[recovered from the vector store — section9.html p.1]

Section 9 DPDPA

Processing of personal data of children. 9.(1) The Data Fiduciary shall, before processing any personal data of a child or a person with disability who has a lawful guardian obtain verifiable consent of the parent of such child or the lawful guardian, as the case may be, in such manner as may be prescribed. Explanation.—For the purpose of this sub-section, the expression “consent of the parent” includes the consent of lawful guardian, wherever applicable. (2) A Data Fiduciary shall not undertake such processing of personal data that is likely to cause any detrimental effect on the well-being of a child. (3) A Data Fiduciary shall not undertake tracking or behavioural monitoring of children or targeted advertising directed at children. (4) The provisions of sub-sections (1) and (3) shall not be applicable to processing of personal data of a child by such classes of Data Fiduciaries or for such purposes, and subject to such conditions, as may be prescribed.
(5) The Central Government may, if satisfied that a Data Fiduciary has ensured that its processing of personal data of children is done in a manner that is verifiably safe, notify for such processing by such Data Fiduciary the age above which that Data Fiduciary shall be exempt from the applicability of all or any of the obligations under sub-sections (1) and (3) in respect of processing by that Data Fiduciary as the notification may specify. Applicable DPDP Rule 2025

Rule 10: Verifiable Consent for Processing of Personal Data of Child or of Person with Disability Who has Lawful Guardian

Rule 11: Exemptions from certain obligations applicable to processing of personal data of child

Read More on The Rule 10 of DPDP Rules and its Legal Interpretation

Read more on BLOG : Childrens of illiterate parents BANNED from social media IN INDIA?

Read more on BLOG : Consent under DPDPA - Comprehensive Understanding

← Section 8 DPDPA

[recovered from the vector store — section9.html p.2]

Table of contents

Report error

Your message
×

Please keep in mind that this form is only for feedback and suggestions for improvement. Unfortunately, questions will not be answered.

Do not fill this field

0 of 1000 max characters

Submit

Comprehensive Legal Interpretation of Section 9 of the Digital Personal Data Protection Act, 2023

"Children are not things to be molded, but are people to be unfolded." - Jess Lair

Section 9 - Processing of Personal Data of Children

Statutory Text

Section 9(1). The Data Fiduciary shall, before processing any personal data of a child or a person with disability who has a lawful guardian obtain verifiable consent of the parent of such child or the lawful guardian, as the case may be, in such manner as may be prescribed.

Explanation. For the purpose of this sub-section, the expression "consent of the parent" includes the consent of lawful guardian, wherever applicable.

Section 9(2). A Data Fiduciary shall not undertake such processing of personal data that is likely to cause any detrimental effect on the well-being of a child.
Section 9(3). A Data Fiduciary shall not undertake tracking or behavioural monitoring of children or targeted advertising directed at children.

Section 9(4). The provisions of sub-sections (1) and (3) shall not be applicable to processing of personal data of a child by such classes of Data Fiduciaries or for such purposes, and subject to such conditions, as may be prescribed.

Section 9(5). The Central Government may, if satisfied that a Data Fiduciary has ensured that its processing of personal data of children is done in a manner that is verifiably safe, notify for such processing by such Data Fiduciary the age above which that Data Fiduciary shall be exempt from the applicability of all or any of the obligations under sub-sections (1) and (3) in respect of processing by that Data Fiduciary as the notification may specify.

Applicable DPDP Rules 2025:

Rule 10: Verifiable Consent

[recovered from the vector store — section9.html p.3]

for Processing of Personal Data of Child or of Person with Disability Who has Lawful Guardian

Rule 11: Exemptions from certain obligations applicable to processing of personal data of child

Table of Contents

1. Executive Summary: Protecting Digital Childhood
Section 9 represents a paradigm shift in how Indian law views children in the digital ecosystem. For the first time, statutory law recognizes that children are not simply "small adults" - they are a vulnerable population requiring heightened protection in the data economy.

