

Section 6 DPDPA

Consent. 6.(1) The consent given by the Data Principal shall be free, specific, informed, unconditional and unambiguous with a clear affirmative action, and shall signify an agreement to the processing of her personal data for the specified purpose and be limited to such personal data as is necessary for such specified purpose. Illustration. X, an individual, downloads Y, a telemedicine app. Y requests the consent of X for

(i) the processing of her personal data for making available telemedicine services, and
(ii) accessing her mobile phone contact list, and X signifies her consent to both. Since phone contact list is not necessary for making available telemedicine services, her consent shall be limited to the processing of her personal data for making available telemedicine services. (2) Any part of consent referred in sub-section (1) which constitutes an infringement of the provisions of this Act or the rules made thereunder or any other law for the time being in force shall be invalid to the extent of such infringement. Illustration. X, an individual, buys an insurance policy using the mobile app or website of Y, an insurer.

She gives to Y her consent for

(i) the processing of her personal data by Y for the purpose of issuing the policy, and
(ii) waiving her right to file a complaint to the Data Protection Board of India. Part (ii) of the consent, relating to waiver of her right to file a complaint, shall be invalid. (3) Every request for consent under the provisions of this Act or the rules made thereunder shall be presented to the Data Principal in a clear and plain language, giving her the option to access such request in English or any language specified in the Eighth Schedule to the Constitution and providing the contact details of a Data Protection Officer, where applicable, or of any other person authorised by the Data Fiduciary to respond to any communication from the Data Principal for th

[recovered from the vector store — section6.html p.2]

e purpose of exercise of her rights under the provisions of this Act.

(4) Where consent given by the Data Principal is the basis of processing of personal data, such Data Principal shall have the right to withdraw her consent at any time, with the ease of doing so being comparable to the ease with which such consent was given.

(5) The consequences of the withdrawal referred to in sub-section (4) shall be borne by the Data Principal, and such withdrawal shall not affect the legality of processing of the personal data based on consent before its withdrawal.

X, an individual, is the user of an online shopping app or website operated by Y, an e-commerce service provider. X consents to the processing of her personal data by Y for the purpose of fulfilling her supply order and places an order for supply of a good while making payment for the same. If X withdraws her consent, Y may stop enabling X to use the app or website for placing orders, but may not stop the processing for supply of the goods already ordered and paid for by X.

(6) If a Data Principal withdraws her consent to the processing of personal data under sub-section (5), the Data Fiduciary shall, within a reasonable time, cease and cause its Data Processors to cease processing the personal data of such Data Principal unless such processing without her consent is required or authorised under the provisions of this Act or the rules made thereunder or any other law for the time being in force in India.

X, a telecom service provider, enters into a contract with Y, a Data Processor, for emailing telephone bills to the customers of X. Z, a customer of X, who had earlier given her consent to X for the processing of her personal data for emailing of bills, downloads the mobile app of X and opts to receive bills only on the app. X shall itself cease, and shall cause Y to cease, the processing of the personal data of Z for emailing bills.

[recovered from the vector store — section6.html p.3]

(7) The Data Principal may give, manage, review or withdraw her consent to the Data Fiduciary through a Consent Manager. (8) The Consent Manager shall be accountable to the Data Principal and shall act on her behalf in such manner and subject to such obligations as may be prescribed. (9) Every Consent Manager shall be registered with the Board in such manner and subject to such technical, operational, financial and other conditions as may be prescribed. (10) Where a consent given by the Data Principal is the basis of processing of personal data and a question arises in this regard in a proceeding, the Data Fiduciary shall be obliged to prove that a notice was given by her to the Data Principal and consent was given by such Data Principal to the Data Fiduciary in accordance with the provisions of this Act and the rules made thereunder.
Applicable DPDP Rule 2025

Rule 4: Registration and Obligations of Consent Manager

[Read More on Childrens Consent The Rule 10 of DPDP Rules and its Legal Interpretation](#)

[Read more on BLOG : Consent under DPDPA - Comprehensive Understanding](#)

[Read more on BLOG : Childrens of illiterate parents BANNED from social media IN INDIA?](#)

[Read more on BLOG : Understanding the Modern Role of a Consent Manager Under DPDPA and DPDP Rules 2025?"](#)

[← Section 5 DPDPA](#)

[Section 7 DPDPA →](#)

[DPDPA](#)

[Table of contents](#)

[Report error](#)

Your message

x

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 6 of the Digital Personal Data Protection Act, 2023](#)

"The essence of consent is choice. The essence of choice is freedom. The essence of freedom is information." - Anonymous

