January 2026

CCIA Comments on Indonesia's Governance of Child Protection in Electronic Systems (PP Tunas)[1]

CHAPTER I – GENERAL PROVISIONS

Article 1(4)

The definition of "Electronic System Operators" (ESOs) under Article 1(4) of the Draft Ministerial Regulation is exceptionally broad, covering "any individual, state administrator, business entity, and the community who provide, manage, and/or operate Electronic Systems." This lack of specificity creates immense legal uncertainty and an unmanageable compliance burden for virtually every digital service provider—e.g., any one of the approximately 200 million active websites globally. Critically, the regulation fails to distinguish between end-user-facing providers and upstream service providers, such as B2B infrastructure or digital technology companies that do not have a direct relationship with the public. To ensure proportionality and feasibility, Indonesia must use a risk-based approach to determine which services are high-risk, narrow this definition to include a reasonable nexus to Indonesia (beyond mere visibility), and exempt entities that provide purely intermediary or foundational B2B technical services (e.g., Content Delivery Networks).

CHAPTER II – MINIMUM AGE INFORMATION

Article 3(3)

Article 3(3) further widens the scope of ESOs to any entity whose products "may be used or accessed" by children. This broad jurisdictional reach is immediately complicated by the rigid categorization requirements imposed on any service captured by this definition. Specifically, the five distinct age brackets mandated by Article 3(2)—3-5, 6-9, 10-12, 13-15, and 16-18—appear arbitrary and technically impractical. It is unclear how companies can be expected to implement such granular restrictions, particularly since the legal "verification" of age under Article 19 and the mandate to effectively verify parental consent under Article 15 exceed current technical capabilities. Specifically, Article 19 requirements demand a level of accuracy that "age estimation" tools cannot provide for narrow, adjacent brackets without necessitating highly intrusive and risky data collection.[2] The Ministry should clarify Article 3(2) age bands and provide flexibility for general-use products not designed for narrow age groups.

Article 5

Additionally, the requirement for mandatory pre-launch self-assessments detailed in Article 5 delays critical safety updates and feature rollouts. Instead, the Ministry should give services

[1] https://peraturan.bpk.go.id/Details/316698/pp-no-17-tahun-2025
[2] https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8525.pdf

the flexibility to determine when assessments are necessary, focusing primarily on major product changes.

CHAPTER III – RISK PROFILE ASSESSMENT

Article 8(3)

Article 8(3) lists broad criteria for risk assessment, including causing "addiction" and "psychological health disorders." Under Articles 10, 12, 14, 15, 16, 17, and 18, a single "high-risk" value in any category designates the entire service as high-risk. However, there is no industry or academic consensus on what features of covered services warrant such designations. This requirement therefore risks being applied inconsistently across the industry, negating the benefits of a unified standard. Instead, the Ministry should establish a holistic, systemic risk assessment that accounts for a product's specific utility and existing safety measures while focusing on the actual likelihood and impact of harm rather than theoretical indicators.

Article 9

Article 9 presents significant operational hurdles by defining "unknown persons" through unverifiable real-world relationships and over-broadly categorizing low-risk public interactions as "contact" risks. To address this, the Ministry should define "unknown persons" via objective, platform-level features—such as user-approved contacts—while clarifying that parentally approved individuals (primarily for users under 13) are no longer considered "unknown." The framework should adopt a harm-based approach that prioritizes the risks of direct, private communication while exempting inherently lower-risk public engagements like comments and mentions.

Article 10

Article 10's blanket classification of profile discoverability as a high-risk indicator fails to account for effective mitigations like granular privacy controls and default-private settings for minors. Discoverability should only be considered a significant risk when paired with the functionality for direct, private contact, rather than triggering a "high-risk" label in isolation.

Article 11

The current definitions of harmful content are overly broad and subjective, risking the inadvertent censorship of low-risk or beneficial material, such as educational, scientific, or documentary content. Instead, the Ministry should adopt specific, high-severity harm thresholds, while replacing the requirement to assess an individual child's psychological maturity with a more feasible focus on the general developmental stages of minor cohorts.

Articles 13-14

Articles 13 and 14 create an inconsistent risk framework by failing to distinguish between harmful "dark patterns" and harmless commercial activities, such as contextual advertising or routine teen transactions. The Ministry should focus on manipulative, covert practices rather

than standard business functions, while taking a developmentally appropriate approach that limits mandatory parental transaction-level approval to children under 13 to respect the autonomy of older teens.

