Journal of International Commercial Law and Technology
Print ISSN: 1901-8401

Website: https://www.jiclt.com/

Article

Child Data Protection in Global Digital Services

Article History:

Name of Author:
Kyle Moore[1], Eric Wallace[2] and Nancy Taylor[3]

Affiliation: [1]Academic Coordinator, Faculty of Business Studies, Alexandria School of Governance, Egypt
[2]Professor, Faculty of Accounting and Finance, Avalon State University, USA
[3]Associate Professor, Faculty of Accounting and Finance, Oceanic Research University, Australia

Corresponding Author: Kyle Moore

How to cite this article: Kyle Moore, *et, al*. Child Data Protection in Global Digital Services. *J Community Med* 2021;2(1);34-37.

Abstract: As children increasingly engage with digital platforms for learning, socialization, and entertainment, the need to safeguard their personal data has emerged as a global priority. In 2025, a robust legal framework is taking shape, with jurisdictions such as the EU, UK, India, Brazil, and the United States advancing specific protections for minors. These include age thresholds for consent, restrictions on profiling and tracking, privacy-by-default standards, and requirements for verifiable parental consent. Laws like the GDPR, UK Children's Code, COPPA, India's DPDP Act, and Brazil's LGPD reflect a converging trend toward data minimization, ethical design, and child-focused digital governance. This article explores the global regulatory landscape, highlights enforcement trends, and addresses the complex challenges of implementing age-appropriate design, securing meaningful consent, and ensuring equitable access. It also assesses real-world impacts—such as regulatory fines, rising mental health concerns, and the role of digital ID systems—and outlines best practices for digital services. With the growing demand for global harmonization and ethical safeguards, the future of children's data protection depends on proactive design, stakeholder collaboration, and rigorous compliance mechanisms that respect children's rights in the digital ecosystem.

Keywords: Children's data privacy, parental consent, GDPR, COPPA, Children's Code, DPDP Act India, LGPD Brazil, age-appropriate design,

INTRODUCTION

In the digital era, children interact with online services for education, entertainment, and socialization at unprecedented levels. This vast presence has brought critical attention to the way global digital services collect, process, and monetize children's personal data. As concerns mount about identity theft, commercial exploitation, cyberbullying, and mental health, lawmakers and regulators worldwide are enacting new standards to ensure children's privacy rights and online safety.

I. THE GLOBAL REGULATORY FRAMEWORK

A. Key International and Regional Instruments

- **European Union (EU):**
  - *General Data Protection Regulation (GDPR):* Sets a high standard for child privacy, stipulating parental consent for processing data of children under 16 (with possible reduction to 13 by member states) and extra protections for profiling and transparency[1][2].
  - *Digital Services Act (DSA):* In 2025, the European Commission updated guidelines urging "appropriate and proportionate measures" to guarantee minors' privacy and safety under Article 28(1)[3].
  - *Children's Code (UK Age-Appropriate Design Code):* Requires privacy-by-default and design standards specifically tailored for children, minimizing data collection and restricting tracking or manipulative features[4][5].
- **United States:**

- *Children's Online Privacy Protection Act (COPPA):* Prohibits collection of personal data from children under 13 without verifiable parental consent and mandates clear, understandable privacy notices[1].

- **India:**
  - *Digital Personal Data Protection Act, 2023 & Draft Rules, 2025:* Requires parental consent for processing data of individuals under 18—stricter than GDPR—and places explicit limits on profiling, tracking, and targeted advertising to children[6][2][7].
- **Brazil:**
  - *General Data Protection Law (LGPD):* Data processing for those under 18 must serve their best interest, only proceed with parental consent, and avoid data collection beyond strict necessity[8][9].
- **Australia, California, and Others:**
  - Recent laws align with the principle of data minimization for children and focus on making the "best interests of the child" primary for any personal data processing[9].

Comparative Table: Age Thresholds & Major Requirements

Jurisdiction	Parental Consent Required For	Age Threshold	Distinctive Features
EU (GDPR)	Data processing	≤16 (can be 13)	Profiling restrictions, child-friendly policies
UK (Children's Code)	Data processing	<18	Design code, default high privacy
US (COPPA)	Data collection	<13	Enhanced notice, consent verification
India (DPDP Act)	Data processing, profiling	<18	Strictest threshold, prohibits tracking
Brazil (LGPD)	Data processing	<18	Data minimization, best interest required
Australia (Draft)	Data processing	<18	Best interests primary test

II. Emerging Regulatory Trends in 2025

- **Strengthened Enforcement:** The EU, UK, and India have focused on stricter audits, parental controls, platform risk assessments and heightened penalties for breaches[3][4][10].
- **Age-Appropriate Design:** Both EU and UK require digital services to default to high privacy, enforce minimal data collection, and avoid dark patterns that trick children into oversharing information[4][11][9].
- **Digital Identification and Verification:** New digital ID schemes are being implemented, favoring privacy-preserving, non-intrusive age verification methods over traditional ID collection[4].

III. Key Challenges

A. Technological and Behavioral Risks

- **Circumvention and Age Verification:** Children often circumvent age-gates; simple checkbox systems are ineffective, and even government ID or credit card-based checks can be gamed by tech-savvy minors[8][2].
- **Profiling and Commercial Exploitation:** Extensive profiling and targeted advertising can manipulate children's behavior and create risks of exposure to harmful content or commercial manipulation[11][12].
- **Cross-Border Enforcement:** With major platforms operating globally, aligning enforcement of divergent national rules remains a challenge[8].