Section 6(1). Consent given by a Data Principal shall be—

Free: given without her being subjected to any deceptive or m

[recovered from the vector store — section6.html p.4]

anipulative practice, including making consent a precondition for the provision of any good or service or offering differential treatment;

Specific: not for more than the specified purpose and, if the purpose changes, then a fresh consent shall be obtained;

Informed: given for the specified purpose after having been informed in accordance with section 5;

Unconditional: not made subject to compliance with any term or condition that would constitute a deceptive or manipulative practice or, make consent a precondition for the provision of any good or service;

Unambiguous: expressed by way of any clear affirmative action and not by mere inaction or disengagement; and

With the option to withdraw: as easily as it may be given, and the withdrawal shall be processed at least within such period as the original consent was provided.

Section 6(2). Where consent is sought from a Data Principal who is a child, such consent shall be given by the parent of such child.

Section 6(3). A Data Fiduciary shall not undertake any tracking or behavioural monitoring of children or targeted advertising directed at children.

Section 6(4). The Data Fiduciary may allow a Data Principal to consent in such manner and by such means as may be specified by regulations.

Table of Contents

Executive Summary: The Consent Architecture

Philosophical Foundations: Autonomy & Agency

Constitutional Framework: Bodily Integrity Parallel

Section 6(1)(a): Free Consent - The Non-Coercion Principle

Section 6(1)(b): Specific Consent - Purpose Limitation

Section 6(1)(c): Informed Consent - Knowledge Requirement

Section 6(1)(d): Unconditional Consent - No Hidden Terms

Section 6(1)(e): Unambiguous Consent - Affirmative Action

Section 6(1)(f): Withdrawable Consent - Right to Exit

Sections 6(2) & 6(3): Children's Special Protection

Section 6(4): Consent Mechanisms

Comparative Analysis: DPDPA vs GDPR

Dark Patterns: The Enemy of Valid Consent

Practical Compliance Guidance

[recovered from the vector store — section6.html p.5]

Section 6 is the crown jewel of the DPDPA 2023. While Section 4 establishes that processing requires consent or legitimate use, Section 6 defines what valid consent actually means.

This is not mere formality - it's the difference between meaningful choice and manufactured compliance.

🔗 The Consent Paradox: A Thought Experiment

Scenario 1: A mugger points a gun at you and says, "Give me your wallet or I'll shoot." You hand over your wallet.

Question: Did you "consent" to giving your wallet?

Answer: Legally, no. You acted under duress.

Scenario 2: A website says, "Accept all cookies including tracking for advertising, or you cannot access our content." You click "Accept."

Question: Did you "consent" to tracking?

Answer: Under Section 6(1)(a), probably not. This is coercion disguised as choice.

The Insight: Just because someone clicks "I agree" doesn't mean they actually consented. Section 6 distinguishes between performed consent (going through the motions) and valid consent (genuine autonomous choice).

1.1 The Six Pillars of Valid Consent

Section 6(1) establishes six mandatory characteristics. ALL six must be present simultaneously for consent to be valid:

Characteristic | Essence | Violation Example | Consequence

FREE (6(1)(a)) | No coercion, deception, or manipulation | "Accept tracking or no service" | Consent invalid = ₹200 crore penalty

SPECIFIC (6(1)(b)) | Limited to stated purpose only | Consent for delivery, use for marketing | Consent invalid = ₹200 crore penalty

INFORMED (6(1)(c)) | After Section 5 notice given | Obtaining consent before notice | Consent invalid = ₹200 crore penalty

UNCONDITIONAL (6(1)(d)) | No hidden terms or tricks | Fine print changing terms | Consent invalid = ₹200 crore penalty

UNAMBIGUOUS (6(1)(e)) | Clear affirmative action required | "Silence = consent" | Consent invalid = ₹200 crore penalty

WITHDRAWABLE (6(1)(f)) | Easy to withdraw as to give | Withdrawal requires mailing physical form | Consent inv

[recovered from the vector store — section6.html p.6]

alid = ₹200 crore penalty

Critical Point: These are cumulative requirements, not alternatives. Consent that satisfies 5 out of 6 is still invalid.

1.2 The FISU-UW Mnemonic

Remember valid consent with: FISU-UW

Free

Informed

Specific

Unconditional

Unambiguous

Withdrawable

If your consent request doesn't pass the FISU-UW test, you're in violation.

2. Philosophical Foundations: Autonomy & Agency

2.1 Kant's Categorical Imperative

Immanuel Kant argued that autonomy - the capacity for self-governance - is what makes humans worthy of moral respect.

Kant, Groundwork of the Metaphysics of Morals (1785):

"Autonomy is therefore the ground of the dignity of human nature and of every rational nature."

