Data Protection for Children

Digital Personal Data Protection Act, 2023 - Pathways towards Implementation

REPORT

PACTA
SOCIAL | IMPACT | LEGAL

SPACE 2 GROW

Foreword

There can be no keener revelation of a society's soul than the way in which it treats its children.

— Nelson Mandela

This quote stays with me not just as a reminder, but a challenge to lead work that enables and supports a just and safe environment for children. In an era where the digital world seamlessly intertwines with the lives of a new generation of "Digital Natives", the responsibility to support these children grows many fold. Globally, 1 in 3 Children access the internet with more than 175,000 children going online for the first time every day. Every time a child goes online, they tap into great opportunities, but also face grave risks. As per the Internet and Mobile Association of India, 66 million Indian children between the ages of 5 and 11 years (forming 15% of the internet users) access the internet everyday. It is in this context that we write this report.

Chitra Iyer
Co-Founder & CEO,
Space2Grow

The DPDP Act 2023 and the Draft DPDP Rules 2025 recognises digital risks to children. The Act places a spotlight on children's data and the need for verifiable parental consent (VPC) before personal data of children can be collected or processed. But VPC, by itself, is not an adequate answer for the problem of children's digital safety. Parental consent cannot replace platform responsibility, child-centric design, or systemic safeguards.

Foreword

This report takes the view that the DPDP Act takes a protective approach, but would not be effective in protecting children against the risks of emerging technologies. The scope of this report includes:

- The technical, ethical, and logistical hurdles in implementing verifiable parental consent in a country with deep digital divides, especially in terms of access and literacy.
- Approaches from global frameworks that can be used to scaffold India's approach.
- Specific recommendations for execution of VPC through a more robust and agency building approach — that is holistic in terms of safety of children, and provides ease for execution for platforms, and government.

We hope that the recommendations inform the implementation of the DPDP Rules, and build systems and processes to scaffold the legislative intent.

Acknowledgement

This report carries the effort of several people and friends of Pacta. This report was authored by K K Prahalad (Legal and Policy Associate, Pacta) and Nivedita Krishna (Founder-Director, Pacta). Anagha Sasidharan's (Senior Legal and Policy Associate, Pacta) contributions were pivotal for gathering data and reviewing drafts. Bhavitraa Thilagar (Communications Design Associate, Pacta) led the report's design. We would also like to thank Space2Grow for their collaboration on the public consultations that informed this report. The inputs provided by Chitra Iyer (Co-Founder & CEO, Space2Grow) throughout this process have been indispensable.

Suggested Citation: Data Protection for Children - Pathways towards Implementing Intentions of the DPDP Act, Pacta, Bengaluru, 2025

Pacta

Table of Contents

Introduction

By the time a child is 13, over 72 million pieces of personal data will have been captured about them.[1]

Data Protection for Children - Pathways towards Implementing Intentions of the DPDP Act

Children today spend a significant amount of time in the digital world, where they are the target of monitoring and data-generating processes,[2] and face risks to their safety.[3] The digital world raises the critical issue of simultaneous voluntary sharing of personal information online, important for children's agency, and the attendant threats to their privacy, important for their safety.[4] This simultaneous straddling of trade-offs and co-benefits of digital access necessitates legislative measures for the protection of children and their vulnerability through their data trails.

---

[1] SuperAwesome, "SuperAwesome Launches Kid-Safe Filter to Prevent Online Ads from Stealing Children's Personal Data - SuperAwesome" (SuperAwesome, July 9, 2020), available at: https://www.superawesome.com/superawesome-launches-kid-safe-filter-to-prevent-online-ads-from-stealing-childrens-personal-data/#:~:text=KSF%20ensures%20that%20every%20digital,collect%20personal%20data%20from%20children

[2] Livingstone S and others, "Children's Data and Privacy Online: Growing up in a Digital Age. An Evidence Review" (London: London School of Economics and Political Science 2019), *available at:* https://eprints.lse.ac.uk/101283/1/Livingstone_childrens_data_and_privacy_online_evidence_review_published.pdf

[3] Iyer C and others, *Digital Safety of Children: Creating Safe Online Spaces* (Digital Safety of Children), *available at:* https://www.space2grow.in/_files/ugd/fcdbc5_16ff89b38c5844f4b9dbee70f7872fce.pdf

[4] Livingstone (n 2)

Internationally, different data protection legislations have introduced different ages until which the consent of the child is not considered valid.[5] **The Indian data protection legislation, the Digital Personal Data Protection Act, 2023 (DPDPA), uses the general age of majority (18) as the cutoff beyond which a person's consent is valid.**[6] It then addresses the need to safeguard children's data and their digital activities, under Section 9, through a **three-pronged approach**:

Prong 1- Verifiable Parental Consent (VPC) mechanisms.

Prong 2 - Prohibition of behavioral monitoring and tracking of children.

Prong 3 - Ban on processing children's data that may cause "detrimental effect on the well-being of the child".[7]

Prongs 2 and 3 provide principle-based approaches to what may not be done with children's data, but Prong 1 provides a specific approach to securing consent for the processing of a child's data i.e., Verifiable Parental Consent.

In this paper, we identify the limitations of VPC (envisaged under DPDPA) in meaningfully protecting children's data and safety online. We provide recommendations of approaches that would scaffold the legislative provisions. Knowing that legislative approaches are necessary, but also insufficient in isolation, our recommendations are framed towards augmenting systemic capacity to protect children's digital personal data. We expect to delve deeper into these recommendations through a series of working papers.

---

[5] Barik S, "Age of Consent for Data Protection: How the Definition of a Child Has Changed over the Years" The Indian Express (July 17, 2023), available at: https://indianexpress.com/article/explained/explained-sci-tech/age-of-consent-data-protection-definition-of-a-child-8836943/

[6] Digital Personal Data Protection Act, 2023, Sec. 2(f)

[7] Digital Personal Data Protection Act, 2023, s. 9.