Article 15

Article 15 imposes a "high-risk" classification on services that cannot effectively verify parental consent for the data processing of all minors under 18. The Ministry should limit mandatory parental consent to children under 13 and recognize that the data risks for teenagers (13-17) are effectively mitigated through robust privacy-by-design defaults–such as private-by-default uploads and the absence of personalized ads–rather than strict parental intervention.

Article 16

Article 16 further broadens the definition of ESO, as the indicators for "may be used or accessed by children" includes subjective factors such as "immersive design" that creates an "illusion for users," "gamification," and the use of "infinite scrolling." Because these features are common across various digital platforms, entities not primarily intended for minors may find it difficult to determine if their design choices inadvertently trigger high-risk classifications and legal obligations. As mentioned above, the Ministry should adopt a holistic risk assessment that considers systemic safety rather than penalizing specific design features, recognizing that digital well-being tools and parental controls effectively mitigate the risks of infinite scrolling and push notifications.

Articles 17-18

Articles 17 and 18 introduce significant legal and operational uncertainty by basing risk classifications on subjective, undefined metrics like "significant periods of time" or "excessive" usage. The Ministry should remove these vague behavioral qualifiers and replace them with specific, measurable harms to align the framework with objective international standards that focus on content that clearly impairs a minor's development rather than subjective interpretations of health outcomes.

Article 19

The current framework creates a legal conflict between articles that automatically "deem" products high-risk and Article 19, which suggests risk can be mitigated to a low level. The mandate should explicitly state that robust mitigation measures can override high-risk classifications and clarify that the provided list of mitigations is a non-exhaustive set of examples, allowing providers the flexibility to implement alternative, context-specific safeguards.

Articles 20-26

The broad definition of ESOs, combined with the Minister's sole authority to determine risk profiles through verification of internal self-assessments detailed in Articles 22-24, mirrors

regulators' "unfettered power" in other jurisdictions like Australia.[3] Leaving risk profiling to the Minister's full discretion creates significant regulatory uncertainty and lacks objective guardrails necessary for industry compliance. This ambiguity is compounded by undefined "spot checks" and the power to summon officials for minor, non-material discrepancies. Instead, the Ministry should establish transparent, neutral criteria, an independent expert review process, and a defined process for providers to object to ministerial determinations. These measures would yield risk designations based on clear, evidence-based harm metrics rather than subjective regulatory determinations. Additionally, by granting the executive branch substantial discretion to label services "high-risk," the law risks targeting popular U.S.-based digital services based on political visibility rather than neutral, function-based risk assessments. This asymmetry creates legal uncertainty and *de facto* barriers to market access, undermining digital trade.

Furthermore, the framework allows unverified community complaints and generic "material changes" to trigger mandatory re-evaluations, risking regulatory instability and unnecessary paperwork for minor product updates. The Ministry should establish rigorous evidentiary standards for "new material facts" and limit mandatory re-assessments to changes that significantly impact core risk categories. Ultimately, classification should focus on residual risk after mitigation efforts are considered, preventing irrelevant product modifications or malicious reports from arbitrarily inflating a services' risk profile.

Article 27

The lack of clear standards is compounded by the inflexible compliance mandates triggered once a service is categorized. Article 27 imposes rigid account ownership restrictions, dictating that children under 16 may only have accounts on products classified as "low-risk." Rather than specifying a clear operational standard, Article 15 mandates that parental consent for data processing must be "verified effectively." If an ESO cannot meet this vague technical threshold, the service is automatically designated as 'high-risk' under Article 15(6), triggering the account creation ban for minors under 16.

These blunt instruments drive minors away from responsible websites with established safety measures and toward more opaque, less-regulated spaces with greater exposure to illegal and dangerous content. For instance, Article 27(8) requires ESOs to provide technical tools that empower parents to supervise their children's activities. However, this parental control is undermined by the threat of "blanket bans"—specifically the "temporary suspension" or "termination of access" authorized under Articles 58 and 59. These state-level bans effectively override individual parental discretion; a parent cannot use supervision tools on a service that the Ministry has blocked entirely. To improve technical efficacy and safety, Indonesia should focus on a harm-based approach that prioritizes parental controls and safety-by-design mitigations over total account prohibitions, while maintaining the targeted scope in Article 27(1) which limits these requirements to services that require account registration.