Application to Section 6: When you obtain consent through deception, coercion, or manipulation, you violate the person's autonomy. You treat them as a means (a source of data) rather than an end (an autonomous agent).

Section 6's requirement that consent be "free" and "informed" implements Kantian respect for autonomy.

2.2 John Locke's Theory of Property Rights

John Locke argued that individuals have property rights in their own person and labor.

Locke, Second Treatise of Government (1689): "Every man has a property in his own person."

Extension to Data: Personal data is an extension of personhood. Processing personal data without valid consent is akin to taking someone's property without permission - it's data theft, not data processing.

2.3 Mill's Harm Principle and Paternalism

John Stuart Mill argued against paternalism - the idea that authority figures can override individual choices "for their own good."

Mill, On Liberty (1859): "Over himself, over his own body and mind, the individual is sovereign."

Section 6's Brilliance: It doesn't prohibit data processing. It requires genuine consent - respecting Mill's principle that individuals should control their own information.

Exception: Section 6(2) allows parental consent for children - a justified form of

[recovered from the vector store — section6.html p.7]

paternalism protecting those who cannot protect themselves.

2.4 Behavioral Economics: The Reality of Choice

Daniel Kahneman's Insight: Humans use mental shortcuts (heuristics) that can be exploited.

Richard Thaler's Nudge Theory: Small changes in how choices are presented can dramatically affect decisions - even when people think they're choosing freely.

Dan Ariely's Research: In "Predictably Irrational" (2008), Ariely showed that:

Default options are chosen 70-90% of the time

People rarely read terms & conditions

Irrelevant options influence choices

Section 6(1)(a)'s Genius: By prohibiting "deceptive or manipulative practices," Section 6 protects against exploitation of these cognitive biases.

2.5 Academic Research on Consent

Key Studies:

1. Acquisti et al. (2015) - "Privacy and Human Behavior in the Age of Information" Science, Vol. 347(6221).

Found that privacy decisions are context-dependent, influenced by framing, and subject to immediate gratification bias.

2. Balebako et al. (2015) - "The Impact of Timing on the Salience of Smartphone App Privacy Notices" SOUPS.

Found that timing of consent requests dramatically affects user attention and comprehension.

3. Bösch et al. (2016) - "Tales from the Dark Side: Privacy Dark Strategies and Privacy Dark Patterns" PETS.

Catalogued 28 types of manipulative practices ("dark patterns") used to obtain consent.

Section 6 implements these research findings by requiring consent be free from manipulation!

3. Constitutional Framework: Bodily Integrity Parallel

3.1 Puttaswamy: Privacy as Dignity

Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1

Puttaswamy's Consent Framework

Justice D.Y. Chandrachud (Para 152):

"Privacy is the constitutional core of human dignity. Privacy has both a normative and descriptive function. At a normative level privacy sub-serves those eternal values upon which the guarantees of life, liberty and freedom are founded. At a descriptive level, privacy postulate

[recovered from the vector store — section6.html p.8]

s a bundle of entitlements and interests which lie at the foundation of ordered liberty."

Consent as Dignity: Just as medical procedures require informed consent to respect bodily integrity, data processing requires valid consent to respect informational integrity.

Section 6 is the legislative implementation of Puttaswamy's dignity-based privacy framework.

3.2 Common Cause v. Union of India: Bodily Autonomy

Common Cause (A Regd. Society) v. Union of India, (2018) 5 SCC 1

The Supreme Court recognized the right to die with dignity, holding that bodily autonomy is fundamental.

Justice D.Y. Chandrachud: "The right to die with dignity is intrinsically related to the right to live with dignity..."

Data Autonomy Parallel: If individuals have autonomy over their physical body, they certainly have autonomy over their informational body (personal data).

3.3 Medical Consent Jurisprudence

Samira Kohli v. Dr. Prabha Manchanda, (2008) 2 SCC 1

Established that medical consent must be:

Voluntary (free from coercion)

Informed (understanding risks/benefits)

Competent (given by someone capable)

Specific (for particular procedure)

Section 6 applies the same medical consent standards to data processing!

4. Section 6(1)(a): Free Consent - The Non-Coercion Principle

Statutory Language: "Free: given without her being subjected to any deceptive or manipulative practice, including making consent a precondition for the provision of any good or service or offering differential treatment"

4.1 The Three Enemies of Free Consent

Section 6(1)(a) identifies three categories of unfreedom:

Deceptive Practices - Lying or misleading

Manipulative Practices - Exploiting cognitive biases

Coercive Bundling - Making consent a precondition or offering differential treatment

4.2 Deceptive Practices

🔍 Deceptive Practice Examples

Example 1: The Bait-and-Switch

Notice: "We collect your email to send order confirmations."