Verifiable Parental Consent and Implementation Challenges

Under the DPDPA, any Data Fiduciary seeking to process the data of a child or a person with disability, has to obtain verifiable consent of the parent or the lawful guardian.

The DPDPA follows the international trend of using consent to legitimize data processing.[8] In India, since a person below the age of 18 does not possess "legal capacity" to provide valid consent, the consent of a parent or legal guardian is substituted. On these lines, the DPDPA introduced the concept of VPC in the Indian data protection framework. Under the Act, any Data Fiduciary seeking to process the data of a child or a person with disability, has to obtain verifiable consent of the parent or the lawful guardian.[9] **The Draft DPDP Rules, released on 3rd January 2025, provide that Data Fiduciaries have to adopt "appropriate technical and organizational measures" to comply with the requirement to collect VPC.**[10]

[8] Emily Elstub, Surveillance Capitalism: The Harm To Childhood, The Insufficiency Of Parental Consent And The Consequent Impermissibility (Universiteit Utrecht, Thesis Submitted for the Degree of Master of Applied Ethics, 2022).

[9] Digital Personal Data Protection Act, 2023, Sec. 9(1).

[10] Draft Digital Personal Data Protection Rules, 2025, Rule 10.

Specific methods stipulated by The DPDP Rules to collect VPC :

- **through details of identity available with the Data Fiduciary**
- **with the consent-giver providing such details either directly or through a virtual token mapped to such details issued by an entity created by the Central or State Government.**[11]

While useful, **VPC mechanisms alone cannot adequately protect children in the digital world. At their core, they seek to transfer accountability for the child's online safety onto their parents or legal guardians, who may not have the ability, information or agency to adequately provide for the child's protection.** In the following section, we seek to analyze the various drawbacks of relying solely on VPC to protect children in the digital world:

a. Consent Fatigue

b. Digital Literacy

c. Limiting Access

d. Technical Challenges

e. Consent vs Control

[11] Draft Digital Personal Data Protection Rules, 2025, Rule 10.

a. Consent Fatigue

VPC mechanisms assume that adults are better placed than children to understand the implications of providing consent for data processing, but this is not necessarily true. Privacy policies are lengthy and complex, often intentionally kept broad and vague.[12] **Many adults, even if they are educated and digitally literate, simply do not (or cannot) read every privacy or data use policy they come across ("consent fatigue").**[13] This problem is magnified in the case of VPC, as parents will now have to read and understand privacy policies with respect to their child's data as well as their own. A Pew Research study found that 56% of Americans frequently click "agree" on privacy policies without actually reading the content, highlighting the challenge of consent fatigue.[14] Further, parents giving informed consent on behalf of their children are not always properly engaged with the process of collecting that consent. A study conducted in a rural and a semi-urban region in Andhra Pradesh saw that only 13.4% of parents actively participated in an observational tuberculosis research involving their infant children.[15] Such low amounts of participation in medical studies raises the question of how effectively parents will exercise their discretion in sharing children's data online.

---

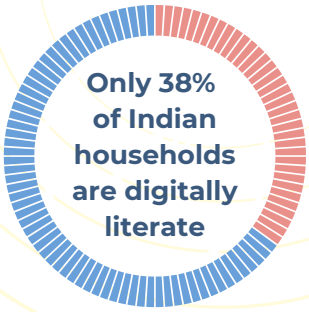
[12] Klosowski T, "Here's What You're Actually Agreeing to When You Accept a Privacy Policy" Wirecutter: Reviews for the Real World (April 14, 2023), available at: https://www.nytimes.com/wirecutter/blog/what-are-privacy-policies/

[13] McDonald AM and others, "The Cost of Reading Privacy Policies" (I/S: A Journal of Law and Policy for the Information Society and others, 2008) journal-article, available at: https://lorrie.cranor.org/pubs/readingPolicyCost-authorDraft.pdf.

[14] McClain C and others, "How Americans View Data Privacy" (Pew Research Center, October 18, 2023) <https://www.pewresearch.org/internet/2023/10/18/how-americans-view-data-privacy/>

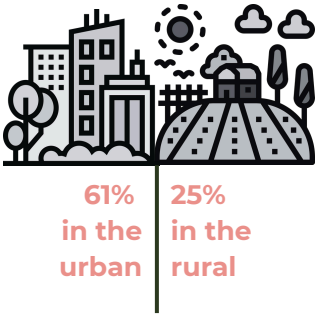
[15] Rajaraman D and others, "How Participatory Is Parental Consent in Low Literacy Rural Settings in Low Income Countries? Lessons Learned from a Community Based Study of Infants in South India" (2011) 12 BMC Medical Ethics 1

b. Digital Literacy



Younger generations consider themselves more digitally literate than their older counterparts.[16] Parents also often believe that their children are better equipped than they are to be safe online.[17] Further, Space2Grow found that while 90% of children they surveyed had faced one or the other form of digital harm or risk on digital platforms, only 14% shared this information with their parents.[18]

Divide in the digital literacy between urban and rural



With trends like these, **especially in a country like India where only 38% of households are Digitally Literate (defined as one where at least one member has the ability to operate a computer and use the Internet), with a significant divide between the urban (61%) and the rural (25%) regions,[19] it may be unfair to assume that all parents are well positioned to protect their children's data from online harm.**

---

[16] Statista, "Self-Perceived Digital Literacy among Young People ASEAN 2020, by Age" (Statista, September 18, 2024), available at: https://www.statista.com/statistics/1247974/asean-perceived-digital-literacy-of-youth-by-age/#:~:text=Self%2Dperceived%20digital%20literacy%20among%20young%20people%20ASEAN%202020%2C%20by%20age&text=A%20September%202020%20survey%20conducted,level%20than%20their%20older%20counterparts.

