Himachal Pradesh National Law University, Shimla (India)
HPNLU JOURNAL OF LAW, BUSINESS AND ECONOMICS (HPNLU JLBE)

JOURNAL ARTICLES *ISSN: 2584-0436* **HPNLU JLBE**

Volume III (2024)

PROTECTING CHILDREN'S PRIVACY IN THE DIGITAL AGE: BALANCING LEGAL FRAMEWORKS, PARENTAL CONSENT, AND ONLINE COMMERCE

Prathma Sharma

CONTENTS

Essay & Comments

PROTECTING CHILDREN'S PRIVACY IN THE DIGITAL AGE: BALANCING LEGAL FRAMEWORKS, PARENTAL CONSENT, AND ONLINE COMMERCE

Prathma Sharma*

Abstract

Emphasising the legal systems and regulations controlling the acquisition, use, and distribution of children's data, this paper investigates the evolving dynamics of children's privacy in the digital age. Emphasising the challenges in balancing the protection of children's rights with the demands of online commerce, this study investigates the consequences of international legal frameworks, including the EU General Data Protection Regulation (GDPR) and the Children's Online Privacy Protection Act (COPPA) in the United States, as well as various national legislation. Particular focus is given to nuances of parental consent, the definition of the age criterion for agreement, and the growing concerns about online behavioural advertising targeted at minors.

Emphasising parental assent and the age of majority, the growing legislative frameworks—best shown by the Digital Personal Data Protection Act in India—recognises the need for flexibility in the treatment of children's data. Particularly in relation to age limitations and content moderation, this study systematically examines the complex balance between protecting children's rights and enabling safe digital engagement.

The paper discusses the need for openness, privacy by design, and data protection impact assessments in the safeguarding of the personal data of children. It supports a more complex and flexible approach for data protection that considers children's evolving cognitive and developmental capacities as well as their rights to privacy and freedom of expression against too much intrusion. Emphasising their practical relevance and the impact of future technologies on children's online experiences, it finally assesses the effectiveness of present regulatory systems in providing adequate protection.

Keywords: *Children's privacy, data protection, GDPR, COPPA, parental consent, online advertising, privacy by design, legal frameworks.*

Introduction

Approved by the 30th International Conference of Data Protection and Privacy Commissioners on October 17, 2008, the Strasbourg Resolution addresses concerns regarding the massive gathering of personal data from minors in digital environments. Particularly in relation to micro-targeting and behavioural advertising, the Commissioners underlined the need for regulations limiting the acquisition, use, and distribution of personal data for children.[1] To help children understand and consent to data harvesting, they also urged companies to create succinct and straightforward privacy policies and user agreements.[2] They also supported the development of educational tools to help children safely navigate the internet and protect their privacy. The Resolution underlines three main reasons why children's internet privacy calls for special attention. Given their age and inexperience, children are more vulnerable than adults.[3] They often lack the tools or technological knowledge needed to handle the privacy risks connected to online behaviour, including photo sharing, messaging, and blogging. Second, digital footprints left by children can be more negative than those of adults. Children's immaturity makes them more prone to make mistakes online, which leads to lifelong records that could later cause shame or difficulty rectifying as they grow. Protecting the privacy of children, means stopping the production of negative or permanent digital content that might damage their security, dignity, or privacy.[4] Third, the United Nations Convention on the Rights of the Child (CRC) defines children's right to privacy by mandating that governments respect and protect these rights.[5]

The CRC is important since it imposes clear responsibilities for governments over children's rights.[6] The CRC emphasises the need for increased care and attention for children since it recognises their particular position within the larger framework of human rights laws protecting personal privacy.[7] The basic concept

---

* Ph.D. Scholar, Himachal Pradesh National Law University, Shimla.

[1] 30th International Conference of Data Protection and Privacy Commissioners, *Resolution on Children's Online Privacy*, STRASBOURG (Oct. 17, 2008).

[2] *Id.*

[3] *Id.*

[4] *How's Life for Children in the Digital Age?: The Impact of Digital Activities on Children's Lives*, OECD (May 15, 2025) available at *https://www.oecd.org/en/publications/how-s-life-for-children-in-the-digital-age_0854b900-en/full-report/the-impact-of-digital-activities-on-children-s-lives_4df70664.html (last visited 15 May, 2025).*

[5] *Convention on the Rights of the Child*, U.N. Treaty Series, 1577, art. 5 (Nov. 20, 1989).

[6] *Id.*

[7] Convention on the Rights of the Child, adopted and opened for signature, ratification and accession by UNGA Res 44/25 (20 November 1989), entered into force 2 September 1990.

guiding laws affecting minors should be the "best interests of the child." Legislators have to ensure that every rule advances the welfare of children. The "3 Ps"—provision, protection, and participation—regulates children's rights under the CRC. These covers ensure a suitable media environment, protecting children from inappropriate internet activities and making sure they can make decisions influencing their own lives.[8] Still, children's growing maturity calls for parents to play an important role in guiding their decision-making process.[9] This paper looks at how certain countries have addressed children's privacy concerns. At first, the book looks at the rise of children's privacy as a major concern for Americans, particularly with the Children's Online Privacy Protection Act (COPPA).[10] The paper compares the American approach with that of Canada and Australia, where general data protection policies have been applied to protect children's privacy. The study looks at how Europe's commitment to privacy as a basic human and children's right has affected both current and new legislation, most famously the General Data Protection Regulation (GDPR), which ranges from broad privacy protections to targeted rules for children.