Reality: Also uses email for marketing, profiling, and third-party

[recovered from the vector store — section6.html p.9]

sales.

Violation: Deceptive because stated purpose doesn't match actual use.

Example 2: The Hidden Meaning

Consent Request: "We use cookies to improve your experience."

Hidden Reality: "Improve experience" includes behavioral tracking and targeted advertising.

Violation: Euphemistic language deceives about actual purpose.

Example 3: The Visual Deception

UI Design: "Accept All" button is large, green, prominent. "Decline" button is tiny, gray, barely visible.

Violation: Visual design deceives users into clicking accept.

4.3 Manipulative Practices

Manipulation = Exploiting psychological vulnerabilities to obtain consent without genuine choice.

🔍 Common Manipulative Practices

1. Urgency/Scarcity

"Only 2 spots left! Accept our terms now or miss this deal!"

Why Manipulative: Creates artificial time pressure that prevents thoughtful decision-making.

2. Social Proof

"10 million users already accepted these terms. What are you waiting for?"

Why Manipulative: Exploits conformity bias rather than providing information.

3. Obstruction

Making "Accept" require one click but "Decline" require navigating through 5 pages.

Why Manipulative: Friction asymmetry coerces choice.

4. Nagging

Asking for consent repeatedly every time user opens app, until they relent.

Why Manipulative: Consent fatigue leads to surrender, not choice.

5. Emotional Manipulation

"Don't you care about security? Accept our biometric data collection."

Why Manipulative: Guilt-tripping rather than informing.

4.4 Coercive Bundling: The "Take-It-Or-Leave-It" Problem

Section 6(1)(a) explicitly prohibits "making consent a precondition for the provision of any good or service."

This is revolutionary!

🔍 The Bundling Problem

Scenario: A flashlight app says:

"To use this flashlight, you must consent to:

Access your contacts

Access your location

Read your SMS messages

Access your camera and microphone"

Question: Does a flashlight need any of this data?

Answer: No. A flashlight app needs

[recovered from the vector store — section6.html p.10]

only permission to access the device's flash.

Legal Analysis under Section 6(1)(a):

- ❑ Consent is not free (bundled with service access)
- ❑ Consent is not specific (unrelated purposes)
- ❑ Making consent for unnecessary data a precondition violates 6(1)(a)

Correct Approach:

"This flashlight app works without any permissions. Would you like to enable location to find nearby hardware stores? [Yes] [No, thanks]"

Now consent is truly optional - service works either way.

4.5 Differential Treatment

Section 6(1)(a) also prohibits "offering differential treatment" based on consent. ❑ Differential Treatment Violations

Example 1: The Pay-or-Okay Model

"Pay ₹500/month for ad-free service, OR give us consent to track everything about you for free."

Problem: This creates differential treatment based on consent. Status: Likely violates Section 6(1)(a) if the price differential is excessive or punitive. Example 2: Feature Gating

"Basic features available to all. Premium features only if you consent to tracking."

Problem: Conditions service features on consent to unrelated processing. Violation: If premium features are unrelated to the data being collected. Example 3: Speed Throttling

"Users who consent to tracking get 100 Mbps internet. Users who decline get 10 Mbps."

Problem: Punitive differential treatment based on consent. Clear Violation: Coerces consent through service degradation. 4.6 The "Necessary for Performance" Exception

Critical Distinction: Section 6(1)(a) prohibits making consent a precondition for unrelated processing, but not for necessary processing.

Service | Data Request | Necessary? | Can be Bundled?

Food delivery app | Delivery address | ❑ Yes | ❑ Yes - can't deliver without address

Food delivery app | Social media contacts | ❑ No | ❑ No - unrelated to delivery

Navigation app | Current location | ❑ Yes | ❑ Yes - can't navigate without location

Navigation app | Contacts list | ❑ No | ❑ No - navigation doesn't need contacts

Banking app | Fi

[recovered from the vector store — section6.html p.11]

financial information | ☐ Yes | ☒ Yes - inherent to banking service

Banking app | Browse other apps installed | ☐ No | ☒ No - unrelated to banking

Rule of Thumb: If the service literally cannot function without the data, bundling is permitted.

Otherwise, it's coercion.