 Why Children Need Special Protection

Developmental Psychology: Children's brains are still developing, particularly:

Prefrontal Cortex: Responsible for decision-making, impulse control (not fully developed until mid-20s)

Risk Assessment: Children cannot fully evaluate long-term consequences

Peer Pressure Vulnerability: More susceptible to social influence

Cognitive Biases: More prone to manipulation

Digital Vulnerability: Children face unique online risks:

Exploitation: Predators, grooming, abuse

Manipulation: Dark patterns, addictive design, microtransactions

Long-term Harm: Digital footprint created before they can consent

Mental Health: Social media anxiety, cyberbullying, FOMO

Privacy Loss: Data collected in childhood follows them for life

Section 9's Philosophy: "Children should be free to be children, not data products."

1.1 The Five-Layer Protection Framework

[recovered from the vector store — section9.html p.4]

ld around children's data:

Layer | Protection | Purpose | Penalty for Violation
Layer 1: Gatekeeping | Verifiable parental consent (9(1)) | Parents control access to children's data | ₹200 crores (Schedule Item 2)
Layer 2: Harm Prevention | No detrimental effects (9(2)) | Protect child well-being | ₹200 crores (Schedule Item 3)
Layer 3: Absolute Prohibitions | No tracking, profiling, targeted ads (9(3)) | Prevent commercial exploitation | ₹200 crores (Schedule Item 2)
Layer 4: Exemption Safeguards | Limited exemptions with conditions (9(4)) | Balance protection with practicality | N/A (depends on violation)
Layer 5: Age Flexibility | Verifiably safe processing (9(5)) | Reward good actors | N/A (incentive mechanism)

1.2 Critical Point: Section 9 Applies to ALL Data Fiduciaries

Common Misconception: "Section 9 only applies to services 'for children' like gaming apps or educational platforms."

Reality: Section 9 applies to ANY Data Fiduciary processing data of ANY child, regardless of whether the service is child-directed.
Examples:

E-commerce site that allows 17-year-olds to shop → Section 9 applies

Social media platform with users of all ages → Section 9 applies to underage users

Banking app used by minors (with parental account) → Section 9 applies

General news website visited by children → Section 9 applies

2. Philosophical Foundations: Children's Rights Theory

2.1 UN Convention on the Rights of the Child (1989)

India ratified the UNCRC in 1992, committing to protect children's rights, including in emerging contexts like digital spaces.

Four Core Principles:

Non-discrimination (Article 2): All children have equal rights

Best Interests (Article 3): Child's best interests must be primary consideration

Right to Life, Survival, Development (Article 6): Includes psychological and social development

Respect for Views of Child (Article 12): Children's opinions matter

Section 9 Implementation:

9(1): Best interests - parents act as decision-makers

9(2):

[recovered from the vector store — section9.html p.5]

Right to development - no detrimental processing

9(3): Protection from exploitation - no commercial manipulation

2.2 Parens Patriae Doctrine

Legal Maxim: "The State as Parent" - Government has duty to protect those who cannot protect themselves.

Origin: English common law, adopted in Indian jurisprudence.

Application to Section 9: State (through DPDPA) steps in to protect children from data exploitation that they (and often parents) cannot understand or prevent.

2.3 Developmental Psychology: Piaget & Kohlberg

Jean Piaget's Cognitive Development Theory:

Ages 7-11 (Concrete Operational): Logical thinking about concrete situations, but not abstract concepts like "data processing"

Ages 12+ (Formal Operational): Abstract thinking emerges, but still developing

Lawrence Kohlberg's Moral Development:

Children under 13 typically at "Conventional Level" - follow rules to please others or maintain social order

Vulnerable to manipulation through social pressure
Section 9's Age 18 Threshold: Recognizes that full capacity for informed consent develops gradually, erring on side of protection.

2.4 Academic Research on Children and Digital Media

Key Studies:

Livingstone & Third (2017) - "Children and Young People's Rights in the Digital Age" New Media & Society.

Found that children face "privacy paradox" - desire privacy but lack skills to protect it. Parental mediation necessary but insufficient.

Twenge (2017) - "iGen: Why Today's Super-Connected Kids Are Growing Up Less Rebellious, More Tolerant, Less Happy"

Documented mental health crisis among children with high social media use. Data-driven algorithmic amplification of harmful content.

Auxier et al. (2020) - Pew Research: "Parenting Children in the Age of Screens"

71% of parents concerned about child's online privacy, but only 39% feel equipped to protect it.