The Creation of Children's Online Privacy as A Trade Issue: A Comparative Study

USA, Australia & Canada

Although both governmental and commercial institutions were compiling personal information about minors, there was no clear reference to children's privacy in the 1970s when data protection laws were first passed in Europe and North America. Children's medical visits and school attendance, for instance, produced comprehensive records that followed them throughout their lives.[11] Collected demographic data on children's tastes in toys, games, and fashion, including warranty registration cards and magazine subscriptions, to inform marketing plans.[12] Children and their parents eventually have access to data kept by public sector companies, particularly in the domains of health and education.[13] Generally, it was assumed that national general data protection laws would

[8] CRC, supra note 5, arts. 17, 31.
[9] CRC, supra note 5, Preamble.
[10] *Id.* art. 3(1).
[11] Dr shashank misra, *Protecting Children's Privacy In The Digital Age: Balancing Legal Frameworks, Parental Consent, And Online Commerce,* XII IJCRT(2025).
[12] *Id.*
[13] Dr. Carolyn Johnston, *Sharing of childr Sharing of children's health data b s health data by health pr y health professionals and essionals and parents – a consideration of legal duties,* XVI IJLT (2020).

control the growing market for children's information.[14] The scene was transformed when the World Wide Web first emerged in the 1990s, as websites started creating online environments specifically targeted at luring children and encouraging them to provide personal information for profit.[15] Acting under the Children's Online Privacy Protection Act (COPPA) in 1998, the United States was the first jurisdiction to recognise this as a separate privacy issue.[16]

Legislation aimed at safeguarding children's privacy, COPPA mandates parental permission before the gathering, use, or disclosure of personal information from anyone under the age of 13. Like consumer protection laws, it functions as a business regulator under control by the Federal Trade Commission (FTC).[17] COPPA requires that owners of websites and other online services—including linked toys and mobile apps—distribute privacy notifications to let parents and children know of data collecting practices.[18] Parental permission for the gathering, use, and distribution of personal data is necessary for these services. Moreover, parents have the right to examine the data of their children; so, services have to uphold the integrity, confidentiality, and security of the acquired data. To give parents control over the personal data gathered from their children online, COPPA stresses parental rights over those of the children.[19] COPPA includes thorough, risk-based requirements for obtaining parental permission. Services using children's data for internal purposes could employ a simpler permission process, such as an email to the parent followed by a confirmation step, sometimes called the "Email plus" method.[20] Services that let minors publicly reveal information, engage in behavioural advertising, or distribute

---

[14] United States Electronic Code of Federal Regulations, Title 16, Chapter 1, Subchapter C, Part 312, § 6502(b)(1)(A).

[15] *Id.* § 312.5.

[16] *Id.* § 6502(b)(1)(B).

[17] *Id.* § 6502(b)(1)(D).

[18] Fed. Trade Comm'n, *Complying with COPPA: Frequently Asked Questions* (Mar. 20, 2015), available at https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions (last visited Jan. 10, 2019).

[19] Fed. Trade Comm'n, *Imperium, LLC Proposed Verifiable Parental Consent Method Application* (FTC Matter No. P135419) (Dec. 23, 2013), available at https://www.ftc.gov/sites/default/files/attachments/press-releases/ftc-grants-approval-new-coppa-verifiable-parental-consent-method/131223imperiumcoppa-app.pdf (last visited Jan. 10, 2019).

[20] Fed. Trade Comm'n, "*Commission Letter Approving Application Filed by Jest8 Limited (Trading As Riyo) For Approval of A Proposed Verifiable Parental Consent Method Under the Children's Online Privacy Protection Rule* (Nov. 19, 2015), available at https://www.ftc.gov/public-statements/2015/11/commission-letter-approving-application-filed-jest8-limited-trading-"riyo (last visited Jan. 10, 2019).

personal data to other parties must follow stricter consent procedures. These could call for parents to send consent documentation by fax, email, mail, credit card number, or identification using official documentation or video conference.[21]

Third-party verification services could be used to maximise the process by lowering the volume of personally handled directly by the service provider.[22] Several strategies have been proposed, including facial recognition technology to verify that a consenting person is the child's parent and knowledge-based authentication, where users answer questions depending on "out-of-wallet" information.[23] Industry standards of behaviour could specify how one gets parental permission.[24] COPPA has affected policies worldwide, mostly because of the great popularity of American websites among children all over.[25] Many services targeted at children have adopted the age-based COPPA model, which requires parental consent only for those under 13, even in areas without age-specific laws. Data security policies in many other countries have been shaped by the corporate interests driving COPPA.[26] Australia and Canada are shining examples of how non-American countries have handled similar problems. Both countries have thorough personal data protection laws combining federal, state, provincial, and territorial limitations. Initially, data protection laws from the 1980s controlled public sector data harvesting in Canada.[27] Until after the 1995 changes to EU laws, which restricted cross-border data flows to countries without sufficient data protection, Canada concentrated on private sector data protection. Private sector legislation was seen as an economic necessity to boost consumer confidence in the growing information economy.[28] The main federal law in Canada controlling the compilation of personal data by private sector companies is the Personal Information and Protection of Electronic Documents Act

---

[21] COPPA, Art. 40(2)(g).

[22] Tonya Rooney & Emmeline Taylor, *Surveillance Futures: Social and Ethical Implications of New Technologies of and Children and Young People*, ROUTLEDGE (2016).

[23] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31-50.

[24] *Building Canada's Information Economy and Society: The Protection of Personal Information,* INDUSTRY CANADA & DEPARTMENT OF JUSTICE (White Paper, C (2nd series), 1998)."

[25] Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5.

[26] Federal Trade Commission, *Children's Online Privacy Protection Rule,* COPPA, available at https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa. (last visited December, 2024).

[27] Dr shashank misra, *Protecting Children's Privacy In The Digital Age: Balancing Legal Frameworks, Parental Consent, And Online Commerce,* XII IJCRT(2025).

[28] Privacy Commissioner of Canada Investigation, *Report of Findings into the Complaint Filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) Against Facebook Inc. Under the Personal Information Protection and Electronic Documents Act*, PIPEDA (2009-008).

(PIPEDA).[29] It applies everywhere unless a province or territory passes similar laws. Through the Australian Privacy Principles, the Federal Privacy Act 1988 controls public and private sectors, including credit reporting agencies in Australia.