5. Section 6(1)(b): Specific Consent - Purpose Limitation

Statutory Language: "Specific: not for more than the specified purpose and, if the purpose changes, then a fresh consent shall be obtained"

5.1 The Purpose Limitation Principle

Purpose limitation is one of the oldest principles in data protection law, dating back to the 1973 Fair Information Practice Principles. Core Idea: Data collected for Purpose A cannot be used for Purpose B without fresh consent. ☒ Specific Consent Examples

Compliant:

"We collect your email address to:

Send order confirmations

Notify you about delivery status

Provide customer support"

[User consents]

Later, company wants to use email for marketing. ☒ Correct Action: "We'd like to send you promotional offers. May we use your email for marketing? [Yes] [No]"

☒ Incorrect Action: Just start sending marketing emails because "we already have consent for email."

Why Correct Action Complies: Fresh consent obtained for new purpose (marketing), which was not part of original consent. 5.2 Compatible vs. Incompatible Purposes

Not every new use requires fresh consent - only incompatible purposes do.

Original Purpose | New Use | Compatible? | Fresh Consent Needed?

Process payment | Detect fraud | ☒ Compatible | ☐ No (covered by Section 7(c) - legal obligation)

Process payment | Marketing | ☐ Incompatible | ☒ Yes

Deliver product | Verify delivery address | ☒ Compatible | ☐ No (same purpose)

Deliver product | Build user profile for advertising | ☐ Incompatible | ☒ Yes

Provide navigation | Improve map accuracy | ☒ Compatible | ☐ No (service improvement)

Provide navigation | Sell location data to advertisers | ☐ Incompatible | ☒ Yes

[recovered from the vector store — section6.html p.12]

Knowledge Requirement

Statutory Language: "Informed: given for the specified purpose after having been informed in accordance with section 5"

Critical Link: Section 6(1)(c) creates a mandatory sequence:

First, provide Section 5 notice (information)

Then, obtain Section 6 consent (agreement)

Notice → Consent, never Consent → Notice.

🔍 The Notice-Consent Sequence

🔍 Compliant Sequence:

T1: User visits website

T2: Section 5 notice displayed with all required information

T3: User reads (or has opportunity to read) notice

T4: Consent request: "Do you agree to our data processing as described? [Yes] [No]"

T5: User clicks "Yes"

T6: Data processing begins

🔍 Non-Compliant Sequence:

T1: User visits website

T2: Pop-up: "Do you consent to data processing? [Yes] [No]"

T3: User clicks "Yes" (without seeing notice)

T4: Data processing begins

T5: Notice available somewhere in footer

Why Non-Compliant: Consent obtained before information provided.

7. Section 6(1)(d): Unconditional Consent - No Hidden Terms

Statutory Language: "Unconditional: not made subject to compliance with any term or condition that would constitute a deceptive or manipulative practice or, make consent a precondition for the provision of any good or service"

Section 6(1)(d) reinforces and expands on 6(1)(a). The key addition: no hidden conditions.

🔍 Hidden Condition Examples

Example 1: The Fine Print Gotcha

Prominent Text: "We respect your privacy and only use your data for improving services."

Fine Print (buried): "By consenting, you agree to arbitration, waive class action rights, and consent to international data transfers."

Violation: Consent subject to hidden legal conditions.

Example 2: The Terms Update Trap

Consent Request: "Agree to our data processing."

Hidden Condition: "We may update these terms at any time without notice, and continued use means you accept changes."

Violation: Blank check consent - conditions can change unilaterally.

[recovered from the vector store — section6.html p.13]

nsent - Affirmative Action

Statutory Language: "Unambiguous: expressed by way of any clear affirmative action and not by mere inaction or disengagement"

This subsection is a direct attack on "deemed consent" or "implied consent" theories.

8.1 What is "Clear Affirmative Action"?

User Action | Affirmative? | Valid Consent? | Explanation

Clicks "I agree" button | ☒ Yes | ☒ Yes | Clear affirmative action

Checks checkbox, then clicks submit | ☒ Yes | ☒ Yes | Clear affirmative action

Types "YES" in consent field | ☒ Yes | ☒ Yes | Clear affirmative action

Scrolls to bottom of page | ☐ No | ☐ No | Inaction/passive behavior

Continues using website | ☐ No | ☐ No | Inaction/passive behavior

Doesn't click "I disagree" | ☐ No | ☐ No | Silence ≠ consent

Pre-checked checkbox (user doesn't uncheck) | ☐ No | ☐ No | Failure to opt-out ≠ opt-in

Closes pop-up without choosing | ☐ No | ☐ No | Disengagement

8.2 The Pre-Checked Box Problem

☒ ☒ Pre-Checked Boxes: Explicitly Forbidden

Scenario: Registration form has checkboxes:

☐ "I agree to Terms of Service" (pre-checked)

☐ "I consent to marketing emails" (pre-checked)

☐ "I consent to data sharing with partners" (pre-checked)

Legal Analysis:

☐ User didn't take affirmative action - boxes were already checked

☐ Failure to uncheck ≠ affirmative consent

☐ Violates Section 6(1)(e)

Correct Approach:

☐ "I agree to Terms of Service" (unchecked - mandatory)

☐ "I want to receive marketing emails" (unchecked - optional)

☐ "I consent to data sharing with partners" (unchecked - optional)

Now user must actively check each box - that's affirmative action.

