DENTONS HPRP

Grow | Protect | Operate | Finance

# Children online: how Indonesia's government is setting new rules for protection in the digital world

Prepared by:

**Andre Rahadian (Partner), Mika Isac Kriyasa (Partner), Thalia Kalista (Associate)** and Yasyfa Alifya Radiany (Assosiate)

The recent enactment of Government Regulation Number 17 of 2025 concerning Governance of Electronic System Implementation in Child Protection ("**GR 17/2025**") on 27 March 2025. As digital transformation accelerates and information and communication technology become increasingly influenced in every aspect of daily life, children have emerged as active users of a wide range of digital platforms and tools. From computers, laptops, tablets, and smartphones to game consoles, websites, and social media, children are engaging with a diverse array of products, services, and features developed or operated by Electronic System Providers ("**ESP**"). These technologies are not just sources of entertainment, they serve as essential instruments that children use to fulfill their needs and interests, particularly in how they interact and communicate within the digital realm.

## Background: Children as Users

The internet exposure rate in Indonesia has reached approximately 79,5%, with an estimated 221 million users.[1] This big internet wave has brought Indonesia as one of the leading countries globally in terms of usage volume. According to data from statistics, an overwhelming 88,99% of children aged 5 years and above access the internet primarily for social media purposes.[2]

A child in this category referred to as someone who is under 18 (eighteen) years of age.[3] In various situations, children do not yet possess the capability to fully comprehend the risks or potential violations of their rights that may arise from the use of products, services, and features.[4] This lack of readiness makes electronic interactions or communications conducted by children potentially increase the risk of their privacy and safety being exposed.[5] Some concrete examples of such negative impacts include the use or sale of children's data for marketing purposes or other unlawful interests, as well as economic exploitation and sexual abuse of children.[6]

## General Obligation for ESP

ESP in this manner shall refer to any individual, state administrator, business entity, or member of the public who provides, manages, and/or operates an Electronic System, either independently or jointly, for their own purposes and/or for the purposes of other parties.[7] By referring to MOCD Regulations Number 5 of 2020 concerning Private Electronic System Provider ("**MOCD 5/2020**"), ESP shall also include foreign entities who registered their Electronic System in Indonesia.

ESP are required to provide protection for children who use or access Electronic Systems.[8] The protection as referred to includes the protection of children's rights as stipulated in the laws and regulations concerning the use of Products, Services, and Features that are developed and/or operated by Electronic System Operators.[9]

In providing Products, Services, and Features for Children, Electronic System Operators must apply technology and operational technical measures to provide protection from the development stage to the implementation stage of the Electronic System.[10]

[1] Ministry of Communication and Digital, "Komitmen Pemerintah Melindungi Anak di Ruang Digital" https://www.komdigi.go.id/berita/artikel/detail/komitmen-pemerintah-melindungi-anak-di-ruang-digital, accessed on 24 April 2024.

[2] Annur, Cindy Mutia, Databoks, "BPS: 88,99% Anak 5 Tahun Ke Atas Mengakses Internet untuk Media Sosial" https://databoks.katadata.co.id/teknologi-telekomunikasi/statistik/911fee2b83d9741/bps-8899-anak-5-tahun-ke-atas-mengakses-internet-untuk-media-sosial, accessed on 24 April 2024.

[3] Article 1 paragraph (1) of GR 17/2025.

[4] Elucidation of GR 17/2025

[5] Ibid.

[6] Ibid.

[7] Article 1 paragraph (4) of GR 17/2024

[8] Article 2 paragraph (1) of GR 17/2024

[9] Article 2 paragraph (2) of GR 17/2024

[10] Article 2 paragraph (3) of GR 17/2024

In providing the protection, ESP are required to provide:[11]

a. information regarding the minimum age limit for children who may use their products or services;

b. a mechanism for verifying child users; and

c. a mechanism for reporting the misuse of products, services, and features that violate or have the potential to violate children's rights.

These Products, Services, and Features shall consist of (i) Products, Services, and Features that are specifically designed to be used or accessed by Children; or (ii) Products, Services, and Features that may potentially be used or accessed by Children.

Products, Services, and Features that are potentially used or accessed by Children must meet specific indicators to ensure compliance with child protection regulations.[12] These indicators include the existence of internal policies or documented statements from Electronic System Operators that clearly acknowledge the accessibility of such Products, Services, and Features by children. Further, strong evidence should demonstrate that a significant portion of users who regularly use these Products, Services, and Features are children. Additionally, if the content or themes of these Products, Services, and Features are explicitly directed toward children, or if the visual elements and design are tailored in a child-friendly manner, they may also fall within this category. Even if a Product, Service, or Feature is not explicitly targeted at children, but is similar to those that are, and it is known that children frequently access it, then it is also subject to these considerations. The final determination of which Products, Services, and Features fall under this classification is established by a Ministerial Decree.