Section 9 addresses these research findings through mandatory parental consent and absolute prohibitions.

3. Constitutional Framework: Best Interest

[recovered from the vector store — section9.html p.6]

s of the Child

3.1 Article 21: Right to Life and Personal Liberty

Supreme Court has consistently held that Article 21 includes right to healthy development for children.

MC Mehta v. State of Tamil Nadu, (1996) 6 SCC 756 (Child Labour Case):

"Children are the greatest gift to humanity. They are the future of the nation. Their development is the key to the progress of the country."

Application to Section 9: Right to healthy development includes protection from digital exploitation, surveillance, and manipulation.

3.2 Article 39(f): Child Protection Directive

Article 39(f) (Directive Principle): "That children are given opportunities and facilities to develop in a healthy manner and in conditions of freedom and dignity and that childhood and youth are protected against exploitation..."

Section 9 implements this constitutional directive in the digital sphere.

3.3 Bachpan Bachao Andolan v. Union of India (2011)

Bachpan Bachao Andolan v. Union of India, (2011) 5 SCC 1:

Supreme Court held that child rights are fundamental, not merely aspirational. State must take proactive measures to protect children from exploitation.
Section 9's Proactive Measures:

Mandatory parental consent (not optional)

Absolute prohibitions (not negotiable)

Criminal penalties for violations

4. Who is a "Child" Under DPDPA?

Definition (Section 2(k)): "Child" means an individual who has not completed the age of eighteen years.

4.1 Bright-Line Rule: Under 18 = Child

DPDPA adopts a bright-line rule: Anyone under 18 is a child, period. No exceptions.

Age | Status Under DPDPA | Section 9 Applies? | Notes
0-17 years, 364 days | Child | ✅ Yes | Full Section 9 protections
18 years, 0 days | Adult | ❌ No | Regular consent rules apply
17 years (nearly 18) | Child | ✅ Yes | No "mature minor" exception
16 years (can marry in some states) | Child | ✅ Yes | Marriage doesn't grant data majority

4.2 Why 18? Comparative Analysis

Jurisdiction | Age of Digital Consent | Notes
India (DPDPA) | 18 ye

[recovered from the vector store — section9.html p.7]

ars | Highest protection threshold
USA (COPPA) | 13 years | Lower threshold, criticized
EU (GDPR) | 16 years (Member States can lower to 13) | Variable by country
UK (Age-Appropriate Design Code) | 18 years (strict protection) | Similar to India
Australia | Proposed 16 years | Under consideration

India's Choice of 18:

Aligns with age of majority for contracts (Indian Contract Act, 1872)

Matches voting age (Constitution)

Consistent with other child protection laws (POCSO, JJ Act)

Higher protection = safer approach

5. Section 9(1): Verifiable Parental Consent

Statutory Language: "The Data Fiduciary shall, before processing any personal data of a child or a person with disability who has a lawful guardian obtain verifiable consent of the parent of such child or the lawful guardian..."

5.1 Three Key Requirements

BEFORE processing: Consent must precede data collection

VERIFIABLE consent: Must actually verify it's the parent/guardian

OF THE PARENT: Not the child's own consent

5.2 What is "Verifiable" Consent?

Rule 10 (DPDP Rules 2025) prescribes verification methods:

 Approved Verification Methods
1. Aadhaar-Based Verification (Recommended)

Parent provides Aadhaar number

OTP sent to registered mobile

Age verified (must be 18+)

Relationship to child verified (if Aadhaar family linking available)

2. Credit/Debit Card Verification

Parent provides card details

Small charge (₹1-2) processed, immediately refunded

Confirms parent has financial instrument (proxy for adulthood)

Cardholder name must match declared parent name

3. Video KYC

Live video call with parent

Government ID shown on camera

Face match with ID

Child present on call (confirms relationship)

4. Digital Signature Certificate

Parent signs consent using DSC

High assurance of identity

Useful for high-value services

5. Bank Account Verification

Micro-deposit to parent's bank account

Parent confirms deposit amount

Verifies account ownership

6. Offline Verification (Paper Form)

Phy

[recovered from the vector store — section9.html p.8]

sical form signed by parent

ID copy attached

Notarized or witnessed

Useful for schools, offline services

5.3 Inadequate Verification Methods (Non-Compliant)

 Invalid Verification Methods

1. Checkbox "I am the parent"

Problem: No verification. Child can lie.