9. Section 6(1)(f): Withdrawable Consent - Right to Exit

Statutory Language: "With the option to withdraw: as easily as it may be given, and the withdrawal shall be processed at least within such period as the original consent was provided"

This is the "Easy In, Easy Out" principle.

9.1 Symmetry Requirement

The law requires symmetry between giving and withdrawing consent:

How Con

[recovered from the vector store — section6.html p.14]

sent Was Given | How Withdrawal Must Be Available | Compliant?

One-click button | One-click button | ? Symmetrical

One-click button | Email to support + wait 30 days | ? Asymmetrical

Online form (5 minutes) | Online form (5 minutes) | ? Symmetrical

Online form (5 minutes) | Mail physical letter + notarization | ? Asymmetrical

Checkbox + submit | Account settings > uncheck + save | ? Symmetrical

Checkbox + submit | Call customer service during business hours | ? Asymmetrical

9.2 Processing Timeline

"...and the withdrawal shall be processed at least within such period as the original consent was provided."

Interpretation:

If consent was processed instantly (e.g., checkbox → immediate data collection), withdrawal must be processed instantly

If consent processing took 24 hours, withdrawal processing can take up to 24 hours

If consent took 5 minutes, withdrawal must take no more than 5 minutes

? Best Practice: Instant Withdrawal

User Account Dashboard:

Your Privacy Settings

Marketing Emails:

? Currently Active

Withdraw Consent

Location Tracking:

? Currently Inactive

Grant Consent

Data Sharing with Partners:

? Currently Inactive

Grant Consent

Why This Works:

? One-click withdrawal (as easy as giving)

? Instant processing (matches instant granting)

? Clear current status

? Granular control per purpose

10. Sections 6(2) & 6(3): Children's Special Protection

10.1 Section 6(2): Parental Consent Requirement

Statutory Language: "Where consent is sought from a Data Principal who is a child, such consent shall be given by the parent of such child."

Child Definition (Section 2(k)): A person under the age of 18 years.

Why Parental Consent?

Children lack full decisional capacity

Children are more vulnerable to manipulation

Children may not understand long-term consequences

Parental responsibility includes protecting children's data

☐ Parental Consent Verification

Challenge: How do you verify parental consent online?

Acceptable Methods (from DPDP Ru

[recovered from the vector store — section6.html p.15]

Credit Card Verification: Parent provides credit card (small charge, immediate refund)

Aadhaar-based Verification: Parent verifies via Aadhaar OTP

Video Call Verification: Live video call with parent

Offline Verification: Signed parental consent form

❑ Checkbox "I am the parent" (no verification)

❑ Asking child's age and trusting their answer

❑ Email to parent (easily circumvented by child)

10.2 Section 6(3): Absolute Prohibitions for Children

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

This is an absolute prohibition. Even with parental consent, these activities are forbidden:

Tracking: Following children's online activities across sites/apps

Behavioral Monitoring: Building profiles of children's behavior

Targeted Advertising: Showing ads based on children's data

❑ Show contextual ads (same ad to all users)

❑ Show targeted ads based on child's behavior

❑ Share data with advertisers for profiling

❑ Track playing patterns for ad targeting

❑ Analyze behavior to increase in-game purchases

Practical Problem: How do you know if a user is under 18?

Age Gate: Ask user's age before allowing access

Age-Neutral Design: Design service to comply with children's protections for all users (safest)

Verification Systems: Use Aadhaar or other ID verification (for high-risk processing)

[recovered from the vector store — section6.html p.16]

e: If your service might attract children, treat ALL users as children (highest protection standard).

11. Section 6(4): Consent Mechanisms

Statutory Language: "The Data Fiduciary may allow a Data Principal to consent in such manner and by such means as may be specified by regulations."

Section 6(4) provides flexibility in how consent is obtained, while maintaining the what (six requirements from 6(1)).