[17] "Briefing Paper: Children's Data Protection" (CUTS C-CIER 2022) <https://cuts-ccier.org/pdf/bp-childrens-data-protection.pdf>.

[18] Space2Grow, Virtual Threats Real Harm

[19] Digital Literacy" (Dattopant Thengadi National Board for Workers Education and Development) <https://dtnbwed.cbwe.gov.in/images/upload/Digital-Literacy_3ZNK.pdf>

c. Limiting Access

While the digital world contains many risks, it also provides children the opportunity to develop critical learning skills and the capabilities to operate independently.[20] Any barriers that restrict children's access to various online resources should be carefully considered. VPC programs, no matter how well implemented, will pose such barriers. Attempts to provide VPC may fail due to errors in submissions, including blurry government ID photos. **VPC methods that rely on credit cards or government-issued ID cards also exclude a large group of unbanked and undocumented caregivers.** Further, VPC requirements may cause concerns among guardians who are asked to provide sensitive personal or financial information, creating concerns about privacy and security. Complex VPC mechanisms may also be too time-consuming and cumbersome for guardians to complete, which can then lock children out of accessing those digital services.[21] **A related problem arises from the digital gender gap in India, where girls and women are denied access to digital technologies by 'male gatekeepers'.**[22] In such households, especially if a single device is shared between multiple children, it is likely that the introduction of cumbersome VPC mechanisms further increase the digital divide and limit women's access to the digital world.

---

[20] UNICEF, "Done Right, Internet Use among Children Can Increase Learning Opportunities and Build Digital Skills" (November 27, 2019) <https://www.unicef.org/press-releases/done-right-internet-use-among-children-can-increase-learning-opportunities-and-build>

[21] Future of Privacy Forum, "THE STATE OF PLAY: Is Verifiable Parental Consent Fit For Purpose?" (2023) <https://fpf.org/wp-content/uploads/2023/06/FPF-VPC-White-Paper-06-02-23-final2.pdf>

[22] "India Needs to Double down on Bridging Its Digital Gender Gap" (*UNFPA India*) <https://india.unfpa.org/en/news/india-needs-double-down-bridging-its-digital-gender-gap>

d. Technical Challenges

VPC compliance implies a significant burden on all stakeholders, and many Data Fiduciaries may not have the technical resources available to comply.

Data Fiduciaries are likely to face various challenges including:

1. Difficulty in distinguishing between kids and adults online (as kids can pose as adults and adults can pose as kids).
2. Difficulty in establishing a relationship between a particular child and a particular adult, and then establishing the nature of that relationship.
3. Exclusion of certain families due to parental consent mechanisms, as some parents may not have or may be reluctant to provide financial or ID information that is required for some verification mechanisms to function properly.[23]
4. Exclusion of certain children as they may not have an engaged parent or responsible adult, such as those in foster care or institutional homes; verifying parental consent is difficult. Unclear guardianship structures may exclude them from digital platforms altogether.

[23] Future of Privacy Forum (n 21)

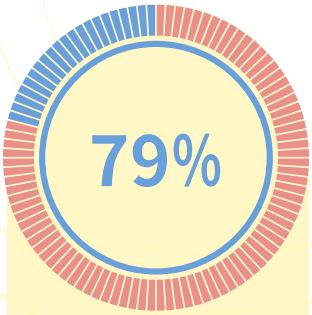
These technical challenges would result in VPC collection creating a significant cost of compliance for Data Fiduciaries. They would have to set up processes which are likely to be "time-consuming, cumbersome and costly."[24] **Estimates in the United States suggest that the costs of such processes may range from US$35,000 in developing infrastructure to US$70,000-120,000 in ongoing annual costs.**[25] A study conducted by CUTS estimated the costs of a range of possible VPC solutions and suggested that DigiLocker, a relatively low- cost and digital public infrastructure-enabled method (suggested by the Draft Rules) may cost around US $45,436 per year for 1,000,000 annual verifications.[26] Such costs will create a significant barrier for organizations without large capital and resources for compliance, especially start-ups and NGOs.

[24] Iqubbal A and Jugiani K, "Economic Analysis of Verifiable Parental Consent Mechanisms: Evaluating Impact on Consumers and Data Fiduciaries" (CUTS C-CIER 2025) <https://cuts-ccier.org/pdf/economic-analysis-of-verifiable-parental-consent-mechanisms-evaluating-impact-on-consumers-and-data-fiduciaries.pdf>

[25] The Report of the Advisory Commission on Electronic Commerce: Hearing before the Subcommittee on Telecommunications, Trade, and Consumer Protection of the Committee on Commerce, House of Representatives, One Hundred Sixth Congress, Second Session, April 6, 2000. U.S. Government Printing Office, 2000, p. 83.

[26] Iqubbal and Juliani (n 24)

e. Consent vs Control



of children prefer to seek help from peers or to self-intervene when faced with digital risks, highlighting their desire for independence from their guardians.

Critically, parental consent should not be conflated with parental control, though the collapse of consent for access to services and collection of data into a single "I Agree" button often causes this confusion. VPC mechanisms are meant to ensure that a child's data is only processed with the consent of their guardian, which is based on the premise that the guardians are better equipped to understand the consequences and risks of these operations. While this means that guardians will need to know the details of the data being processed by the Data Fiduciary, it does not mean they need to control all aspects of the child's access.[27] Space2Grow also found that 79% of children prefer to seek help from peers or to self-intervene when faced with digital risks, highlighting their desire for independence from their guardians.[28] Young people today form their identities in an increasingly digital world,[29] and it remains crucial that they are able to do so with relative independence.

