic Information and Transactions Law, Law No. 27 of 2022 on Personal Data Protection, Government Regulation No. 17 of 2025, and Minister of Communication and Digital Regulation No. 9 of 2026. Comparative materials include Australia's Social Media Minimum Age framework and the United States' Children's Online Privacy Protection Rule. The analysis finds that Indonesia's framework now contains a more developed regulatory basis for age assurance, risk assessment, platform duties, supervision, and sanctions. The central challenge is therefore not a complete absence of regulation, but the practical implementation of proportionate age assurance, feature-level risk controls, transparent compliance evidence, and accessible remedies. The article proposes an integrated model combining risk-based age assurance, privacy-by-design, auditable platform accountability, and education-based prevention. The model treats age limits as one component of a broader governance system rather than as a stand-alone solution.

INTRODUCTION

Social media has become an important environment in which children communicate, learn, create content, and form social relationships. These opportunities coexist with risks that may arise from user interaction and from the design of digital services. Direct messaging, livestreaming, open communities, recommendation systems, and persistent content circulation can expose children to unwanted contact, bullying, sexual exploitation, harmful material, and privacy loss. These risks cannot be explained solely by children's individual choices or parental supervision; they are also shaped by and platform architecture, default settings, and the way services collective and use personal data.

The problem of children's online safety therefore requires a governance approach that combines protection, access to beneficial digital services, and respect for children's rights. The OECD's review of 50 online services used by children found substantial variation in age-assurance practices and reported that only a small number systematically assured users' ages when accounts were created (OECD, 2025a). The finding illustrates a gap between declared minimum-age policies and the mechanisms used to implement them. An age gate based primarily on self-declaration may provide limited protection where users can easily enter an inaccurate date of birth or where safeguards are applied only after a problem is reported.

Indonesia has developed a multi-layered legal framework for child protection in electronic systems. The Child Protection Law establishes the state's obligation to protect children from violence and exploitation. Law No. 1 of 2024 amending the Electronic Information and Transactions Law strengthens the legal basis for child protection in electronic-system governance. Law No. 27 of 2022 on Personal Data Protection establishes safeguards for personal-data processing, including special protection for children's data. Government Regulation No. 17 of 2025 on the Governance of Electronic System Implementation in Child Protection then sets out obligations for electronic-system providers, including age-related safeguards and risk-based protection. Its implementing regulation, Minister of Communication and Digital Regulation No. 9 of 2026, further develops the implementation framework (Indonesia, 2014, 2022, 2024, 2025a, 2026).

This regulatory development changes the question that should guide legal analysis. The issue is no longer adequately framed as whether Indonesia has rules on children's online protection. Rather, it is whether the existing framework can be translated into clear, proportionate, and verifiable obligations for platforms. The implementation of age assurance must also be reconciled with privacy and data minimisation. A system that protects children by requiring

every user to submit full identity documents or biometric data may create a different set of risks, including excessive collection, retention, profiling, and data breaches.

Comparative experience offers useful but non-transferable models. Australia's Social Media Minimum Age framework places an obligation on covered platforms to take reasonable steps to prevent users under 16 from holding accounts on age-restricted social media services (Australia, 2024; eSafety Commissioner, 2026). The United States' Children's Online Privacy Protection Act (COPPA) framework focuses on parental consent and safeguards around the collection and use of personal information of children under 13; amendments finalised in 2025 strengthened controls on third-party disclosure and data retention (Federal Trade Commission [FTC], 2025). These models pursue different regulatory goals and should not be treated as interchangeable.

This article argues that Indonesia should not rely exclusively on either a blanket age threshold or parental consent. Instead, it should develop an integrated system in which account eligibility, feature-level risk, privacy-preserving age assurance, regulatory supervision, and digital education reinforce one another. The article contributes to this debate by connecting Indonesia's current legal framework with comparative regulatory approaches and proposing an implementation model that can be evaluated through evidence of platform compliance.