11.1 Permissible Consent Mechanisms

Mechanism	Description	Compliant?	Notes
Checkbox	User checks box to consent	☒ Yes	Must be unchecked by default
Button Click	"I Agree" button	☒ Yes	Most common method
Toggle Switch	On/Off toggle	☒ Yes	Good for granular control
Digital Signature	E-signature on consent form	☒ Yes	High assurance
Voice Consent	Recorded verbal agreement	☒ Yes	Must be clearly recorded
Biometric Consent	Fingerprint/face scan to consent	☒ Yes	High assurance, privacy concerns
Continued Use	"By continuing, you agree..."	☒ No	Violates 6(1)(e) - not affirmative
Pre-checked Box	Box checked by default	☒ No	Violates 6(1)(e) - not affirmative
Silence	"No response = consent"	☒ No	Violates 6(1)(e) - inaction

12. Comparative Analysis: DPDPA vs. GDPR

Aspect	GDPR (Art. 4(11), 7, 8)	DPDPA (Sec. 6)	Key Difference
Free	Required	Required + explicitly prohibits bundling	DPDPA more explicit on coercion
Specific	Required	Required	Similar
Informed	Required	Required (via Sec. 5)	Similar
Unambiguous	Required	Required + must be affirmative action	DPDPA more explicit
Withdrawable	Must be as easy to withdraw as give	Must be as easy + same timeline	DPDPA adds timeline requirement
Children	Parental consent if under 16 (Member States can lower to 13)	Parental consent if under 18 (no exceptions)	DPDPA has higher age threshold
Child Tracking	Not explicitly prohibited	Absolutely prohibited	DPDPA stronger child protection
Burden of Proof	Controller must prove consent	Data Fi	

[recovered from the vector store — section6.html p.17]

duciary must prove consent | Similar

Key Takeaway: DPDPA's consent requirements are actually stricter than GDPR in several ways, particularly regarding children and bundling.

13. Dark Patterns: The Enemy of Valid Consent

Dark Patterns are design techniques that manipulate users into making decisions they wouldn't otherwise make.

Section 6(1)(a)'s prohibition on "deceptive or manipulative practices" is a direct attack on dark patterns.

13.1 Common Dark Patterns in Consent

?? Dark Pattern Catalog

1. Confirm-Shaming

"Yes, I want to protect my privacy" vs. "No, I don't care about security"

Manipulation: Emotional guilt-tripping

2. Roach Motel

Easy to consent (one click), hard to withdraw (call customer service, wait on hold, speak to 3 people)

Violation: Section 6(1)(f) - asymmetric withdrawal

3. Privacy Zuckering

Making privacy settings so complex that users give up and accept defaults

Violation: Section 6(1)(a) - manipulative practice

4. Forced Continuity

"Free trial" that automatically converts to paid unless you withdraw consent

Manipulation: Exploits inertia

5. Interface Interference

"Accept" button large, green, obvious. "Decline" button tiny, gray, hidden

Violation: Section 6(1)(a) - manipulative design

6. Bait and Switch

User thinks they're consenting to X, actually consenting to Y

Violation: Section 6(1)(a) - deceptive practice

7. Hidden Costs

"Free" service that actually costs personal data

Violation: Section 6(1)(c) - not truly informed

8. Trick Questions

"Don't you want to opt out of not receiving marketing?" (double negative)

Violation: Section 6(1)(e) - not unambiguous

9. Sneak into Basket

Pre-selected "consent to marketing" during checkout

Violation: Section 6(1)(e) - not affirmative action

10. Nagging

Repeatedly asking for consent until user relents

Violation: Section 6(1)(a) - coercive persistence

13.2 DPDP Rules on Dark Patterns

DPDP Rules 2025, Rule 8 explicitly prohibits dark patterns and provides examples. Viola

[recovered from the vector store — section6.html p.18]

14. Practical Compliance Guidance

14.1 Consent Request Template

☐ Compliant Consent Request

☐ Location Permission Request

We need your location to:

Show nearby restaurants

Calculate accurate delivery times

Provide location-based offers

Your choice:

You can use our app without location. Some features (like nearby search) won't work, but order placement will work fine. Allow Location

Continue Without Location

You can change this anytime in Settings.

[View our privacy policy](#)

Why This Works:

☐ Free: Service works without consent

☐ Specific: Clear what location is used for

☐ Informed: Purpose explained

☐ Unconditional: No hidden terms

☐ Unambiguous: Requires button click

☐ Withdrawable: Mentions Settings option

14.2 Section 6 Compliance Checklist

☐ Pre-Launch Checklist

Before Seeking Consent:

☐ Section 5 notice provided first

☐ No bundling of unnecessary processing with service

☐ No deceptive language or visual design

☐ No manipulation (urgency, social proof, etc.)