[27] Van Der Hof S and Ouburg S, "Methods for Obtaining Parental Consent and Maintaining Children Rights" (Leiden University 2021) <https://scholarlypublications.universiteitleiden.nl/access/item%3A3494450/download>

[28] Iyer (n 3)

[29] Hallgren C and Bjork. A, "Young People's Identities in Digital Worlds" (2023) 40 The International Journal of Information and Learning Technology 49 <https://www.diva-portal.org/smash/get/diva2:1724240/FULLTEXT02>

Key Takeaway

The conjunction of challenges in collecting Verified Parental Consent (VPC), including consent fatigue, limited digital literacy, restricting access, technical constraints, and the quandary between parental consent and control, makes it evident that the current legal mandate under the Digital Personal Data Protection Act, followed by limited compliance mechanisms in the draft Rules is insufficient to ensure the effective protection of children's personal data as intended by the legislature.

A whole-of-government approach, with additional executive directives, policy initiatives, and civil society involvement, is necessary to scaffold the legislative intent and implement the DPDP Act meaningfully.

The following section carries detailed recommendations on how this scaffolding may be achieved.

Recommendations - Solutions for India to Scaffold Legislative Approaches

Recommendation 1: Safe Harbour Programs

We recommend the introduction of Safe Harbour programs to facilitate actionable compliance with child safety legal intentions in India.

Safe harbour programs have been envisaged under COPPA (Children's Online Privacy Protection Act, 1998) the children's digital safety law in the United States. Under COPPA , industry groups and other digital actors are allowed "to seek FTC approval for self-regulatory guidelines that implement protections that are 'the same or greater' than the COPPA Rule."[30] A member of an FTC-approved COPPA safe harbor program is considered to comply with COPPA guidelines.[31]

Safe Harbor Programs provide various advantages to participating Data Fiduciaries:

1. **Safe Harbor programs provide a set of technical or organizational measures and standards to their members to establish effective safety of children.** This addresses the "how to" for various organizations who are keen to develop child safe digital experiences but are unsure about how to go about it. Thus, safe harbour programs level the "technical expertise" playing field.

---

[30] "Do Your COPPA Safe Harbor Claims Hold Water?" (Federal Trade Commission, June 13, 2022) <https://www.ftc.gov/business-guidance/blog/2020/05/do-your-coppa-safe-harbor-claims-hold-water>

[31] *Id.*

2. A Safe Harbor program has the advantage of being ex-ante rather than a one-time or a *caveat emptor*-based safeguard. It is an active representation of a platform having adopted the essential guardrails for child safety, as a pre-condition for the certification. **Safe harbour programs typically incorporate auditing or monitoring mechanisms, or provide compliance guidance to its participating companies.** For example, a company may seek Safe Harbor certification to have a product or process audited or to certify that its website or app meets legal standards.

   In the Indian context, this is especially important because:
   a. The DPDP Act is a citizen-dependent act, i.e., it depends on aware citizens to enforce the rights before the Data Protection Board ("DPB")
   b. Under the DPDP Act, the DPB has no *suo motu* powers to initiate inquiries or actions against non-compliant entities.
   c. The DPDP Act itself only provides post-facto relief to a citizen whose data protection rights are breached by Data Fiduciaries.

3. In most circumstances, a disciplinary review for a COPPA violation for a company that has a Safe Harbor affiliation will allow for a cure period instead of a formal FTC investigation, thus reducing the risks of unnecessary litigation or high penalty to the participating company.

4. Parents' participation in Safe Harbor programs also allows Data Fiduciaries to present a seal of trust to potential customers, both guardians and children, and outshine rivals lacking this seal.

Standard setting and Safe Harbor programs are not an entirely novel concept in India. Industries already seek standard certifications like the ISO standards to showcase their products' credibility and manage risks. Further, India has also seen the introduction of similar programs before. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 were amended in 2023 to provide the Ministry of Electronics and Information Technology (MEITY) the authority to recognize self-regulatory bodies that can ensure that various online real money games are permissible under the Rules.[32] However, the Ministry is yet to designate any such self-regulatory body.[33] **EdTech Tulna is an example of an industry-specific evaluation index that aims to help governments and institutions make informed decisions about EdTech solutions by providing quality standards and evaluations.**[34]

[32] The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, Rule 4A.

[33] Agrawal A, "Online Gaming Rules Are Not Enforceable Govt Tells Court" Hindustan Times (March 29, 2025) <https://www.hindustantimes.com/india-news/online-gaming-rules-are-not-enforceable-govt-tells-court-101743202910764.html>

[34] "EdTech Tulna - Standards" (*EdTech Tulna*) <https://www.edtechtulna.org/standards>

While EdTech Tulna's latest standards look at compliance with data protection legislation, learner well-being, and data security practices of platforms for its evaluation,[35] none of the evaluations it has published so far have examined these issues.[36] However, the fact that EdTech Tulna has been used in states such as Haryana, Uttar Pradesh, and Madhya Pradesh as a technical evaluation framework to select learning software indicates the demand for such industry-specific standard-setting entities.[37] **A focused set of standards for children's data protection that can extend its applicability to digital contexts including ed-tech, gaming, social media, entertainment, e-commerce, etc., will hence find demand and be both necessary and useful.** The standards will level the playing field and provide the "how to" in addition to the principle-based approach set out under the DPDPA. Safe Harbor programs that seek to protect children online will need the recognition of the DPB, the National Commission for Protection of Children's Rights, and other statutory bodies. **Buy-in from the government would ensure that the standards set are widely adopted, and give confidence to both the Data Fiduciaries and Data Principals.**

---

[35] "EdTech Tulna - Tulna 2.0" (EdTech Tulna) <https://www.edtechtulna.org/tulna-2>

[36] *Evaluation Centre Catalogue*.. EdTech Tulna. https://www.edtechtulna.org/evaluation-centre-catalogue

[37] Agrawal, S. (2023, March 22). *How Haryana, UP & MP are leading the way in regulating edtech content in govt schools*. ThePrint. https://theprint.in/india/how-haryana-up-mp-are-leading-the-way-in-regulating-edtech-content-in-govt-schools/1450311/

Recommendation 2: Digital Public Infrastructure-Based Approach Necessary to Implement VPC equitably

We recommend that the government adopt a DPI-based approach to facilitate verifiable parental consent. A DPI approach will lend to a standardized framework similar to KYC for UPI-based transactions.