METHOD

This study uses doctrinal legal research. The statutory approach is applied to examine the content, relationship, and implementation of Indonesian legal instruments governing child protection, electronic systems, and personal-data processing. The conceptual approach clarifies the concepts of age assurance, risk-based regulation, privacy-by-design, platform accountability, auditability, co-regulation, and digital citizenship. The comparative approach considers Australia's Social Media Minimum Age framework and the United States' COPPA framework to identify regulatory options relevant to Indonesia.

Primary legal materials consist of Law No. 35 of 2014 amending the Child Protection Law, Law No. 1 of 2024 amending the Electronic Information and Transactions Law, Law No. 27 of 2022 on Personal Data Protection, Government Regulation No. 17 of 2025, Minister of Communication and Digital Regulation No. 9 of 2026, Australia's Online Safety Amendment (Social Media Minimum Age) Act 2024, and the United States' COPPA Rule. Secondary materials include OECD publications on age assurance and the Council of Europe's Digital Citizenship Education Handbook. Materials were collected through document study and analysed qualitatively through legal interpretation, comparison of

regulatory objectives and instruments, and assessment of whether the rules establish responsibilities that can be monitored and enforced.

The research is doctrinal and policy-oriented rather than an empirical evaluation of platform compliance. Accordingly, the article identifies legal and institutional design issues but does not claim to measure the actual effectiveness of the Indonesian regime in reducing harm. Such claims would require platform-level data, implementation records, and independent outcome evaluation.

RESULT AND DISCUSSION

From General Child Protection to Risk-Based Digital Governance

The Indonesian framework should be read as a connected legal structure rather than as a single age-restriction rule. The Child Protection Law supplies the substantive obligation to protect children, while the electronic-information regime addresses responsibilities arising from the provision and use of electronic systems. The Personal Data Protection Law constrains how information may be collected, used, retained, and disclosed. Government Regulation No. 17 of 2025 translates these principles into governance duties for electronic-system providers, and Minister of Communication and Digital Regulation No. 9 of 2026 supplies implementing provisions (Indonesia, 2014, 2022, 2024, 2025a, 2026).

This framework supports a shift from reactive responses to individual incidents toward preventive governance. A purely reactive model waits for reports of bullying, exploitation, or harmful content before taking action. A preventive model also examines foreseeable risks built into products and features, including the ease with which strangers can contact children, the default visibility of profiles, the design of recommendation systems, and the availability of reporting and appeal mechanisms. Risk-based governance does not mean that every service must be treated identically. It requires providers and regulators to identify relevant risks, justify the safeguards selected, and review whether those safeguards work.

The existence of detailed implementing rules also means that a claim of a continuing regulatory vacuum must be stated carefully. As of 2026, Indonesia has adopted Minister of Communication and Digital Regulation No. 9 of 2026 as an implementing instrument for Government Regulation No. 17 of 2025. The remaining analytical issue is whether the rules and their administration produce sufficiently clear technical expectations, consistent assessments, and verifiable compliance. This is an implementation and oversight question, not a claim that no legal framework exists.

Age Thresholds, Account Eligibility, and Privacy-Preserving Age Assurance

Age thresholds and age assurance perform different functions. An age threshold specifies the age at which a user may access an account, service, or feature. Age assurance refers to the methods used to establish or estimate

whether the user falls within a relevant age range. A threshold without a credible assurance mechanism may be ineffective; an intrusive assurance mechanism may undermine privacy even if it improves age accuracy. A sound legal design must address both effectiveness and proportionality.

Age assurance commonly involves age verification, age estimation, or age inference. Verification uses authoritative evidence or credentials to confirm age. Estimation predicts an age range through technical methods and may involve statistical error or bias. Inference draws conclusions from indirect indicators, such as account activity or contextual signals, but can encourage opaque profiling if it depends on extensive behavioural data. The OECD (2025a, 2025b) shows that age-assurance methods and their legal requirements vary substantially across services and jurisdictions. No single method is suitable for every service or risk.