Compliance: Violates Section 9(1)

2. Email to parent

"Consent email sent to parent@email.com. Click link to approve."

Problem: Child can create fake email, access parent's email, or use own email.

Compliance: Not "verifiable"

3. Age Gate Only

"Are you over 18? [Yes] [No]"

Problem: Child can lie. No parent involvement.

Compliance: Violates Section 9(1)

4. Parent's Birthday

"Enter your parent's date of birth"

Problem: Child knows this information.

Compliance: Not verifiable
5. SMS to Parent's Number

"OTP sent to parent's mobile"

Problem: Child may have access to parent's phone, or use own number. Compliance: Weak verification (better than nothing, but not ideal)

5.4 The Consent Process Flow

 Compliant Parental Consent Flow

Step 1: Age Detection

User indicates age (birthday, age gate, etc.)

↓

Step 2: Under 18 Detected

System identifies user as child

↓

Step 3: Parental Notice

"You are under 18. To use this service, we need your parent's consent."

"What data we collect: [List]"

"Why we need it: [Purposes]"

↓

Step 4: Parent Contact Collection

"Please provide your parent's email address and phone number"

↓

Step 5: Verification Initiation

Email/SMS sent to parent:

"Your child [Name] wants to use [Service]. We need your verified consent. Click here to verify your identity and provide consent."

↓

Step 6: Parent Identity Verification

Parent chooses verification method:

Aadhaar OTP

Credit card verification

Video KYC

etc.
↓

Step 7: Informed Consent

After verification, show parent:

What data will be collected

How it will be used

How long it will be kept

Parent's rights (access, deletion, withdrawal)

↓

Step 8: Parent Decision

[Approve] [Deny]

↓

Step 9: C

[recovered from the vector store — section9.html p.9]

hild Notification

If approved: "Your parent has given consent. You can now use the service."

If denied: "Your parent did not give consent. We cannot provide the service."

5.5 Challenges and Solutions

⚠️ Practical Challenges

Challenge 1: Parent Doesn't Have Aadhaar/Smartphone

Solution: Offer multiple verification methods including offline (paper form)

Challenge 2: Parent Unwilling to Share Aadhaar

Solution: Privacy concerns valid. Offer alternatives (credit card, video KYC)

Challenge 3: Orphans or Children in Institutional Care

Solution: Legal guardian (institutional head, government official) can consent

Challenge 4: International Users (Child in India, Parent Abroad)

Solution: Accept international verification methods, but child must be in India for DPDPA to apply

Challenge 5: High Verification Cost

Solution: Balance security with practicality. Aadhaar OTP is low-cost and effective

6. Section 9(2): No Detrimental Effect on Well-Being

Statutory Language: "A Data Fiduciary shall not undertake such processing of personal data that is likely to cause any detrimental effect on the well-being of a child."

This is a harm-based prohibition. Processing that harms children is categorically forbidden, even with parental consent.

6.1 What is "Detrimental Effect on Well-Being"?

Well-being includes:

Physical well-being: Health, safety, bodily integrity

Mental well-being: Psychological health, self-esteem, emotional development

Social well-being: Relationships, social skills, peer interactions

Educational well-being: Learning, cognitive development, academic progress

Moral well-being: Values, ethics, character development

⚠️ Processing with Detrimental Effects

1. Addictive Design Patterns

Example: Gaming app uses variable reward schedules (loot boxes) to create addiction.

Detrimental Effect: Mental health (addiction), social (isolation), educational (distraction)

Violation: Section 9(2) - harms well-being

2. Body Image Manipulation

Example: Social me

[recovered from the vector store — section9.html p.10]

dia app uses facial recognition to suggest "beauty filters," algorithmic feed amplifies unrealistic beauty standards.

Detrimental Effect: Mental health (body dysmorphia, eating disorders, low self-esteem)

Violation: Section 9(2)

3. Exploitation of FOMO

Example: App sends constant notifications ("Your friends are online! Don't miss out!") to keep children engaged.