Digital Public Infrastructure (DPI) can be described as "a set of shared, secure, and interoperable digital systems designed to support broad access to public and private services".[38] Examples of DPI include digital identity (such as Aadhaar) and digital payments (UPI) infrastructure.[39] DPIs, if implemented well, can generate efficiency for both the public and private sector while promoting interoperability, inclusivity and security.[40]

Creating a DPI framework for consent and VPC sharing across entities can hence potentially drastically reduce the burden on individual organizations to create independent consent collection and recording mechanisms.

---

[38] Emilsson, C., & González-Zapata, F. (2024). DIGITAL PUBLIC INFRASTRUCTURE FOR DIGITAL GOVERNMENTS. OECD. https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/12/digital-public-infrastructure-for-digital-governments_11fe17d9/ff525dc8-en.pdf

[39] Laha, K. (n.d.). *Understanding India Stack*. Protean. https://proteantech.in/articles/understanding-india-stack/

[40] Emilsson, C., & González-Zapata (n 38)

Currently, the DPDP Act and the Rules envisage the creation of Consent Managers who can assist Data Principals to "give, manage, review and withdraw" their consent.[41] The Rules also provide for a token-based process based on DigiLocker for securing verifiable parental consent.[42]

Creating infrastructural support as a DPI would take away the burden of individually creating and administering VPC mechanisms from scratch for most organizations. A DPI approach to VPC would also imply that all organizations collecting children's data would have access to the same process for obtaining verifiable parental consent, thus ensuring uniformity of processes. Adopting a DPI-based approach to facilitate VPC provides a standardised framework (similar to KYC for UPI-based transactions) that can hence reduce inefficiencies and minimise the repeated submission of sensitive data, limiting data transfers.[43]

[41] Digital Personal Data Protection Act, s. 2(g)

[42] Draft Digital Personal Data Protection Rules, Rule 10.

[43] Iqubbal and Juliani (n 24)

Recommendation 3: Launch a State-Driven Accessible Grievance Redressal Platform to Receive Concerns on Breaching Child-Centric Provisions of the DPDP Act

We recommend creating a single-window grievance redressal process—National Personal Data Protection Helpline, modeled on the National Consumer Helpline—as a mechanism to address concerns relating to data protection including children's data protection.

The DPDP law is designed such that its effectiveness in terms of protecting personal data relies on an aware and active citizenry. But there is little scaffolding to enable the citizens to advocate for their rights. As it stands in the DPDP Act, Data Principals can file grievances pertaining to a breach of their rights under the DPDP Act before the Data Protection Officer appointed by the respective Data Fiduciary.[44] Data Principals must further exhaust the option of approaching the respective Data Fiduciary before approaching the DPB.[45] The Act and Rules currently do not provide specific timelines within which Data Fiduciaries must address or close the grievances filed by the Data Principals. Further, the DPB can only act upon a complaint by a Data Principal or through reference by the Central Government.[46] The Board has no *suo motu* powers. This effectively limits accessible and broad-based options for the citizens to file grievances on breach of their data protection rights.

[44] Digital Personal Data Protection Act, s. 13

[45] Digital Personal Data Protection Act, s. 13(3)

[46] Digital Personal Data Protection Act, s. 27

The DPDPA currently provides for the DPB to function as a digital office, mandating it to adopt techno-legal measures such that its processes, including receipt of complaints, hearings and pronouncements of decisions, are digital by design.[47] Such measures can streamline processes and increase accessibility. We recommend that the DPB also set up an accessible helpline exclusively for data protection complaints against digital Data Fiduciaries, on the lines of the National Consumer Helpline (NCH) for consumer grievances,[48] to supplement opportunities to enforce Data Principals' rights. Aside from providing a single point of access for consumers for grievance redressal through various channels (ranging from toll-free numbers and WhatsApp to a web portal and the Umang app), NCH also partners with companies under 'Convergence' initiative. Under this, consumer grievances are forwarded directly to the companies, where they can respond within 30 days. This ensures that the government remains aware of the trends of grievances in real-time and can step in to take suitable remedial action if necessary. For example, during the Covid-19 pandemic, following a rise in complaints (on the NCH) against food delivery platforms like Swiggy and Zomato, the DCA initiated a dialogue to address and allay consumer grievances.[49] A similar approach for data protection grievances can be co-anchored by the National Commission for Protection of Child Rights (NCPCR) to ensure that grievances related to children's data can be adequately addressed.

---

[47] Digital Personal Data Protection Act, s. 28,

[48] *NCH-Convergence Program*, https://consumerhelpline.gov.in/public/convergenceprogram

[49] Jain, M. (2022, June 15). *Why companies like Zomato and Swiggy are in trouble with the Indian government over user complaints?* MEDIANAMA. https://www.medianama.com/2022/06/223-customer-complaints-grievance-zomato-swiggy-2/

Recommendation 4: Children's Online Data Protection Code

We recommend that India adopt an age appropriate design code to set standards for the implementation of principles of child well-being enshrined in Section 9 of the DPDP Act.