### Risk Assessment on the Electronic System

Products, Services, and Features as are based on their risk levels to children, which are classified into three tiers: **high risk, medium risk, and low risk**.[13] This classification is determined by evaluating several factors, including exposure to inappropriate behaviour or content; the presence of violent, pornographic, or criminal elements; features that allow interaction with unknown users; potential violations of children's personal data; threats to children's psychological well-being; and the impact on their physical development.

If a Product, Service, or Feature is determined to have a high-risk level, it may be subject to additional obligations or restrictions. These may include limitations on promotion, requirements for specific safety features, or even access restrictions for child users. The responsibility lies with the Electronic System Operator to conduct a regular risk assessments, apply appropriate technical safeguards, and ensure ongoing protection for child users. The implementation of such measures must align with applicable regulations and may be subject to government oversight or ministerial decisions.

### Parents' Consent

Electronic System Providers are required to obtain consent from a child's parent or legal guardian before granting access to products, services, or features.[14] If the services are intended for children under 17 years old, providers may also request the child's consent but must notify the parent or guardian for confirmation. Providers must allow a reasonable amount of time to obtain this consent. If consent is denied by the parent or guardian, the provider is prohibited from giving the child access. In such cases, the provider must terminate access and delete any personal data collected from the child.

### Age Group

ESP that require users to register or hold an account must enforce the following age-based rules:[15]

| Age Group | Requirements |
|---|---|
| Under 13 years old | May only register for child-specific, low-risk products, services, and features—and only with prior parental or guardian consent. |
| Ages 13 to under 16 | May register for low-risk products, services, and features—with parental or guardian consent. |
| Ages 16 to under 18 | May register for any products, services, and features—but still only with parental or guardian consent. |
| 18 years and older | May register and access all products, services, and features freely, without parental approval. |

[11] Article 2 paragraph (4) of GR 17/2024
[12] Article 4 paragraph (2) of GR 17/2024
[13] Article 5 paragraph (1) of GR 17/2025
[14] Article 9 paragraph (1) of GR 17/2025
[15] Article 21 of GR 17/2025

## Child Privacy and Data Protection

Children's personal data under this regulation encompasses any information that can identify or profile a child, including:[16]

| Data Category | Scope |
|---|---|
| Identification data | real name, aliases, postal or email addresses, online identifiers (IP, account names), social security or license numbers, passports, and similar unique identifiers. |
| Commercial information | records of products or services purchased, obtained, considered, or consumed, and related transaction histories or trends. |
| Biometric data | fingerprints, facial scans, voiceprints, or similar biological measurements. |
| Internet and network activity | browsing history, search queries, and interactions with online applications or advertisements. |
| Geolocation data | real-time or historical location information. |
| Audio/visual data | photographs, videos, voice recordings, and other similar media. |
| Professional and educational information | details about the child's work (if any) and schooling. |
| Inferences and profiling | conclusions drawn from any of the above to create a profile reflecting the child's preferences, characteristics, psychological trends, behavior, abilities, or aptitudes. |
| Other sensitive personal data | financial information, security credentials (passwords, access tokens), private communications (emails, messages), health records, and information about race, religion, or philosophical beliefs. |

These types of personal data, collected from children, require strict compliance with privacy and security standards to ensure their protection.[17] This includes obtaining proper parental consent and offering transparent options for data access, correction, or deletion.

## Education and Digital Literation

ESP are required to conduct education and empowerment initiatives to build a digital ecosystem that ensures the protection and fulfilment of children's rights. This education must be provided to[18] both children and their parents or guardians, particularly for those using products, services, and features developed or operated by the providers. Empowerment efforts include increasing digital literacy among the public, enhancing employee competencies regarding child protection, and developing infrastructure that supports children's digital literacy. Providers must also report their educational and empowerment activities to the relevant Minister and participate in evaluations based on submitted reports.