Detrimental Effect: Mental health (anxiety), social (peer pressure), educational (distraction)

Violation: Section 9(2)

4. Privacy Violations Leading to Bullying

Example: Platform publicly displays children's personal information, enabling targeted harassment.

Detrimental Effect: Mental health (trauma, depression), social (bullying), physical (self-harm risk)

Violation: Section 9(2)

5. Age-Inappropriate Content Exposure

Example: Video platform's recommendation algorithm exposes 10-year-old to violent or sexual content.

Detrimental Effect: Mental health (trauma, desensitization), moral (value distortion)

Violation: Section 9(2)
6. Data Breach Causing Identity Theft

Example: Poor security leads to breach of children's data, used for fraud or exploitation.

Detrimental Effect: Physical (safety risk), mental (trauma), financial (long-term credit damage)

Violation: Section 9(2)

6.2 The "Likely to Cause" Standard

Section 9(2) uses "likely to cause" - not "actually causes."

This is a PRECAUTIONARY standard:

Don't need to prove actual harm occurred

Don't need to wait for children to be harmed

If processing is likely (probable, foreseeable) to harm children, it's prohibited

Burden is on Data Fiduciary to prove processing is NOT likely to harm

7. Section 9(3): Absolute Prohibitions

Statutory Language: "A Data Fiduciary shall not undertake tracking or behavioural monitoring of children or targeted advertising directed at children."

This is the "triple lock" on children's data - three activities that are ABSOLUTELY FORBIDDEN, even with parental consent.

7.1 Prohibition #1: Tracking

What is "

[recovered from the vector store — section9.html p.11]

Tracking"?

Following a child's activities across websites, apps, or online services over time to build a profile of their behavior. Prohibited Tracking Activities

Cross-Site Tracking:

Child visits Site A (shopping), Site B (gaming), Site C (education). Tracker follows child across all three to build profile. Violation: Section 9(3)

Cross-App Tracking:

Child uses App X, Y, Z. Common SDK tracks child across all apps. Violation: Section 9(3)

Location Tracking:

App continuously tracks child's physical location throughout day, building movement patterns. Violation: Section 9(3)

Search History Tracking:

Search engine tracks all searches by child over time. Violation: Section 9(3)

Social Graph Tracking:

Platform tracks who child interacts with, frequency, topics, to map social connections.
Violation: Section 9(3)

Permitted (Not "Tracking"):

 Session cookies (functional, not tracking)

 Within-app analytics (e.g., which game levels completed - as long as not shared cross-app)

 One-time location lookup (e.g., "Where are you?" for local content) if immediately discarded

 Parent-initiated location sharing for safety (Find My Phone) if parent controls it

7.2 Prohibition #2: Behavioral Monitoring

What is "Behavioral Monitoring"?

Observing, analyzing, and recording a child's behavior patterns to predict or influence future behavior.
 Prohibited Behavioral Monitoring

1. Psychological Profiling

Analyzing child's content interactions to infer personality traits, emotions, vulnerabilities.

Example: "This child shows signs of anxiety based on search patterns. Show content that exploits that."

Violation: Section 9(3)

2. Predictive Analytics

Using child's data to predict future behavior or preferences.

Example: "This child is likely to purchase in-game items. Increase prompts."

Violation: Section 9(3)

3. A/B Testing for Engagement

Testing different app features on children to see which increases engagement/usage.

Example: "Test re

[recovered from the vector store — section9.html p.12]

d vs. blue notification dot on 10,000 child users to maximize clicks."

Violation: Section 9(3)

4. Sentiment Analysis

Analyzing child's posts, messages, or content to determine emotional state.

Example: "Detect when child is sad, show uplifting content to increase usage."

Violation: Section 9(3)
5. Habit Formation Monitoring

Tracking when child is most vulnerable (tired, bored, stressed) to push notifications/content. Example: "Child most likely to engage at 10 PM on school nights. Schedule notifications then."

Violation: Section 9(3)

7.3 Prohibition #3: Targeted Advertising

What is "Targeted Advertising"?