Internationally, various governments have introduced Codes that seek to protect children and their activities in the digital world. These Codes are not necessarily new legislation, but set standards on how existing legislations apply to children accessing digital services and are created after thorough consultations with all stakeholders. Such Codes can recommend additional protections that may be offered to children while also clarifying existing obligations that Data Fiduciaries have.

For instance, **the United Kingdom's Information Commissioner's Office introduced The Age-Appropriate Design Code, which contains 15 standards that online services need to follow to ensure that they are complying with their obligations under data protection law to protect children's data online**.[50] Similarly, **Ireland's Data Protection Commission created the Fundamentals for a Child-Oriented Approach to Data Processing. The Irish "Fundamentals" are a set of 14 guidelines designed to enhance the protection of children's personal data.** These guidelines aim to create safer and more privacy-respecting online environments for children.[51]

---

[50] ICO. (n.d.). Introduction to the Children's code. https://ico.org.uk/for-organizations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/introduction-to-the-childrens-code/; Please refer to Annexure 1 for a brief on the Standards of the Age Appropriate Design Code

[51] Data Protection Commission. (2021). FUNDAMENTALS FOR A CHILD-ORIENTED APPROACH TO DATA PROCESSING. In *Data Protection Commission*. https://www.dataprotection.ie/sites/default/files/uploads/2021-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_FINAL_EN.pdf; Please refer to Annexure 2 for a brief on the Fundamentals for a Child-Oriented Approach to Data Processing.

California's Age-Appropriate Design Code Act (CAADCA), a law that requires special data safeguards for underage users online slotted to come into effect in 2024, was stayed by a Federal Judge for likely violating the right to free speech.[52] Further, the **Australian Information Commissioner is currently conducting consultations to develop a Children's Online Privacy Code, after the Privacy and Other Legislation Amendment Act, 2024 introduced a mandate for the same.**[53]

Clearly, such Codes focused on protecting children's digital activities are becoming increasingly common. It is critical that these Codes are created only after extensive consultations with all stakeholders, including children themselves, their parents, industry groups, civil sector organizations, etc. A similar Code in India must meld in with other regulatory initiatives (civil and criminal) that deal with data protection and child safety, including but not limited to the Information Technology Act, 2000, the Protection of Children from Sexual Offences Act, 2012, the Bharatiya Nyaya Sanhita, 2023 and guidelines released from time to time by institutions like the NCPCR. Rather than being viewed as an additional regulatory lever, the Code should embody practical measures and implementable safeguards to ensure processing of children's data in a manner that is compliant with the DPDP Act.

---

[52] Stempel, J. (2023, September 19). Judge blocks California law meant to protect children's online safety. Reuters. https://www.reuters.com/legal/judge-blocks-california-law-meant-protect-childrens-online-safety-2023-09-18/

[53] OAIC. (2025, March 19). *Children's online privacy code*. OAIC. https://www.oaic.gov.au/privacy/privacy-registers/privacy-codes/childrens-online-privacy-code

Recommendation 5: Promote Research at Intersection of Digital Services and Children's Well-being.

We recommend more evidence-based and longitudinal research on digital platforms and their impacts on children across different age groups and socio-economic backgrounds. To do this, research communities need access to platform data and funding for research.

In India, little empirical data is available to build the bridge between the evolving digital milieu, ensuing harms and accruing co-benefits. While the NCRB reports cybercrimes against children,[54] data abusive practices are neither tracked nor systematically reported. This is further complicated in the current scenario as the DPB has no suo motu powers against Data Fiduciaries. This means that **the success of the legislative provisions under the DPDP Act relies on an aware and active citizenry.** Evidence-based research and discourse establishing causality and correlation between digital data sharing and ensuing harms are critical to ensure the meaningful implementation of a well-intentioned law.

[54] National Crime Records Bureau. (2023). Crime in India 2022. https://www.ncrb.gov.in/uploads/nationalcrimerecordsbureau/custom/1701607577CrimeinIndia2022Book1.pdf, p. 371 - 476

One significant challenge to evidence-based research is the unavailability of data pertaining to digital platforms and funding for such research. **The lack of transparency in these platforms makes it difficult to prove causality between the design of the platforms and the alleged real-world consequences.**[55] This then means that it is near impossible for even educated citizens to form accurate, evidence-based opinions on the risks of the platforms they use daily.

Recognizing the need for research into platforms and their design and the need for accurate data for the same, **in the United States, during the Biden administration, Sen. Chris Coons sponsored a Bill called the Platform Accountability and Transparency Act (PATA) in 2022".**[56] The PATA, if passed, would require social media companies to share more data with the public and researchers. The bill aims to foster a better understanding of the impact platforms have on children, families, national security, and society more broadly by producing reliable information about large social media companies and their design choices.[57]

---

[55] Harvard Law Review,. (2024, May 10). Platform Accountability and Transparency Act, s. 1876, 118th Cong. (2023). Harvard Law Review. https://harvardlawreview.org/print/vol-137/platform-accountability-and-transparency-act-s-1876-118th-cong-2023/

[56] *THE PLATFORM ACCOUNTABILITY AND TRANSPARENCY ACT*. (2023). Chris Coons. https://www.coons.senate.gov/imo/media/doc/pata_one_pager_118th_congress_june_2023.pdf

[57] Harvard Law Review (n. 55); Please refer to Annexure 3 for more details on PATA

A law similar to PATA in India will serve to build pathways of transparency in understanding and mitigating algorithmic harms from intrusive/ unsafe data practices of platforms in a timely and an ongoing manner.

The DPDP Act mandates significant data intermediaries to conduct Data Protection Impact Assessment (DPIA) and periodic audits of their processing activities.[58] Significant Data Fiduciaries also have to submit a report of the DPIA and audit conducted to the DPB.[59] We recommend that the DPB then aggregate such data that is not confidential and make it public, as it would enable researchers' understanding of digital vulnerabilities and also build public trust in governance both at the Data Fiduciary level and the government.