Still, neither of these models addresses minors as data subjects nor sets an age at which they can consent to have their data processed. Children lack the legal capacity to make decisions about their personal information until they reach adulthood or are recognised as mature minors, which complicates enforcement. Establishing an unofficial standard, the Children's Online Privacy Protection Act (COPPA) in the United States requires most services aimed at minors under 13 years of age to gain parental clearance. Privacy commissioners from Australia and Canada have aggressively tackled concerns related to children.[30] The Strasbourg Resolution was developed in great part by the Canadian Commissioner, and their rulings in the 2009 Facebook case and the 2013 Nexopia case were vital in applying broad data protection standards to limit the gathering of personal information on social networking sites. Similarly, addressing children's privacy issues, the Australian Commissioner has provided clear recommendations on how to control children's authorisation and has used legislative actions. Following the passage of COPPA in the United States, the debate over children's privacy in Australia started earnestly with the Privacy Amendment (Private Sector) Act in 2000. Introduced but rejected was a proposal to require parental permission for the gathering of personal data from minors under 13.[31] In 2001, a group on children's privacy was formed, yet it lacked clear results. Reviewing the Privacy Act 1988 years later, the Australian Law Reform Commission (ALRC) recommended changes to strengthen children's and adolescents' safety.[32] The ALRC suggested a consent model whereby individual evaluation would be combined with a presumption that those 15 years of age and above possessed the capacity to make decisions.[33] They understood that evaluating every child individually—especially in online environments—may not always be feasible or practical.[34] As such, they recommended a broad assumption that those 15 years of age and above possessed the capacity to assent, unless there are specific grounds to doubt their understanding.[35] Later on, this model was included in the non-

[29] Privacy Commissioner of Canada Investigation, *Social Networking Site for Youth, Nexopia, Breached Canadian Privacy Law*, PIPEDA Report of Findings (2012).
[30] D. Williams , *First Meeting of Consultative Group on Children's Privacy*, I ALRC 2254 (2001).
[31] *Australian Privacy Law and Practice,* III ALRC (2008).
[32] Office of the Australian Information Commissioner, *Australian Privacy Principles Guidelines: Privacy Act 1988*, ALRC 12-13 (2015).
[33] *Id.*
[34] *Id.*
[35] *Id.*

binding recommendations of the Australian Commissioner, which advises companies to assess every situation to determine whether parental or guardian permission is needed or if a child can consent.

The European Union: The Human Rights Approach

Strong protections for privacy as a fundamental human right have moulded EU privacy laws. Many EU policy documents highlight the increasing attention paid to children's rights, particularly in the digital sphere. The Charter of Fundamental Rights especially expresses the EU's will to protect children's rights. Originally universal, privacy rules have evolved to recognise the unique circumstances of children's online privacy both inside the EU and globally. Differentiating the treatment of children and adults regarding data privacy has both normative and pragmatic reasons. From a normative standpoint, it is necessary to protect children's rights—more especially, their best interests—while preventing conflicts between the rights of adults and children using developing capacities and involvement.[36] Children come across increased online hazards according to empirical research because of complex data collection techniques and their natural vulnerability as online users.[37] Studies in social science have revealed that children—especially teenagers—show more inclination for risk-taking and impulsive behaviour, which could compromise their ability for autonomous long-term decision-making. Researchers have linked children's developmental needs—including identity building and autonomy—with their internet behaviour and privacy decisions. Online data-collecting techniques, therefore, often take advantage of these shortcomings, which causes concerns among academics and legislators both.[38] Unlike adults, these elements make youngsters more susceptible to internet damage, including victimisation and financial exploitation of their data. Children under the EU's general data protection rules of Directive 95/46/EC have been included since 1995, classed as a homogeneous group of data subjects with adults.[39] Regardless of age or

[36] Kirsty Hughes, *The Child's Right to Privacy and Article 8 European Convention on Human Rights*, in Michael Freeman (ed.), *Current Legal Issues: Law and Childhood Studies*, XIV OXFORD UNIVERSITY PRESS (2012).

[37] Cheryl B. Preston & Brandon T. Crowther, *Legal Osmosis: The Role of Brain Science in Protecting Adolescents*, HOFSTRA L. REV. 447 (2014).

[38] Livingstone, S., Stoilova, M., Nandagiri, R., *Children's data and privacy online: Growing up in a digital age*, LSEPS (2019), available at https://eprints.lse.ac.uk/101283/1/Livingstone_childrens_data_and_privacy_online_evidence_review_published.pdf (Last visited 15 Feb 2025).

[39] European Union Agency for Fundamental Rights and Council of Europe, *Handbook on European Law Relating to the Rights of the Child* (2022) available at:

nationality, this directive seeks to protect every person whose data is handled inside the EU.[40] Lack of clear legal guidelines on children's data across the EU has resulted in different state laws, therefore creating an inconsistent regulatory environment.[41]

For children's permission regarding personal data processing, some EU countries—including Hungary, the Netherlands, and Spain—have set clear age limits. Except for vital information like the child's identification and address, which is required for getting parental authorisation, Spain's Personal Data Protection Law restricts the gathering of data of minors' family members without approval.[42] Contract law clauses have been used by other countries to determine whether kids can make decisions about their data.[43] In certain cases, children might consent to fundamental data processing operations if they can independently engage in basic legal actions free from parental approval.[44]

Most EU nations evaluate the matter separately, considering factors like the child's best interests, maturity, understanding of the consequences of consent, and the type of data involved.[45] The UK Information Commissioner's Office (ICO) says a child's competence to consent to data processing should determine comprehension rather than age.[46] Parental permission is required for children under twelve in the UK when services target them. Parental permission is needed in Belgium when a child cannot understand the consequences of consenting to data processing, particularly in circumstances involving sensitive data or when the processing does not benefit the child.[47] Many nations have lately granted special rights to children and their parents so that they may access and erase

---

https://fra.europa.eu/en/publication/2022/handbook-european-law-child-rights. (last visited on December, 2024).