Showing ads to a child based on their personal data, behavior, or profile. Ad Type | Description | Allowed for Children?
Contextual Ads | Based on current content (e.g., toy ad on toy website) | Yes
Generic Ads | Same ad shown to all users (e.g., movie trailer) | Yes
Behavioral Ads | Based on child's browsing history, interests, profile | NO - Violates 9(3)
Retargeting Ads | Following child across web after visiting a site | NO - Violates 9(3)
Personalized Ads | Tailored to child's demographics, location, interests | NO - Violates 9(3)
Lookalike Targeting | Targeting children similar to existing customers | NO - Violates 9(3)

 Compliant Advertising for Children

Example 1: Educational App

Math learning app for ages 8-12.
Permitted: Show same educational book ad to ALL users

Prohibited: Show specific books based on each child's learning level (behavioral targeting)

Example 2: Kids' Entertainment Platform

Streaming service with children's shows. Permitted: Show movie trailer to all kids watching cartoons

Prohibited: Show different trailers based on each child's viewing history

Example 3: Gaming Website

Free online games for children. Permitted: Banner ad for new game (same for everyone)

Prohibited: Ad for game similar to ones child played before (personalized)

7.4 Critical Question: "Even With Parental Consent?"

YES. Sect

[recovered from the vector store — section9.html p.13]

ion 9(3) prohibitions apply even if parent consents.

Why? Some harms are so severe that parents cannot waive protection.

Legal Principle: Volenti non fit injuria (to one who consents, no harm is done) does NOT apply when:

Consent involves rights of third party (child's future rights)

Activity is against public policy

Harm is irreparable

Analogy: Parents cannot consent to child labor, even if family needs income. Some protections are non-waivable.

8. Sections 9(4) & 9(5): Exemptions and Age Flexibility

8.1 Section 9(4): Limited Exemptions

Statutory Language: "The provisions of sub-sections (1) and (3) shall not be applicable to processing of personal data of a child by such classes of Data Fiduciaries or for such purposes, and subject to such conditions, as may be prescribed."

Rule 11 (DPDP Rules 2025) prescribes exemptions:

 Exempted Processing (Rule 11)
1. Educational Institutions (for educational purposes)

Exempt From: Parental consent (9(1))

Conditions:

Processing necessary for educational service delivery

School/college has in loco parentis authority

Parents notified of processing

Safeguards in place

Example: School maintaining student records, grades, attendance

2. Medical Emergency Processing

Exempt From: Parental consent (9(1))

Conditions:

Immediate medical necessity

Parent unavailable or delay would cause harm

Processing limited to emergency treatment

Example: Ambulance processing child's medical data during emergency

3. Government Services for Child Welfare

Exempt From: Parental consent (9(1))

Conditions:

Statutory obligation under child protection laws

Processing in child's best interest

Oversight by competent authority

Example: Child Welfare Committee processing data of children in need of care

IMPORTANT: Section 9(3) prohibitions (tracking, profiling, targeted ads) have NO exemptions. They apply universally.

8.2 Section 9(5): Age Flexibility Mechanism

Statutory Language: "The Central Government may, if satisfied that

[recovered from the vector store — section9.html p.14]

a Data Fiduciary has ensured that its processing of personal data of children is done in a manner that is verifiably safe, notify for such processing by such Data Fiduciary the age above which that Data Fiduciary shall be exempt from the applicability of all or any of the obligations under sub-sections (1) and (3)..."

This is a "regulatory sandbox" for child data protection - a reward mechanism for exemplary Data Fiduciaries.
 Age Flexibility: How It Works

Step 1: Data Fiduciary's Application

Company applies to Central Government demonstrating:

Robust child safety measures

Track record of exemplary compliance

Independent audits showing "verifiably safe" processing

Age-appropriate design principles implemented

Step 2: Government Evaluation

Ministry evaluates application considering:

Technical safeguards

Organizational policies

Compliance history

Third-party certifications

User feedback

Step 3: Notification (If Satisfied)

Government may issue notification:

"For [Company X], in respect of [Service Y], the age of child protection shall be 16 years (instead of 18) subject to conditions: [List]"

Effect:

For that specific company and service, users aged 16-17 are treated as adults (can give own consent, exempted from Section 9(3) prohibitions).
Example Scenario:

Company: Educational platform with 10-year track record, zero breaches, extensive child safety features

Application: Request to treat 16-17 year-olds as adults

Justification: Age-appropriate educational content, strong moderation, privacy-by-design architecture

Government Decision: Grants age flexibility to 16

Result: 16-17 year-olds can use platform without parental consent

Key Points:

Age flexibility is entity-specific and service-specific

Can be revoked if standards slip

Incentivizes best-in-class child protection

Recognizes that 16-17 year-olds have more capacity than younger children

9. Persons with Disability: Guardian Consent

Section 9(1) also covers "person with disability

[recovered from the vector store — section9.html p.15]

who has a lawful guardian."