Further, government, philanthropic and academic funding for research needs to be made available to enable research into the effects of platform design, based on which industry responses and citizen-driven action can take place.

[58] Digital Personal Data Protection Act, s. 10(2).

[59] Draft Digital Personal Data Protection Rules, Rule 12.

Recommendation 6: Digital Literacy Programs

We recommend that widely accessible digital literacy programs be launched by the government with the support of civil society initiatives.

India has taken significant steps forward in digital learning. For instance, using Digital Public Infrastructure (DPIs) like Digital Infrastructure for Knowledge Sharing (DIKSHA), a free-to-use school platform with multiple solutions for students, teachers, and administrators, makes it possible for the various stakeholders who make up the education ecosystem to participate, contribute, and leverage a common platform to achieve learning goals at scale for the country.[60] Operating in the increasingly complex digital environment requires crucial skills and knowledge, which many in India currently lack. We recommend that widely accessible digital literacy programs be launched by the government with the support of civil society initiatives.

Many countries, recognizing the importance of digital literacy, have introduced programs in their education systems to incorporate learnings about digital technology. **Finland, one of the foremost nations in this respect, has ensured that digital literacy is a key component in the curriculum. Students are given access to digital devices in all classrooms, and teachers use digital technology in their lessons. Students are also taught about digital citizenship, including how to use such technology safely and responsibly.**[61] These programs acclimatize young people in using technology within a safe environment and prepare them for operating independently in the digital world.

---

[60] Maruwada, S. (2023, March 27). Digital Public Goods for Education: The Indian Experience. Carnegie Endowment for International Peace. https://carnegieendowment.org/research/2023/03/digital-public-goods-for-education-the-indian-experience?lang=en

[61] Finland Education Hub. (2023, October 19). *Digital Literacy in Finnish Education: a model for the world*. Finland Education Hub. https://finlandeducationhub.com/digital-literacy-in-finnish-education-a-model-for-the-world/

Conclusion

Protecting children's data online remains an important goal for the government, and the DPDP Act has laid early foundations towards that goal. However, pathways towards the implementation of the legislative intent behind the DPDP Act remain obscure.

While VPC mechanisms can be an important mechanism to protect children's data, focusing only on platforms' role can blind us to the responsibility of other stakeholders. We hope that the early actionables this paper provides can fructify the intention of the DPDP to protect children's data. **By ensuring that more parents and children are aware of their rights in the digital world and providing support for the exercise of those rights, we hope to create a more equitable and safe digital world for all.** We will follow up these recommendations with more detailed research and actionables.

Annexure 1

The **Age-Appropriate Design Code**, also known as the **Children's Code**, created by the **Information Commissioner's Office (ICO) of UK**, provides 15 standards that organizations providing online services likely to be accessed by children need to meet. These standards are:

1. **Best interests of the child:** The best interests of the child should be a primary consideration when designing or developing online services likely to be accessed by a child.
2. **Data protection impact assessments:** organizations must undertake a DPIA to assess and mitigate risks to the rights and freedoms of children who are likely to access their services, which arise from data processing. organizations must take into account differing ages, capacities, and development needs and ensure that their DPIA builds in compliance with this code.
3. **Age-appropriate application:** organizations must take a risk-based approach to recognizing the age of individual users and ensure they effectively apply the standards in this code to child users. They must either establish age with a level of certainty that is appropriate to the risks to the rights and freedoms of children that arise from data processing, or apply the standards in this code to all users instead.
4. **Transparency:** The privacy information the organizations provide to users, and other published terms, policies, and community standards, must be concise, prominent and in clear language suited to the age of the child. They should also provide additional specific 'bite-sized' explanations about how they use personal data at the point that use is activated.
5. **Detrimental use of data:** organizations should not use children's personal data in ways that have been shown to be detrimental to their well-being, or that go against industry codes of practice, other regulatory provisions, or Government advice.

6. **Policies and community standards:** Organizations should uphold their published terms, policies, and community standards (including but not limited to privacy policies, age restriction, behaviour rules and content policies).
7. **Default settings:** Settings must be 'high privacy' by default (unless a compelling reason can be demonstrated for a different default setting, taking account of the best interests of the child).
8. **Data minimisation:** Organisations should only collect and retain the minimum amount of personal data they need to provide the elements of the service in which a child is actively and knowingly engaged. Children should be given separate choices over which elements they wish to activate.
9. **Data sharing:** Organisations should not disclose children's data unless they can demonstrate a compelling reason to do so, taking account of the best interests of the child.
10. **Geolocation:** Organisations should switch geolocation options off by default (unless they can demonstrate a compelling reason for geolocation to be switched on by default, taking account of the best interests of the child). They should also provide an obvious sign for children when location tracking is active. Options which make a child's location visible to others must default back to 'off' at the end of each session.
11. **Parental controls:** If the service provides parental controls, the child should be given age-appropriate information about this. If the online service allows a parent or carer to monitor their child's online activity or track their location, the child should be given an obvious sign when they are being monitored.

12. **Profiling:** Organisations should switch options which use profiling 'off' by default (unless they can demonstrate a compelling reason for profiling to be on by default, taking account of the best interests of the child). Profiling should only be allowed if they have appropriate measures in place to protect the child from any harmful effects (in particular, being fed content that is detrimental to their health or well-being).
13. **Nudge techniques:** Organisations should not use nudge techniques to lead or encourage children to provide unnecessary personal data or weaken or turn off their privacy protections.
14. **Connected toys and devices:** If organisations provide a connected toy or device, they must ensure that they include effective tools to enable conformance to this code.
15. **Online tools:** Organisations should provide prominent and accessible tools to help children exercise their data protection rights and report concerns.