[40] *Id*.

[41] European Commission, *Data Protection Rules as a Trust-Enabler in the EU and Beyond – Taking Stock*, 14 COM (2019).

[42] European Parliamentary Research Service, *Protecting children online Selected EU national and regional laws and initiatives*, EPRS, European Parliament (2025) available at https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/769570/EPRS_BRI(2025)769570_EN.pdf. (last visited on Feb. 15 2025).

[43] Baker McKenzie, *Global Privacy and Information Management Handbook,* IAPP (2017).

[44] Article 29 Working Party, *Opinion 2/2009 on the Protection of Children's Personal Data (General Guidelines and the Special Case of Schools)*, WP 160 (Feb. 11, 2009).

[45] Milda Macenaite and Eleni Kosta, *Consent for processing children's personal data in the EU:following in US footsteps?*, 26 ROUTLEDGE 146 (2017).

[46] Belgian Privacy Commission, *Advice No. 38/2002 of 16 September 2002 Concerning the Protection of the Private Life of Minors on the Internet* (2002).

[47] *Id.*

personal information.[48] Establishing the presumption that those aged 12 or above have the maturity to understand and exercise their rights, the UK Data Protection Act created policies to preserve data protection rights in Scotland. France granted kids the "right to be forgotten" in 2016, so they may quickly delete their personal information on the internet.[49] Moreover, minors 15 years of age and above in France can use their rights of access, rectification, and objection; they may also choose to prevent their parents from being informed or accessing their personal information.[50] Declaring that the child's right to privacy trumps freedom of expression and press freedom, some countries have put policies in place to protect children's data in non-criminal judicial processes and media reporting.

The different national approaches to children's data protection within the EU led to uncertainty on the application of relevant laws. Services compiling children's data regularly ran against legal uncertainty and had to coordinate several legal systems.[51] Among European privacy experts, the subject of the age at which minors might agree to data processing has been dubbed "the million-euro question".[52] Non-binding rules published by several data protection agencies have helped to somewhat offset the lack of clear data protection laws for minors in many EU countries.[53] These rules comprise comprehensive recommendations for protecting children's online privacy. Moreover, particular authorities have sent parents and children booklets, articles, and websites. Comprising representatives from all EU data protection agencies, the Article 29 Working Party, an advisory body, published a view on children's data, particularly with relation to educational institutions.[54] Using ideas from the Convention on the Rights of the Child (CRC), including the child's best interest, protection, care, participation, and emerging maturity, within the framework of data protection,

---

[48] UK Data Protection Act 1998, § 66.

[49] Cansu Caglar, *Children's Right to Privacy and Data Protection: Does the Article on Conditions Applicable to Child's Consent Under the GDPR Tackle the Challenges of the Digital Era or Create Further Confusion?*, XII EJLT (2021).

[50] *Id.*

[51] Italian Data Protection Code (Legislative Decree No. 196 of 30 June 2003) §§ 50, 52.5; Code of Practice Concerning the Processing of Personal Data in the Exercise of Journalistic Activities, [1998] O.J. 179, § 7.

[52] Giovanni Buttarelli, *The Children Faced with the Information Society* (Speech, 1st Euro-Ibero American Data Protection Seminar 'On Protection of Minors', Data Protection, CARTAGENA DE INDIAS (May 26, 2009).

[53] Belgian Privacy Commission, *Advice No. 38/2002 of 16 September 2002 Concerning the Protection of the Private Life of Minors on the Internet*; Dutch Data Protection Authority, Guidelines for the Publication of Personal Data on the Internet (2007).

[54] Article 29 Working Party, *Opinion 2/2009 on the Protection of Children's Personal Data (General Guidelines and the Special Case of Schools)*, WP 160 (Feb. 11, 2009).

this point of view highlighted a child rights perspective.[55] The Working Party looked at how the field of education may benefit from general data protection concepts—that is, data quality, fairness, validity, proportionality, and data subject rights.[56] The Working Party took a flexible approach to consent, suggesting that, instead of enforcing strict age limits for parental permission, the child's maturity and the complexity of data processing be assessed.[57] Children's data need more strict protection and care than that of adults, the Working Party underlined.

The European Union General Data Protection Law

The EU General Data Protection Regulation (GDPR) has made significant changes, particularly to meet the needs of minors as data subjects.[58] It especially acknowledges that, especially in online situations, kids need more protection than adults since they might not fully understand the dangers, consequences, and protections connected with the handling of their data (Recital 38). For children, the GDPR creates a two-layered protection system. The first tier consists of generic GDPR rules relevant to children's online behaviour, including the right to erasure, data portability, data protection by design and by default, and data protection impact assessments.[59] The second tier comprises particular rules for children, including restrictions on marketing and profiling, most famously the ban on automated decisions that significantly affect children (Article 8), and the need for parental agreement (Article 8).[60] Under the GDPR, the most important—though controversial—requirement is the parental permission duty. Article 8(1) GDPR permits personal data collecting and processing for minors under 16 only with parental permission or agreement.[61] The law lets EU Member States lower the age of consent to 13, therefore creating different national age regulations. This independence has led to differences inside the EU, which challenge companies providing cross-border services and compromise the expected GDPR harmonisation.[62] Article 8 has not been implemented consistently and lacks empirical support. First attempts to follow US norms, including COPPA, ran

[55] *Id*.
[56] *Id.*
[57] *Id.*
[58] General Data Protection Regulation, 2016 O.J. (L 119) 1–88.
[59] Milda Mačėnaitė & Eleni Kosta, *Consent of Minors to Their Online Personal Data Processing in the EU: Following in US Footsteps?*, 26(2) INFO. & COMM. TECH. L. 146 (2017).
[60] Sherif Badawy, *Social Media Terms and Conditions and Informed Consent From Children: Ethical Analysis*, JMIR (2021).
[61] General Data Protection Regulation, 2016, Art. 8.
[62] Article 29 Working Party, *Guidelines on Consent under Regulation 2016/679*, WP 259, 25 (Apr. 10, 2018).