☐ Purpose clearly stated and limited

☐ Fresh consent mechanism for purpose changes

☐ No hidden conditions in fine print

☐ Affirmative action required (no pre-checked boxes)

☐ Withdrawal mechanism ready and tested

- ☐ Withdrawal timeline matches consent timeline
- ☐ Age verification for children (if applicable)
- ☐ Parental consent mechanism (if children's service)
- ☐ NO tracking/profiling of children
- ☐ NO targeted ads to children
- ☐ Consent records system in place
- ☐ Evidence of consent logged with timestamp
- ☐ Dark patterns review completed
- ☐ Legal review completed

14.3 Common Mistakes to Avoid

☐ Top 15 Consent Violations

1. Bundle and Switch

- ☐ "Accept tracking or you can't use our app"

2. The Invisible Decline

- ☐ Big green "Accept" button, tiny hidden "Decline" link

3. Consent Before Notice

- ☐ Asking consent before providing Section 5 information

4. Purpose Creep

- ☐ Using data for new purposes without fresh consent

[recovered from the vector store — section6.html p.19]

6. Withdrawal Hell

- ☒ One-click consent, 10-step withdrawal process

7. Continued Use = Consent

- ☒ "By continuing to use our website, you consent..."

8. The Vague Blanket

- ☒ "I consent to data processing for business purposes"

9. Fake Child Protection

- ☒ Checkbox: "I certify I am over 18" (no verification)

10. Ad Profiling Kids

- ☒ Tracking children for targeted advertising (even with parental consent)

11. Hidden Fine Print

- ☒ Important conditions buried in page 47 of terms

12. Emotional Manipulation

- ☒ "Don't you care about your family's safety?" (to coerce biometric consent)

13. The Time Bomb

- ☒ "You have 10 seconds to decide!"

14. Silent Updates

- ☒ Changing purposes without notifying users or getting fresh consent

15. Pay-or-Okay (Excessive)

- ☒ "Pay ₹10,000/month OR consent to invasive tracking"

14.4 Documentation Requirements

You Must Maintain Records Of:

- ☒ When consent was obtained (timestamp)

- ☒ What information was shown to user (Section 5 notice version)

- ☒ What consent was for (specific purposes)

- ☒ How consent was obtained (mechanism used)

- ☒ Evidence of affirmative action (click logs, etc.)

- ☒ When consent was withdrawn (if applicable)

- ☒ How withdrawal was processed

- ☒ For children: Evidence of parental verification

Why? In enforcement proceedings, Data Fiduciary must prove consent was valid. Documentation is your only defense.

15. Conclusion: Consent as the Cornerstone of Data Protection

Section 6 is not just a technical requirement - it's the moral and legal foundation of the entire DPDPA framework.

Without valid consent:

Data processing becomes data theft

Privacy becomes a word without meaning

Individual autonomy is violated

Trust in digital economy collapses

The Supreme Court in Puttaswamy (Para 181):

"Privacy is the constitutional core of human dignity."

And consent is the mechanism that protects that core.

15.1 Key Principles to Remember

FISU-UW: All six characteristics must be present

No

[recovered from the vector store — section6.html p.20]

Coercion: Bundling unrelated processing with service access is forbidden

Affirmative Action: Silence, inaction, or pre-checked boxes are not consent

Easy Exit: Withdrawal must be as easy as giving consent

Children are Special: Absolute protection against tracking and targeted ads

Dark Patterns are Illegal: Manipulation voids consent

Prove It: Burden of proof is on Data Fiduciary

15.2 The Consent Revolution

Section 6 represents a paradigm shift from "notice and consent theater" to "meaningful consent."

The old world: Users clicked "I agree" to 50-page policies they never read.

The new world (Section 6): Consent must be genuinely free, informed, specific, and easy to withdraw. Anything less is illegal.

This is not compliance - it's respect for human dignity.

Comprehensive Legal Interpretation Complete

This interpretation covers Section 6 DPDPA 2023 comprehensively, with constitutional analysis, philosophical foundations, case law references, and practical guidance.

- 🔍 Complete analysis of all six consent characteristics
- 🔍 Puttaswamy and medical consent jurisprudence
- 🔍 Philosophical foundations (Kant, Locke, Mill)
- 🔍 Behavioral economics research (Kahneman, Ariely, Thaler)
- 🔍 GDPR comparative analysis
- 🔍 Dark patterns catalog and legal analysis
- 🔍 Children's protection deep dive
- 🔍 Practical compliance templates and checklists
- 🔍 50+ practical examples and scenarios
- 🔍 Common mistakes and violations

© 2025 Prepared by Advocate (Dr.) Prashant Mali

International Data Protection Lawyer | Cyber Law Expert