9.1 Who Qualifies?

Rights of Persons with Disabilities Act, 2016: Defines disabilities including:

Intellectual disability

Mental illness

Autism spectrum disorder

Cerebral palsy

Multiple disabilities

Others affecting decision-making capacity

Key Requirement: Person must have a LAWFUL GUARDIAN appointed by court or recognized by law.

Not All Persons with Disabilities Need Guardian Consent:

Person with physical disability (no cognitive impairment) = regular consent

Person with intellectual disability WITH guardian = guardian consent required

Person with intellectual disability WITHOUT guardian = can self-consent if capable

9.2 Guardian Verification

Data Fiduciary must verify:

Person has disability affecting consent capacity

Guardian is legally appointed (court order, disability certificate, etc.)

Guardian's identity (same verification methods as parental consent)
10. Comparative Analysis: DPDPA vs GDPR vs COPPA

Aspect | India (DPDPA) | EU (GDPR) | USA (COPPA)
Age Threshold | 18 years | 16 years (can lower to 13) | 13 years
Parental Consent | Mandatory + verifiable | Mandatory (verification not specified) | Mandatory + verifiable
Profiling Ban | ✅ Absolute (9(3)) | ✅ Absolute (Art. 22) | ❌ Not absolute
Targeted Ads Ban | ✅ Absolute (9(3)) | ⚠️ Not explicit in GDPR | ❌ Allowed with consent
Tracking Ban | ✅ Absolute (9(3)) | ⚠️ Not explicit ban | ❌ Allowed with consent
Well-Being Standard | ✅ Explicit (9(2)) | ✅ Via "best interests" (Recital 38) | ❌ Not explicit
Age Flexibility | ✅ Yes (9(5) - by govt notification) | ✅ Yes (Member States set) | ❌ No (fixed at 13)
Disability Protection | ✅ Explicit (9(1)) | ✅ Via accessibility requirements | ❌ Not explicit

India's Approach: Most Protective

Highest age threshold (18 vs 13-16 elsewhere)

Absolute prohibitions on tracking, profiling, targeted ads

Explicit harm prevention standard

Specific protection for persons with disabilities

11. Practical Compliance Guidance

11.1 Secti

[recovered from the vector store — section9.html p.16]

on 9 Compliance Checklist

 Complete Child Protection Compliance

BEFORE LAUNCH:

 Age verification mechanism implemented

 Parental consent system designed (choose verification method)

 Verification method approved under Rule 10

 ZERO tracking of children (no cross-site, cross-app tracking)

 ZERO behavioral monitoring of children

 ZERO targeted advertising to children (only contextual/generic ads)

 Harm assessment completed (9(2) compliance)

 No addictive design patterns for children

 Age-appropriate content filters

 Privacy-by-default for children
 Guardian consent system (if serving persons with disabilities)

 Exemption application (if applicable under Rule 11)

 Staff training on child protection obligations

ONGOING:

 Regular audits of child data processing

 Monitor for compliance with Section 9(3) prohibitions

 Parent communication system (rights, controls, transparency)

 Incident response plan for child data breaches

 Age flexibility application (if seeking 9(5) benefit)

 Annual review of well-being impact (9(2))

11.2 Common Section 9 Violations

 Top 15 Child Protection Violations
1. Fake Age Gate

 "Are you over 18? [Yes] [No]" with no verification

Penalty: ₹200 crores

2. Email-Only Parental Consent

 Sending consent link to unverified email

Penalty: ₹200 crores

3. Cross-App Tracking of Children

 SDK tracking child across multiple apps

Penalty: ₹200 crores

4. Behavioral Ad Targeting to Children

 "This child likes dinosaurs. Show dinosaur toy ads."