---

3 https://ccianet.org/wp-content/uploads/2025/12/Australias-Social-Media-Minimum-Age-Act-Poses-Threats-to-U.S.-Digital-Competitiveness.pdf

CHAPTER IV – SUPERVISION OF ELECTRONIC SYSTEMS OPERATIONS

Articles 30-37

Articles 30-37 grant the Minister authorities to "trace people," "collect descriptions," and "assess electronic system facilities." However, these powers are currently triggered by "potential" violations or speculative reports of acts that "will" occur, rather than actual breaches. This broad regulatory discretion granted to the Minister, coupled with expansive investigative powers that mandate the collection and processing of sensitive information from ESOs, creates significant privacy and security risks for companies and associated user data. Instead, supervision must be conditioned on strict judicial oversight, alignment with existing data protection laws, and decentralized, privacy-preserving standards that prohibit the creation of centralized identity databases that could be exploited by malicious actors or subject to governmental abuse.

Furthermore, enforcement triggers–such as the 25-child intervention threshold–should be based on actually affected individuals rather than untechnical estimates of those who "might be" impacted. To ensure proportionality, the "further examination" process should include a materiality threshold for summons and explicitly allow for "no-admission settlements," similar to the frameworks used by the KPPU or OJK. This shift would prioritize collaborative, efficient safety improvements over resource-intensive adversarial proceedings, focusing regulatory efforts on rectifying material harms rather than speculative discrepancies.

CHAPTER V – ADMINISTRATIVE SANCTIONS

Article 53

Article 53 permits severe sanctions, including administrative fines, "temporary suspension," and "termination of access" (blocking). While the Draft RPM stipulates that fines will follow non-tax state revenue regulations (Article 57(2)), the Ministry should establish a clear, predictable cap on fines, include a judicial review mechanism, and reserve "termination of access" only for the most extreme cases of repeated, intentional non-compliance to avoid creating *de facto* trade barriers against foreign service providers.

Article 55

Article 55(5) introduces significant legal uncertainty by basing administrative sanctions on overly broad and subjective considerations, such as the "gravity" of a violation and vague "other factors" that may aggravate or mitigate penalties. These criteria should be limited to clear, objective, and measurable factors that provide ESOs with a transparent understanding of potential liability.

CHAPTER VI – OBJECTION AND ADMINISTRATIVE APPEAL PROCEDURES

Article 63(4)

Article 63(4) stipulates that filing an objection shall "not delay the implementation of the decision" regarding administrative sanctions. This "enforce-first" model violates the principles

of legal certainty and fairness, as it subjects providers to potentially irreversible penalties–such as the "termination of access" authorized under Article 59–before the validity of the sanction is fully adjudicated. While Article 66 allows for a state administrative court review, the absence of a mandatory stay means that the commercial and reputational damage would be impossible to undo even if the provider eventually wins the appeal.

To ensure due process and prevent the immediate execution of sanctions that may later be ruled an abuse of authority, the regulation should be amended to provide an automatic stay of all sanctions while an objection under Article 64 or an administrative court appeal under Article 68 is pending. This would align the regulation with the broader spirit of Indonesian administrative justice, ensuring that punitive measures are only enforced once a decision is truly final and binding.

CHAPTER VII – TRANSITIONAL PROVISIONS

Article 71(1)

Article 71(1) provides a six-month transition period for ESOs to adjust to the new governance and technical requirements. Given the technical difficulties involved in implementation, any fixed timeline at this point would be inappropriate. At a minimum, this timeline must be synchronized with the two-year adjustment period granted by Government Regulation (GR) 17/2024 to maintain legal validity. Under the Indonesian hierarchy of laws (Lex Superior Derogat Legi Inferiori), a Ministerial Regulation cannot impose a more restrictive window than the higher-level GR from which it derives its authority.

Given the technical ineffectiveness of current age-gating tools and the potential for regulatory contagion to drive users to less-regulated spaces, even a two-year window may be insufficient for the maturation of secure, standards-based age assurance. Instead of a fixed deadline, Indonesia should allow for a comprehensive, public assessment of technical feasibility, economic impact, and privacy risks to ensure that such mandates do not stifle digital innovation or create unmanageable operational burdens.