against challenges, and various age restrictions were recommended without any justification. Furthermore, the EU missed a chance to improve child protection in relevant legislation, such as the proposed ePrivacy Regulation, which did not distinguish between adults and children as data subjects nor handle the particular consent requirements for minors.[63]

Although the GDPR establishes a benchmark for the protection of children's data both inside and outside of Europe, certain of its provisions—especially Article 8—need more explanation to ensure effective application.[64] Whether some online services—including those provided by non-profits or those with major offline components—qualify as information society services and hence call for parental consent requirements is debatable.[65] Moreover, services meant for adults yet used by children still generate questions about their GDPR compliance.[66] Whether a service targets children will depend on factors like content, the usage of animated characters, and advertising; legal precedents could help to clarify this point.[67] While the Article 29 Working Party has argued for a reasonable approach to consent gathering, consistent with the idea of data minimisation, the GDPR lacks particular means for obtaining or validating parental assent.[68] The working group notes that, in low-risk circumstances, a simple email confirming parental permission could be sufficient.[69] Still, in high-risk situations, more thorough verification could be needed. The working party emphasises that the degree of verification should match the risks related to the data processing engaged in. Moreover, the GDPR suggests indirectly, in some cases, even though it does not specifically demand age verification. Should a kid consent without meeting the age requirements, data processing is considered illegal. Controllers are obliged to use reasonable steps to determine the age of the child; these steps are appropriate for the type and hazards related to the processing. Should a child say they are under the age of consent, controllers must obtain parental permission, therefore confirming that the person providing consent is either a parent or legal guardian. The verification technique cannot involve pointless data processing. Recital 30 of the GDPR specifies a special exception to the parental consent mandate in some instances, including directly offered preventive or counselling services to

---

[63] *Id.*

[64] *Id at 61.*

[65] *Id.*

[66] Stanislaw Piasecki, *Complying with the GDPR when vulnerable people use smart devices*, XII IDPL 113 (2022).

[67] Sabrina Neeley, *Using animated spokes-characters in advertising to young children - Does increasing attention to advertising necessarily lead to product preference?*, JOA (2004).

[68] Dr shashank misra, *Protecting Children's Privacy In The Digital Age: Balancing Legal Frameworks, Parental Consent, And Online Commerce*, XII IJCRT (2025).

[69] *Id.*

minors.[70] This exemption is based on the idea that minors could need access to particular services for their welfare and that requiring parental permission could prevent that access. Online helplines for victims of sexual abuse might provide treatment without involving parents since parental involvement may worsen these circumstances.

Children, Consent, and Data Protection: The DPDP Act, 2023

The DPDP Act's[71] goal is to legally acknowledge, in line with accompanying constitutional rulings and the Supreme Court of India's established right to privacy, legally.[72] Under this recognised right, one has personal autonomy via which they may regulate their information. Under this approach, the main operator works through consent-based procedures. The present state of affairs raises several important questions around kid categorisation, approval rights for data collecting and permissible data usage limits. The issues highlighted need to be addressed if we are to ascertain the course children will follow to become India's "*Digital Nagariks*" (Digital Citizens). Published for public consultation in November 2022, the Draft Digital Personal Data Protection Bill of 2022[73] Defines the majority age as 18 years old.[74] The Bill outlines several illegal activities.[75] And lays severe guidelines on how personal data can be acquired and handled. Review of the 20,000 public comments, along with multiple conversations, revealed that this data processing method required both changes and corrections.[76] Providing goods and services to young people in the new digital economy has become essential since it meets their particular demands, independent of content type. While providing information appropriate for their age range, the protection of children's privacy and data security takes front stage.

Age verification combined with adult content filtering and mental health service delivery needs particular protection measures since these purposes demand secure data handling practices. Children between 0 and 18 are classified as minors with limited stated limitations under Indian law since 1875[77]. Since minors under the law lack competence to sign contracts, most agreements need

---

[70] Joseph Savirimuthu, *Datafication as parenthesis: reconceptualising the best interests of the child principle in data protection law*, 34 IRLCT 310 (2017).
[71] The Digital Personal Data Protection Act, 2023 ("Act").
[72] *Justice K. S. Puttaswamy v. Union of India*, (2017) 10 SCC 1 (India).
[73] The Digital Personal Data Protection Bill, 2022 ("Draft"), available here https://prsindia.org/billtrack/draft-the-digital-personal-data-protection-bill-2022.
[74] *Id* at Section 2(3).
[75] *Id* at S. 10.
[76] *National Strategy for Artificial Intelligence,* NITI Aayog, Government of India (2023).
[77] The Indian Majority Act, 1875, S. 3.

consent from their parents or guardians.[78] The exclusive reliance on parental consent or consent from a single source cannot sufficiently explain the presence of minor users on online programs due to the allowed specific exceptions, which favour the child.[79] The Act and Draft[80] especially identify children between the ages of 0 and 18.[81] The structure is based on ideas established by GDPR and CCPA[82], so defining adaptable degrees of data security guidelines.[83] According to the Draft rules[84], the Act calls for parental consent before handling any personal data.[85] While the suitable laws specify the procedures to be followed for verification, a validation process has to confirm the permission. The Act mandates guardians of all children under their control—including those with disabilities—confirm consent for them.[86] The Act gives the government power to approve exemptions allowing for the processing of personal data for children. Depending on set criteria, specific coverages from exclusions apply to some Data Fiduciaries[87] and specific objectives (the "*Class Exemption*").[88] The act allows a Data Fiduciary to get parental permission by demonstrating security within their data handling procedures (the "*safety dilution*").[89] The adjustment seeks to strike a compromise between modern service operational needs and children's data protection.