## Obligations of ESPs

In the spirit of granting child protection, ESPs are required to implement the following obligations which, due to their legal and regulatory complexities, may necessitate the assistance of a legal counsel. The work we can assist with in fulfilling the related obligations includes, among others, the following:

| Obligations | Legal Counsel's Role |
|---|---|
| secure verifiable parental or guardian consent | preparing parental or guardian consent form in compliance with PDP Law[19] and GR 17/2025 |
| complete Data Protection Impact Assessments ("**DPIA**") | preparing DPIA in compliance with PDP Law and GR 17/2015 |
| configure the default settings of any products, services and features that are designed for or that are potentially accessible by children to a high level of privacy | advising on privacy-by-design settings and ensuring alignment with legal requirements for child data protection |
| provide accurate, complete and nonmisleading information to users in order to ensure product understanding | reviewing user-facing materials (e.g., terms of service, privacy policies) to ensure legal compliance and clarity |
| conducting education and empowerment of digital ecosystems | assisting in the development of educational content and programs that comply with applicable laws and child protection standards |

[16] Article 8 paragraph (5) b of GR 17/2025
[17] Article 17 of GR 17/2025
[18] Article 12 of GR 17/2025

| Obligations | Legal Counsel's Role |
|---|---|
| issue notifications, such as symbols or signals, when monitoring or tracking a child's activities or location | ensuring notification practices comply with legal standards on transparency and child monitoring limitation |
| offer functionality that is in line with the ages and developmental stages of children | advising on age-appropriate design and ensuring that offerings comply with child development and legal standards |
| clearly identify the parties responsible for the processing of children's personal data, as accessed through internet-connected toys or devices | drafting and/or reviewing agreements to clearly designate data controller/processor responsibilities and ensure legal accountability |
| ensure that any third parties that are appointed by or partner with ESP comply with child protection provisions | drafting and/or reviewing third-party agreements and conducting legal due diligence to ensure child protection compliance |
| appoint an official or officer who carries out the function of protecting personal data | advising ESPs on the qualifications, role, and responsibilities of the appointed officer in line with regulatory requirements |

### Sanctions

Violations of the above obligations related to the operation of Electronic Systems, especially concerning the protection of children's rights, are subject to administrative sanctions. These sanctions may include:

- written warnings;
- temporary suspensions, or termination of services.

The Minister has the authority to impose, announce, and publish these sanctions to the public through the Ministry's official platform. The type and severity of the administrative sanctions will depend on several factors, such as the nature and impact of the violation, the scale of the harm caused, and the level of negligence or intent involved. Special consideration is given to violations that affect children's safety and rights within electronic systems.

Although the regulations specify administrative sanctions, this does not preclude the possibility of criminal sanctions if relevant provisions of the Indonesian Criminal Code or other criminal laws are violated. For instance, if the violation also constitutes a criminal offense under the PDP Law, Child Protection Law, Indonesian Criminal Code, or other applicable criminal provisions, criminal liability may still be imposed in addition to administrative measures.

When this Government Regulation comes into effect, Electronic System Providers and other related parties involved in the management of Products, Services, and Features must adjust and comply with its provisions within a maximum period of two (2) years from the date the Regulation is enacted.

### Enforcement of GR 17/2025

It is important to emphasize that the obligations under Government Regulation Number 17 of 2025 apply extraterritorially. This means that foreign companies providing or offering digital products, services, or features to children in Indonesia, whether directly or indirectly, are required to comply with this regulation. This includes foreign ESPs that may not be physically established in Indonesia but whose digital offerings are accessible by or directed toward Indonesian children. This principle aligns with the universal nature of child protection and is further supported by the mandatory registration requirement for foreign ESPs under the MOCD Reg. 5/2020 concerning Private Electronic System Providers.

Furthermore, the Indonesian government has several mechanisms at its disposal to ensure compliance by ESPs, particularly foreign ones, with child protection regulations. These include:

1. Requiring the registration of foreign ESPs in Indonesia through the Online Single Submission (OSS) system as a prerequisite for bringing them under the scope of national jurisdiction.
2. Implementing administrative enforcement measures, such as issuing written warnings, temporary suspensions, or even blocking access to services in cases where violations of children's rights under GR 17/2025 are identified.
3. Requesting audits or compliance reports related to the ESPs' internal policies for child users, including age verification mechanisms, child data protection policies, and the performance of regular risk assessments.
4. Expanding international cooperation for legal enforcement, particularly in cases where foreign ESPs fail to comply in good faith or are based in jurisdictions lacking comparable child protection frameworks.

[19] Law No. 27 of 2022 concerning Personal Data Protection ("**PDP Law**")

These actions reinforce the broader data protection obligations for children as outlined in relevant personal data protection regulations and strengthen the state's position in ensuring that all digital actors—regardless of their country of origin—are held accountable for the impact of their services on children in Indonesia.

## Conclusion

In conclusion, the implementation of this Government Regulation marks a significant step toward strengthening the protection of children's rights in the digital ecosystem. Electronic System Providers are now obligated to prioritize child safety, transparency, and parental involvement across their products, services, and features. With clear requirements for consent, data protection, digital literacy education, and administrative sanctions for non-compliance, the regulation creates a more accountable and child-friendly online environment. The two-year transition period allows sufficient time for stakeholders to adapt, ensuring that the digital space evolves responsibly and in line with the best interests of children.

- o0o -