The principle of proportionality therefore requires a tiered approach. Less intrusive methods should be considered for lower-risk services, while stronger assurance may be justified for features associated with higher risks. Any escalation in assurance should be justified by the risk and should not automatically require collection of complete identity documents or biometric information. The system should also include correction and review procedures for users who are incorrectly classified, so that an error in age estimation does not become an unchallengeable barrier to access.

Privacy-by-design is essential to this approach. The Personal Data Protection Law treats children's data and biometric data as sensitive categories requiring special attention, and establishes principles governing lawful and limited processing (Indonesia, 2022). A privacy-preserving model should therefore collect only the attributes necessary to determine eligibility, restrict the use of assurance data to that purpose, limit retention, and prevent reuse for advertising or unrelated profiling. Where technically feasible, a trusted third party or attribute-based mechanism could confirm an age category and return only the minimum result required by the service, rather than disclosing a user's full identity.

The policy objective should not be maximum data collection in the name of child protection. Instead, it should be sufficient assurance for a clearly defined risk, with the least intrusive method that can reasonably achieve the required level of confidence. This aligns child safety with the data-minimisation obligations of the Indonesian legal framework and with the privacy safeguards present in Australia's minimum-age regime and the United States' COPPA framework (Australia, 2024; FTC, 2025).

Comparative Lessons from Australia and the United States

Australia's Social Media Minimum Age framework, which took effect on 10 December 2025, requires covered social media platforms to take reasonable steps to prevent Australians under 16 from creating or maintaining accounts. The obligation is directed primarily at platform providers rather than relying exclusively on parents to enforce age limits. The Australian model offers a clear compliance target and places responsibility on services whose design and registration systems shape access (Australia, 2024; eSafety Commissioner, 2026).

However, a minimum-age model does not remove the need to consider privacy, proportionality, or access to beneficial online services. If platforms respond by requiring all users to provide highly identifying information, the implementation may create new data risks. The Australian approach is therefore most useful to Indonesia as an example of platform-side responsibility and reasonable-steps obligations, not as a rule that must be copied without regard to Indonesian law and context.

The United States' COPPA framework takes a different approach. It requires covered operators to obtain verifiable parental consent before collecting, using, or disclosing personal information from children under 13, subject to the rule's scope and exceptions. The FTC's 2025 amendments strengthened protections concerning third-party disclosure, data retention, and transparency in approved safe-harbor programmes (FTC, 2025). COPPA therefore provides a useful example of data-governance obligations and parental consent, but it is not a comprehensive substitute for rules addressing harmful content, grooming, or risky platform features.

The two models reveal different regulatory emphases: Australia focuses on preventing account ownership below a specified age on covered services, while COPPA focuses on the collection and use of children's personal information. Indonesia's framework can combine relevant elements without adopting either model wholesale. It can impose platform-level duties, differentiate risks by service and feature, and require privacy-preserving age assurance and meaningful parental involvement where appropriate. The key is to specify which risks each instrument addresses and how compliance will be demonstrated.

Platform Accountability, Co-Regulation, Auditability, and Sanctions

Legal duties are effective only when providers can understand what is required and regulators can assess whether those requirements have been met. Platform accountability should therefore extend beyond the existence of a written policy or a minimum-age notice. Providers should be able to document their risk assessments, the rationale for selecting particular age-assurance methods, the safeguards applied to high-risk features, the handling of complaints, and the

correction of errors. Such evidence allows oversight to focus on actual system design and implementation rather than on formal statements of commitment.

Co-regulation may help translate broad legal objectives into technical practices that can evolve as services change. Under this approach, the state defines outcomes and minimum legal standards, while industry codes or technical standards specify how services in different categories can meet them. Co-regulation should not mean voluntary self-regulation without oversight. Codes need clear approval criteria, public accountability, periodic review, and regulatory power to intervene where the measures are inadequate. The legal duties established by Government Regulation No. 17 of 2025 and its implementing regulation provide the basis against which such implementation mechanisms should be assessed (Indonesia, 2025a, 2026).