Like the Draft[90], the Act notes parents and legal guardians as "*data principals*" for their children.[91] Usually, processing personal data of a minor requires parental permission.[92] Particularly when parents and children disagree over permission, the application of Data Principal rights, or the resolution of grievances, the possibility of totally substituting a child's autonomy with that of the parent creates great challenges. Though the new phrase lets a child exercise their rights in tandem with their parent, the broad definition of "*processing*"[93] and the clear directive for "*verifiable parental agreement*" could cause Data Fiduciaries to turn

[78] The Indian Contract Act, 1872, S.11.
[79] Partnership Act, 1932, S. 30.
[80] *Supra* note at 73, S. 2(3)/
[81] *Supra* note of 73, S. 2(f).
[82] California Consumer Privacy Act, 2018. Cal. Civ. Code §§ 1798.120 (West 2018).
[83] Singapore Personal Data Protection Act, 2012.
[84] *Supra* note at 73, S.10(1), Draft.
[85] Digital Personal Data Protection act, *2023*, S.2(t).
[86] *Id* at 85 Section 9(1)
[87] *Supra* note at 85, S. 2(i).
[88] *Supra* note at 85, S. 9(4).
[89] *Supra* note at 85, S. 9(5).
[90] *Supra* note at 85, S. 2(6).
[91] *Supra* note at 85, S. 2(j).
[92] *Id* at 61.
[93] Supra note at 85, S.2(x).

down such requests.[94] Moreover, by following the age of majority, the Act ignores the child's capacity for judgment—a consideration taken into account in present Indian penal law.[95] This leads one to investigate, if any, minors' rights regarding their personal information outside of parental control. Whether by rulemaking, Data Protection Board (DPB) rulings, or often asked questions, clarity on this issue would be much appreciated. With harm defined as bodily injury, identity theft, harassment, obstruction of approved benefits, or infliction of significant loss, the Draft proposed that Data Fiduciaries be forbidden from processing personal data in a manner that could jeopardise a child.[96] The Act has deleted the concept of "*damage*,"[97] and Data Fiduciaries are now forbidden from any handling that might compromise the welfare of a kid.[98] Data fiduciaries have to act in a fiduciary capacity, aggressively thinking through any negative consequences their data processing could cause for children. The Act also imposes restrictions on "*tracking or behavioural monitoring of minors*" and "*targeted advertising aimed at minors*," just like the Draft does. These rules might also cover techniques like age gating and content screening, which ensure that advertising and content are appropriate for children, even if the meanings of these terms remain very unclear.

Unlike the Draft[99], the Act[100] Let's Class Exemption and Safety Dilution apply on the restrictions on data processing for minors.[101] This adaptability allows exemptions for protective measures, including age gating and sophisticated age verification, therefore guaranteeing the ongoing availability of age-appropriate content and services, including educational and entertainment resources for teenagers. Together with the bans on tracking, behavioural monitoring, and profiling, the rules specified in the Act will be crucial in defining the specific categories of Data Fiduciaries and the settings in which the criteria for getting verifiable consent are inapplicable. Like the Draft, the Act keeps the punishment for violating extra responsibility with children's data at two hundred crore rupees.[102] This punishment highlights the need for explicit, specific delegated law, which is necessary to give businesses certainty regarding compliance and legislative intent in the management of personal data of children. The Act's clauses particularly benefit businesses targeted at this demographic and

[94] Supra note at 85, S. 9(1).
[95] Indian Penal Code, 1860, S. 82.
[96] *Supra* note at 73, S. 10(2).
[97] *Supra* note at 73, S. 2(10).
[98] Supra Note at 85, S. 9(2).
[99] Supra note at 73, S. 10(3).
[100] *Supra* note at 85, S. 9(3).
[101] Supra note at 85, S. 9(4), 9(5).
[102] Supra note at 85 Entry 3.

industries serving children since they allow them to engage with children in a way that is both safe and safeguarding of their interests. Along with the potential of a lowered age threshold for parental assent in some cases, the exemption of specific data processing activities gives companies a more defined strategy to correctly handle children's data while preserving their welfare.

A Critique of the Legal Framework

The privacy of children necessitates specific protection, both in the digital domain and the physical environment. A digital trail made by children begins before birth, yet continues until their death. Digital services demand personal information sharing from children, though they typically do not grasp how such data sharing entails potential risks or the theoretical concepts involved. The Hon'ble Apex Court emphasised this matter correctly when it declared privacy as an essential human right in "*K.S. Puttaswamy*." The rapidly developing digital world makes children's personal data protection a key issue for this generation. Children's rising involvement with online services has triggered multiple data collection events, which lead to privacy concerns because appropriate safety measures have not been established. The Digital Personal Data Protection (DPDP) Act, 2023 of India, creates a complete regulatory structure that safeguards personal data at all stages, including data belonging to minors. Records of children receive special handling because they face privacy risks more intensely than adults under the Digital Personal Data Protection (DPDP) Act framework. An initial explanation of both the "*children's personal data*" definition and its included information types must precede examining the law's child-related specifications. The Digital Personal Data Protection Act, 2023, through its Section 2(f), defines children as all persons who remain younger than 18 years old. The category of Children's Personal Data includes all data about children that allows identification through direct methods or alternative means. The set of identifying information includes name, residence data, date of birth and biometrics, as well as school reports and distinct pieces of information which can either directly or indirectly identify a child or shed light on their activities. Online activities pursued by children produce a wide variety of data because their activities cover a full spectrum of options.