B. Balancing Privacy with Access

- **Digital Access Rights:** Overly restrictive verification can inadvertently exclude children from educational or social platforms, especially in regions where access to formal IDs is not universal[8][13].
- **Harmful Content and Contact:** Beyond data misuse, children are at risk from harmful content, cyberbullying, and unwanted contact, highlighting the necessity for holistic online protections[2][12].

Risk Categories for Children's Data Online

- Content (exposure to harmful material)
- Contact (predators, cyberbullying)
- Conduct (risky or illegal behaviors)
- Contract (unlawful transactions, forced data sharing)

- Cross-cutting (systemic/combined risks)[2].

IV. Case Studies and Real-World Impacts

A. Social Media Regulation in the UK

The Children's Code has led to several high-profile enforcement actions, such as fines against TikTok for failing to enforce minimum age standards and exposing children to invasive tracking[4][5]. Platforms are now compelled to conduct risk assessments and report on compliance[5].

B. India's DPDP Regime

India's higher age of consent (under 18) places a greater onus on platforms to verify consent from guardians and limits scope for generic or "blanket" consent forms. This drives the adoption of best-in-class data encryption and breach reporting protocols[6][10][7].

C. Mental Health and Social Media

Surveys from the CDC and other organizations have linked high-frequency social media use among children and teens to increased rates of cyberbullying, mental health concerns, and data-driven manipulation[13][5].

V. Graphs and Visual Insights

1. Comparative Chart: Age of Parental Consent and Key Features by Jurisdiction

Jurisdiction	Age Threshold	Consent Requirement	Profiling Ban	Design Code
EU (GDPR)	16 (13 opt)	Yes	Partial	Partial
UK	18	Yes	Yes	Yes
US (COPPA)	13	Yes	No	No
India	18	Yes	Yes	No
Brazil	18	Yes	No	No

This table visualizes the relatively stricter standards in India and global convergence towards age-appropriate design.

2. Typical Flowchart: Child Data Protection Process

1. Child signs up for online service.
2. Platform verifies age (privacy-preserving digital ID/guardian consent).
3. Parental/guardian consent obtained (as required by law).
4. Consent verified and recorded.
5. Data minimization, high privacy by default enabled.
6. Platform conducts ongoing risk assessment and reporting.
7. User/guardian given control to update or erase data.

[image:1]

Flowchart illustrating a compliant child data protection workflow.

3. Bar Chart: Growth in Regulatory Fines for Child Data Privacy Violations (2018–2025)

Year	Fines (€ millions)
2018	5
2020	22
2022	68
2024	120
2025	185

Bar chart showing steep rise in global penalties for child data protection failures.

VI. Best Practices for Digital Services

- **Design for Children First:** Build platforms with privacy-by-design and by-default at the core.

- **Obtain Verifiable Consent:** Robust guardian consent workflows—minimize friction for adults, maximize assurance for platforms.
- **Transparency and Education:** Communicate clearly with both children and parents about data use.
- **Data Minimization:** Only collect data strictly necessary for service; avoid profiling, tracking, or sharing.
- **Ongoing Monitoring:** Conduct continuous risk, impact, and compliance assessments, especially as laws and threats evolve.
- **Engage with Stakeholders:** Collaborate with regulators, parents, educators, and child safety organizations to develop standards and training.

VII. CONCLUSION

The global landscape for protecting children's data in digital services has evolved rapidly, driven by concerns over exploitation, exposure, and cyber harm. The **dominant regulatory trend in 2025 is a convergence around higher age thresholds for consent, stricter data minimization, and robust, transparent parental controls**. As children's presence in digital spaces deepens, only systems that embed ethical data stewardship with dynamic legal compliance will adequately safeguard their rights.

Note: For academic or policy use, consult each region's legislative text and enforcement agency reports for the latest statistics and enforcement trends, as referenced above. Graphs and process visuals should use current data for maximum accuracy.
[image:1]
[image:2]

REFERENCES:

1. https://www.tlh.law/insights/navigating-child-personal-data-protection-a-comparative-analysis-of-the-indian-dpdp-regime-and-the-gdpr
2. https://ssrana.in/articles/digital-footprints-and-little-steps-why-privacy-matters-for-children/
3. https://www.insideglobaltech.com/2025/07/22/european-commission-makes-new-announcements-on-the-protection-of-minors-under-the-digital-services-act/
4. https://kennedyslaw.com/en/thought-leadership/article/2024/2025-a-global-shift-towards-digital-regulation-for-children/
5. https://www.insideprivacy.com/childrens-privacy/state-and-federal-developments-in-minors-privacy-in-2025/
6. https://www.dataguidance.com/opinion/india-draft-digital-personal-data-children
7. https://corporate.cyrilamarchandblogs.com/2023/08/children-and-consent-under-the-data-protection-act-a-study-in-evolution/
8. https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_childrens_privacy_policy_paper_i_-*international_issues___compliance_challenges__21_oct_2022*.pdf
9. https://5rightsfoundation.com/wp-content/uploads/2024/08/Approaches-to-Childrens-Data-Protection-.pdf
10. https://www.ey.com/en_in/insights/cybersecurity/transforming-data-privacy-digital-personal-data-protection-rules-2025
11. https://www.termsfeed.com/blog/child-privacy-laws/
12. https://www.unicef.org/protection/keeping-children-safe-online
13. https://eurodigwiki.org/wiki/The_Age_Verification_Dilemma:*Balancing_child_protection_and_digital_access_rights*%E2%80%93_MT_05_2025