Penalty: ₹200 crores

5. Psychological Profiling

 Analyzing child's emotional vulnerabilities for engagement

Penalty: ₹200 crores

6. Addictive Loot Box Design

 Variable reward gambling mechanics targeting children

Penalty: ₹200 crores (9(2) violation)

7. Retargeting Ads to Children

 Following child across web with ads for product they viewed

Penalty: ₹200 crores

8. Location Tracking Without Purpose

 Continuously tracking child's location for profilin

[recovered from the vector store — section9.html p.17]

9. Social Graph Analysis

 Mapping child's friendships and social connections

Penalty: ₹200 crores

10. A/B Testing on Children

 Experimenting with app features to maximize engagement

Penalty: ₹200 crores

11. Search History Profiling

 Building profile based on child's searches

Penalty: ₹200 crores

12. Sentiment Analysis for Manipulation

 Detecting when child is sad to push content

Penalty: ₹200 crores

13. Consent After Processing

 Starting data collection, then asking parent for consent

Penalty: ₹200 crores

14. Ignoring Parental Withdrawal

 Parent withdraws consent, company continues processing

Penalty: ₹200 crores

15. "Educational Purpose" Excuse for Tracking

 "We track students to personalize learning" (if tracking is cross-platform profiling)

Penalty: ₹200 crores

11.3 Design Principles for Child-Safe Services

 Age-Appropriate Design Code

Inspired by UK's Age-Appropriate Design Code, adapted for DPDPA:

1. Best Interests of Child

Design decisions should prioritize child's well-being over commercial interests.

2. Privacy by Default

Highest privacy settings should be default for children.
3. Transparency

Privacy information in language children (and parents) can understand.

4. Detrimental Use Prohibition

Do not use data in ways harmful to children (implements Section 9(2)).

5. No Profiling

Do not build profiles of children (implements Section 9(3)).

6. No Nudging

Do not use nudge techniques to weaken privacy choices.

7. Data Minimization

Collect only data necessary for service function.

8. Age-Appropriate UX

Design interface suitable for child's age and understanding.

9. Parental Controls

Give parents visibility and control over child's data.

10. Safety by Design

Build in safety features (e.g., reporting abuse, moderation).

12. Conclusion: Reclaiming Digital Childhood

Section 9 is not just about data protection - it's about protecting childhood itself in the digital age.

For too long, childr

[recovered from the vector store — section9.html p.18]

en have been treated as "data products" - tracked, profiled, manipulated, and monetized. Their vulnerabilities exploited, their development harmed, their privacy invaded.

Section 9 says: ENOUGH.

"Childhood is not a race to see how quickly a child can read, write and count. It is a small window of time to learn and develop at the pace that is right for each individual child."

This applies equally to digital childhood. Let children develop without being surveilled, profiled, or manipulated at every click.

Key Principles to Remember:

Age 18 is the Bright Line: No exceptions, no "mature minor" doctrine

Parents are Gatekeepers: Verifiable consent required BEFORE processing

Well-Being First: Processing harmful to children is forbidden

Triple Lock: NO tracking, NO profiling, NO targeted ads - EVER

No Consent Override: Section 9(3) prohibitions apply even with parental consent

Proportionate Penalties: Up to ₹200 crores for violations - protecting children is serious

Reward Good Actors: Age flexibility (9(5)) incentivizes best-in-class protection
Section 9 is India's commitment to ensuring that children can be children - even in the digital world.

Comprehensive Legal Interpretation Complete

This interpretation covers Section 9 DPDPA 2023 comprehensively - Processing of Personal Data of Children

 Complete analysis of all five subsections

 UNCRC and children's rights framework

 Developmental psychology foundations

 Constitutional framework (Article 21, 39(f))

 Verifiable parental consent mechanisms

 Detrimental effect analysis (9(2))

 Triple prohibition deep dive (9(3))

 Exemptions and age flexibility explained

 Persons with disability protection

 GDPR & COPPA comparative analysis

 Age-Appropriate Design Code

 50+ practical examples and scenarios

International Data Protection Lawyer | Cyber Law Expert