The three central elements under the DPDP Act for understanding data duration rules are Data Principal, Data Fiduciary, and Data Processor. These three entities collectively provide critical support in maintaining proper lawfulness for child personal data management. A person who owns personal data falls under the category of Data Principal. Under minors' regulations, the child functions as the individual responsible for data purposes. Since children lack a proper understanding of data privacy protection, they need a Data Principal who

functions as their legal representative, such as parents or guardians. When a child joins an e-learning platform, their parent usually provides basic information about the child, alongside consent to allow data collection. A Data Fiduciary refers to an entity that stands as a business or organisation that creates aims and methods for handling personal data processing. Data Fiduciaries maintain legal responsibility to handle all processes of personal data collection and storage, and processing activities. The company operating a social networking platform serves as the Data Fiduciary during instances when young users interact with the application. Alternatively, there exists a Data entity that guarantees that all data stays confined to its designated purpose while also obtaining parental consent. The Data Fiduciary authorises people or businesses to act as Data Processors for personal data tasks. The database administration for children's data passing to a third-party service provider makes the supplier become the Data Processor. In data processing endeavours, the Data Processor operates under the directives given by the Data Fiduciary.

According to the National Commission for Protection of Child Rights (2021), a substantial 30.2% of children aged 8 to 18 used smartphones or electronic devices for their virtual educational needs.[103] These platforms collect detailed personal information, including academic records, together with personal details, which creates concerns about storing and sharing this information. Social media and gaming systems provide attractive features to young users who might not fully grasp the online consequences of information sharing. Google and Facebook receive most of the data obtained from children's applications, according to research findings, although Google takes in the highest proportion.[104] Studies revealed that eighty-five per cent of assessed applications accessed sensitive personal information without required consent, thereby endangering the privacy of children to a great extent. E-Commerce platforms serving young customers systematically collect user interaction data to justify stringent privacy safeguards in their operations. The $11 billion in advertising revenue earned by social media platforms from child and adolescent audiences prompted the need for new regulations in this field, according to the 2022 Harvard study.[105] The DPDP Act

---

[103] Isha Suri & Pallavi Bedi, *Shepherding Children in the Digital Age*, THE TIMES OF INDIA, available at https://timesofindia.indiatimes.com/blogs/voices/shepherding-children-in-the-digital-age/ (last visited Mar 14, 2025).

[104] Annapurna Roy, *Google, Facebook Skim Most Data from Apps for Kids: Study*, THE ECONOMIC TIMES, (Jan. 29, 20240, available at https://economictimes.indiatimes.com/tech/technology/google-facebook-skim-most-data-from-apps-for-kids-study/articleshow/107209705.cms?from=mdr (last visited Mar 14, 2025).

[105] Elizabeth Napolitano, *Social Media Apps Made $11 Billion from Children and Teens in 2022*, - CBS News (2023), available at https://www.cbsnews.com/news/facebook-instagram-tiktok-snapchat-children-advertising-2022-harvard-study/ (last visited Mar 14, 2025).

establishes clear rules for child data collection, processing, and storage operations. Among the principal responsibilities are:

(i.) The DPDP Act, through Section 9, requires Verifiable Parental approval before processing or collecting personal data that involves children.[106]

(ii.) Any given consent requires unconditional status and must be voluntary, together with transparency, explicit confirmation and also needs to be both informed and unequivocal.[107]

(iii.) The Act states clearly that the collected information serves only the approved purpose, but additional data acquisition requires substantial necessity.[108]

(iv.) Data Fiduciaries must protect child welfare by refraining from harmful data management tasks that violate the provisions of the Act.[109]

(v.) According to Section 9(3) of the DPDP Act, Data Fiduciaries must refrain from tracking children technically, while also refraining from conducting profiling and behavioural monitoring operations and advertising services to them.

According to data guidelines, data retention for children applies only to what is necessary to complete the specific reasons of data collection. The data destruction process becomes mandatory once the utilisation of the information stops. The Act provides several rights to Data Principals which allow them to fix personal data and request alterations or deletion, together with consent withdrawal, anytime.[110] Security Protocols require Data Fiduciaries to implement proper security and organisational processes and technical measures so they can protect data from

---

[106] Aditi Agrawal, *NCPCR Likely to Seek Clause for Parents' Consent under Data Protection Rules*, HINDUSTAN TIMES (2024), available at https://www.hindustantimes.com/india-news/ncpcr-likely-to-seek-clause-for-parents-consent-under-data-protection-rules-101724180521788.html (last visited Mar 14, 2025).

[107] Aihik Sur, *DPDP Rules: NCPCR to Recommend MeitY to Bring in KYC-Based Age Verification for Children*, MONEYCONTROL (2024), available at https://www.moneycontrol.com/technology/dpdp-rules-ncpcr-to-recommend-meity-to-bring-in-kyc-based-age-verification-for-children-article-12801563.html (last visited Mar 14, 2025).

[108] *Supra* note at 85, S. 9(2).

[109] Anuradha Gandhi & Rachita Thakur, *SAFE For Kids Act: Protecting Young Users from Harmful Social Media Feeds*, S.S. RANA & CO. (2024), available at https://ssrana.in/articles/safe-for-kids-act-law-protecting-young-users-harmful-social-media-feeds/ (last visited Mar 14, 2025).

[110] *Supra* note at 85, S. 12.

breaches and keep within data protection laws.[111] Selected violations of regulations lead to substantial monetary and administrative penalties for non-compliant organisations. Child data violations trigger monetary punishments that reach up to 200 crore rupees.[112]

Data compliance violations lead to immediate damage to an organisation's reputation and bring about loss of trust from stakeholders as well as decreased client numbers and economic decline. Organisations that fail to comply must face legal actions that cost them both court costs and possible payment of damages.[113] Privacy legislation in both European Union jurisdictions and across the entire global domain has set strict guidelines about protecting children's data through regulations such as the General Data Protection Regulation (GDPR).[114]

The video-sharing service paid 345 million euros as a penalty in 2023 due to its failure to verify parental consent properly, and Meta received 405 million euros for GDPR violations during child data protection in 2022. Microsoft faced legal charges for privacy violations related to child data collection without consent from parents during the lawsuit regarding Microsoft Chromebooks. The Danish Data Protection Authority (DPA) imposed a processing ban on Microsoft because the company failed to properly assess risks before the company could resume data operations. The DPDP Act receives anti-democratic critiques because of Draft Rule 10, as well as other provisions that trigger fundamental violations of privacy rights, even though the law was introduced to protect private rights.[115] The requirement to verify user ages poses multiple operational problems because it requires entire system-wide validation for all users, thus creating potential

---

[111] *Insufficient Legal Basis to Use Google Workspace as an Educational Tool in Schools*, INPLP (2024), available at https://inplp.com/latest-news/article/insufficient-legal-basis-to-use-google-workspace-as-an-educational-tool-in-schools/ (last visited Mar 14, 2025).