Auditability is a necessary condition for meaningful platform accountability. Depending on the risk, evidence may include age-assurance documentation, testing results, records of underage-account reports, response times, feature-level safeguards, complaint outcomes, and records of corrective action. Audits should be designed to avoid collecting more children's personal data than necessary. A regulator should be able to test whether a provider's system meets the relevant legal standard without turning the audit process into an additional source of surveillance.

Administrative enforcement should be proportionate to the seriousness, duration, and impact of a violation, while remaining consistent with applicable law and due process. Responses may include directions to remedy deficiencies, formal warnings, financial penalties, restrictions on particular products or features, or stronger measures where legally authorised and warranted. A feature-targeted response may be more proportionate than suspending an entire service where the risk arises from a particular function. Conversely, repeated or systemic failures should not be treated as minor procedural lapses merely because a platform has published a safety policy.

The concept of a safe-harbour or certification pathway requires particular care. Such a mechanism should not create immunity from legal responsibility. At most, independently assessed compliance programmes may provide evidence of good-faith risk management or support proportionate enforcement decisions where the law permits. Any incentive should depend on verifiable performance, transparent criteria, and continuing review. The objective is to encourage prevention and improvement without allowing certification to replace substantive legal duties.

Digital Citizenship, Parental Mediation, and School-Based Prevention

Age assurance and enforcement cannot independently address every form of online harm. Children also need the knowledge and support required to

recognise unsafe interactions, protect personal information, respond to coercive behaviour, and report harmful incidents. Richardson and Milovidov (2022) describe digital citizenship as a set of values, attitudes, skills, knowledge, and critical understanding that enables responsible participation in digital life. This framework extends beyond basic technical competence to include well-being, rights, privacy, security, and responsible interaction.

Parental mediation can connect platform controls with children's everyday use of digital services. It may involve discussion of online experiences, shared rules, age-appropriate settings, and guidance on how to report troubling interactions. However, parental supervision should not be treated as a substitute for platform responsibility. Parents cannot independently and redesign recommendation systems, disable unsafe defaults for every user, or investigate all forms of platform-mediated exploitation. Platforms should provide unders tandable controls and information that make parental involvement meaningful rather than shifting the entire burden of protection onto families.

Schools can provide a structured setting for digital citizenship education, counselling, and response to online incidents that affect students' well-being and learning. A school-based approach may include age-appropriate instruction on privacy, consent, respectful communication, grooming and sextortion warning signs, evidence preservation, and reporting pathways. It should also establish clear procedures for responding to disclosures, protecting confidentiality, and referring cases to appropriate services. The Council of Europe's digital citizenship framework supports integrating these competencies into education rather than treating online safety as an isolated technical topic (Richardson & Milovidov, 2022).

For education to function as part of governance, it should be accompanied by measurable objectives. Indicators may include the availability of age-appropriate materials, educator training, child-friendly reporting information, school response protocols, and periodic evaluation of programme implementation. Education is not a replacement for legal enforcement, but it can strengthen prevention and help children exercise their rights within a digital environment.

An Integrated Governance Model for Indonesia

The analysis supports an integrated model with four connected components. First, account eligibility and feature access should be determined through risk assessment rather than a single undifferentiated rule for every service. Second, age assurance should be proportionate, privacy-preserving, correctable, and limited to the purpose for which it is used. Third, platform duties should be auditable through evidence of design choices, safeguards, complaint handling, and remedial action. Fourth, digital citizenship, parental

mediation, and school-based procedures should support prevention and response.

These components should be implemented through a transparent division of responsibility. The state should define legal outcomes, technical minimums, supervisory procedures, and sanctions. Platforms should assess and mitigate foreseeable risks, provide age-appropriate safeguards, protect personal data, and produce evidence of compliance. Parents and schools should be supported through clear information and accessible tools, but should not bear the primary responsibility for risks created by platform design. Children should have understandable information, accessible reporting channels, and a means to challenge mistaken age classifications or decisions affecting their access.