Annexure 2

The **Data Protection Commission of Ireland** introduced the **Fundamentals for a Child-Oriented Approach to Data Processing** in 2021. The Fundamentals have a slightly broader focus than the UK's Age-Appropriate Design Code, as it is not focused only on the engineering and design of online products and services.

1. **Floor of protection:** Online service providers should provide a "floor" of protection for all users, unless they take a risk-based approach to verifying the age of their users, so that the protections set out in these Fundamentals are applied to all processing of children's data.
2. **Clear-cut consent:** When a child has given consent for their data to be processed, that consent must be freely given, specific, informed and unambiguous, made by way of a clear statement or affirmative action.
3. **Zero interference:** Online service providers processing children's data should ensure that the pursuit of legitimate interests do not interfere with, conflict with, or negatively impact, at any level, the best interests of the child
4. **Know your audience:** Online service providers should take steps to identify their users and ensure that services directed at/ intended for or likely to be accessed by children have child-specific data protection measures in place
5. **Information in every instance:** Children are entitled to receive information about the processing of their own personal data irrespective of the legal basis relied on and even if consent was given by a parent on their behalf to the processing of their personal data.

6. **Child-oriented transparency:** Privacy information about how personal data is used must be provided in a concise, transparent, intelligible and accessible way, using clear and plain language that is comprehensible and suited to the age of the child.
7. **Let children have their say:** Online service providers shouldn't forget that children are data subjects in their own right and have rights in relation to their personal data at any age. The DPC considers that a child may exercise these rights at any time, as long as they have the capacity to do so and it is in their best interests.
8. **Consent doesn't change childhood:** Consent obtained from children or from the guardians/ parents should not be used as a justification to treat children of all ages as if they were adults.
9. **Your platform, your responsibility:** Companies who derive revenue from providing or selling services through digital and online technologies pose particular risks to the rights and freedoms of children. Where such a company uses age verification and/ or relies on parental consent for processing, the DPC will expect it to go the extra mile in proving that its measures around age verification and verification of parental consent are effective.
10. **Don't shut out child users or downgrade their experience:** If your service is directed at, intended for, or likely to be accessed by children, you can't bypass your obligations simply by shutting them out or depriving them of a rich service experience.
11. **Minimum user ages aren't an excuse:** Theoretical user age thresholds for accessing services don't displace the obligations of organisations to comply with the controller obligations under the GDPR and the standards and expectations set out in these Fundamentals where "underage" users are concerned.

12. **A precautionary approach to profiling:** Online service providers should not profile children and/ or carry out automated decision making in relation to children, or otherwise use their personal data, for marketing/ advertising purposes due to their particular vulnerability and susceptibility to behavioural advertising, unless they can clearly demonstrate how and why it is in the best interests of the child to do so.
13. **Do a DPIA:** Online service providers should undertake data protection impact assessments (DPIA) to minimise the data protection risks of their services, and in particular the specific risks to children which arise from the processing of their personal data. The principle of the best interests of the child must be a key criterion in any DPIA and must prevail over the commercial interests of an organisation in the event of a conflict between the two sets of interests.
14. **Bake it in:** Online service providers that routinely process children's personal data should, by design and by default, have a consistently high level of data protection which is "baked in" across their services.

Annexure 3

The **Platform Accountability and Transparency Act (PATA)** was first introduced in Congress in December 2022 by Senator Chris Coons.[62] The Act aimed to create **three new mechanisms to increase transparency around social media companies**:

1. **Researcher-specific data access:** Under PATA, independent researchers would be able to submit proposals to study social media companies to the National Science Foundation, which is an independent agency that promotes scientific inquiry by approving research and development proposals. If a researcher's request is approved, platforms would be required to provide the necessary data for the study, subject to privacy and cybersecurity protections.
2. **Limited legal safe harbor for automated data collection:** The safe harbor would prevent social media companies from suing or criminally accusing public interest researchers who use automated means to collect public-facing platform information, so long as the researcher uses appropriate privacy safeguards for the data they collect. Companies would not be prevented from taking any technical measures to secure their platforms or stop this kind of data collection, but they would not be able to hold researchers liable for contract violations or threaten potential criminal liability if the research meets the prescribed conditions. Researchers report that the possibility of such liability is a significant obstacle to their ability to analyze platform behavior.

[62] Senator Coons, colleagues introduce legislation to provide public with transparency of social media platforms

3. Enhanced transparency through disclosures: PATA would require covered platforms to disclose certain information that would provide a much stronger understanding of what is happening on platforms that is currently shrouded from view.
   Specifically, platforms would be required to report information about:

   a. **Viral content:** Metrics about content that has gone viral or has been distributed from major public accounts, e.g., data about the extent of dissemination, engagement, audience, and whether the content was recommended, amplified, or restricted.
   b. **Ad library:** Information about advertisers and ads they have run, and metrics about dissemination, reach, engagement, and targeting criteria.
   c. **Algorithmic design:** A semi-annual description of the data used as inputs in ranking or recommendation algorithms and how that data affects the algorithm's output; information about each algorithm's optimization objective; information about how content is scored or ranked; and information about how companies assess new products.
   d. **Content moderation:** Statistics about content that a platform took action against, broken down by the categories like the policy that was violated; geographic and demographic factors; data about the number of times violating content was viewed; information about how violating content was identified; the extent to which violating content was recommended, amplified, or restricted; and estimates about the prevalence of violating content.

PACTA

SOCIAL | IMPACT | LEGAL

https://pacta.in/

hello@pacta.in

Pulse by Pacta

P/37, 11th Cross Rd,
Jeevan Bhima
Nagar, Bengaluru,
Karnataka 560075

@ Pactaindia