[112] Adam Satariano, *Meta Fined $400 Million for Treatment of Children's Data on Instagram*, THE NEW YORK TIMES, Sep. 5, 2022, available at https://www.nytimes.com/2022/09/05/business/meta-children-data-protection-europe.html (last visited Mar 14, 2025).

[113] Anuradha Gandhi & Isha Sharma, *TikTok's Liability: Violation of Children's Data*, S.S. RANA & CO., available at https://ssrana.in/articles/tiktoks-liability-violation-of-childrens-data/ (last visited Mar 14, 2025).

[114] Alan J, *European Center For Digital Rights Believes Microsoft Intruded On Privacy Of Schoolchildren*, (Jun. 4, 2024), available at: https://thecyberexpress.com/european-center-for-digital-rights-microsoft/ (last visited Mar 14, 2025).

[115] *Parental Consent Needed For Children To Join Social Media, Gaming Platforms : Proposal In Draft Digital Personal Protection Rules*, LIVE LAW (2025), available at: https://www.livelaw.in/top-stories/parental-consent-needed-for-children-to-join-social-media-gaming-platforms-proposal-in-draft-digital-personal-protection-rules-279950 (last visited Mar 14, 2025).

difficulties in maintaining compliance requirements. Under the DPDP Act 2023, organisations must strictly protect children's data or face substantial penalty fines. Executive teams must work closely together with governments, along with organisations and public groups, to carry out these rules properly in India and worldwide. Detailed execution requires comprehensive collaboration.

Conclusion

It gets more difficult to ensure that youngsters fully understand the mechanisms of data collecting, use, and dissemination as internet companies obtain and profit from their information. Age limits on data collection are controversial since it is impossible to assign young children the responsibility for mitigating these risks.[116] Though they try to solve this problem, parental permission rules are not the best one, especially considering the Convention on the Rights of the Child (CRC). Academics argue that since they usually give either too much protection or the demands of online commerce top priority, existing consent rules often ignore both the welfare of children and their need for autonomy. Moreover, severe demands for parental agreement could limit children's rights to freedom of expression and knowledge access.[117] Maintaining practical application, the Australian integrated strategy for kid data protection offers flexibility by considering children's cognitive development, autonomy, and involvement. This approach departs from the frameworks set forth by the Children's Online Privacy Protection Act (COPPA) in the United States and the General Data Protection Regulation (GDPR) in the European Union, which rely on a predefined age limit and neglect individual assessments of a child's capacity to consent. Practically, the European and Australian methods may produce similar outcomes. Parental permission for information society services—that is, internet services—is necessary under the GDPR when personal assessments of a child's maturity prove impractical. Though this is not particularly stated in the statute, the GDPR allows individual evaluations for offline processing of personal data. Previously, EU data protection authorities underlined the need for tailored assessments when getting consent from children; nevertheless, this approach is challenging to

[116] Article 29 Working Party, *Opinion 2/2009 on the Protection of Children's Personal Data (General Guidelines and the Special Case of Schools)*, WP 160 (Feb. 11, 2009).

[117] Anca Micheti, Jacquelyn Burkell & Valerie Steeves, *Fixing Broken Doors: Strategies for Drafting Privacy Policies Young People Can Understand*, 30(2) BULL. OF SCI. TECH. & SOC'Y 130 (2010).

enforce legally since it depends on clear guidelines and obligations for data controllers to prevent significant penalties.[118]

Many data protection models include social responsibilities on online services targeted at children to balance the needs of online commerce with children's rights. Early legislation, like COPPA, required explicit privacy rules written in understandable language to support informed permission. The GDPR also emphasises data controllers' openness, responsibility, and the need for rules of behaviour.[119] Research shows, however, that privacy policies often show too much complexity for young people to understand, which reduces compliance rates with privacy laws. Thus, including privacy by design and doing data protection impact analyses might help to enhance the protection of personal information for children.[120] We have to respect the opinions and needs of young people. Studies show that even young people who spread knowledge online nevertheless worry about their privacy. Studies reveal that people use different devices for different purposes, including texting or using ephemeral technology like Snapchat for more private discussions. On these networks, the data collection and disclosure policies reflect those of more public venues like Instagram and Twitter. This shows that even if children try to protect their privacy by limiting their intended audience, the information they provide is nonetheless obtained and used to affect their online behaviour and self-image. The capacity of current strategies to limit the collection of children's data helps one to assess their effectiveness in protecting their online privacy.[121] Examining the 50 most visited websites among Canadian children found that commercial data collecting was rather common—96% of these sites used an average of five trackers to collect user information. Although eighty per cent of websites featured privacy choices, just twelve per cent had default privacy settings set to private. This implies that authorities in data protection have to keep working to ensure that laws provide enough protection of privacy for minors.

---

[118] Simone van der Hof & Eva Lievens, *The Importance of Privacy by Design and Data Protection Impact Assessments in Strengthening Protection of Children's Personal Data Under the GDPR*, 23(1) COMM. L. 33 (2018).

[119] Matthew Johnson, Valerie Steeves, Leslie Shade & Grace Foran, *To Share or Not to Share: How Teens Make Privacy Decisions about Photos on Social Media*, MEDIASMARTS (2017).

[120] *Id.*

[121] *Supra* note 90.