Evaluation should focus on outcomes and verifiable implementation rather than the mere existence of policies. Relevant indicators may include the accuracy and error rates of age-assurance systems, the amount and retention period of data collected, the effectiveness of feature restrictions, complaint response times, remediation rates, and the accessibility of appeal mechanisms. Public reporting should be designed to support accountability while protecting children's identities and sensitive information. Because this study does not include empirical platform data, these indicators are proposed as a framework for future regulatory evaluation rather than as evidence that the current regime has already achieved particular outcomes.

CONCLUSION

Indonesia's child online-safety framework has developed beyond general statements of protection. The Child Protection Law, the electronic-information regime, the Personal Data Protection Law, Government Regulation No. 17 of 2025, and Minister of Communication and Digital Regulation No. 9 of 2026 provide a connected legal basis for protecting children in electronic systems. The central challenge is to ensure that these instruments produce clear, proportionate, and verifiable implementation in social media services. Accordingly, the remaining problem should be described as one of regulatory implementation, technical consistency, supervision, and evidence—not as a complete absence of legal regulation.

Australia's Social Media Minimum Age framework demonstrates the value of assigning responsibility to platforms for enforcing account-age restrictions, while the United States' COPPA framework illustrates the importance of parental consent, data minimisation, retention limits, and restrictions on third-party disclosure. Neither model alone addresses every form of online harm. Indonesia should therefore pursue a combined approach that differentiates risks by service and feature, adopts privacy-preserving age assurance, requires auditable

platform safeguards, applies proportionate enforcement, and embeds digital citizenship education in family and school settings.

The principal contribution of the article is an integrated governance proposal that treats age limits as one instrument within a broader child-protection architecture. Further research should examine how the 2025 and 2026 Indonesian regulations are implemented by platforms, whether age-assurance mechanisms are accurate and privacy-preserving, how complaints and sanctions are administered, and whether the measures produce demonstrable improvements in children's online safety.

BIBLIOGRAPHY

Australia. (2024). Online Safety Amendment (Social Media Minimum Age) Act 2024 (No. 127, 2024). Federal Register of Legislation. https://www.legislation.gov.au/C2024A00127/latest/details

eSafety Commissioner. (2026). Social media age restrictions. Australian Government. https://www.esafety.gov.au/about-us/industry-regulation/social-media-age-restrictions

Federal Trade Commission. (2025, January 16). FTC finalizes changes to children's privacy rule limiting companies' ability to monetize kids' data. https://www.ftc.gov/news-events/news/press-releases/2025/01/ftc-finalizes-changes-childrens-privacy-rule-limiting-companies-ability-monetize-kids-data

Indonesia. (2014). Law No. 35 of 2014 concerning amendments to Law No. 23 of 2002 on Child Protection.

Indonesia. (2022). Law No. 27 of 2022 concerning Personal Data Protection. https://peraturan.bpk.go.id/Details/229798/uu-no-27

Indonesia. (2024). Law No. 1 of 2024 concerning the Second Amendment to Law No. 11 of 2008 on Electronic Information and Transactions.

Indonesia. (2025a). Government Regulation No. 17 of 2025 concerning Governance of Electronic System Implementation in Child Protection. https://jdih.komdigi.go.id/produk_hukum/view/id/965

Indonesia. (2026). Minister of Communication and Digital Regulation No. 9 of 2026 concerning Implementing Regulations for Government Regulation No. 17 of 2025 on Governance of Electronic System Implementation in Child Protection. https://jdih.komdigi.go.id/produk_hukum/view/id/1007

Organisation for Economic Co-operation and Development. (2025a). Age assurance practices of 50 online services used by children. OECD Publishing. https://doi.org/10.1787/a19853ab-en

Organisation for Economic Co-operation and Development. (2025b). The legal and policy landscape of age assurance online for child safety and well-being. OECD Publishing. https://doi.org/10.1787/4a1878aa-en

Richardson, J., & Milovidov, E. (2022). Digital citizenship education handbook: Being online, well-being online, rights online (2022 ed.). Council of Europe. https://www.coe.int/en/web/education/-/digital-citizenship-education-handbook

United States. (1998). Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501–6506.