[recovered from the vector store — section4.html p.1]

Section 4 DPDPA

Grounds for Processing Personal Data.

4.(1) A person may process the personal data of a Data Principal only in accordance with the provisions of this Act and for a lawful purpose,—

(a) for which the Data Principal has given her consent; or

(b) for certain legitimate uses.

(2) For the purposes of this section, the expression "lawful purpose" means any purpose which is not expressly forbidden by law.

SCROLL DOWN FOR LEGAL INTERPRETATION

← Section 3 DPDPA

Section 5 DPDPA →

DPDPA
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

Legal Interpretation of
Section 4: Grounds for Processing Personal Data

The Foundational Legal Basis for All Data Processing Activities

Quick Navigation

 FAQs

Statutory Text: Section 4 DPDPA 2023

Section 4. Grounds for processing personal data:

4.(1) A person may process the personal data of a Data Principal only in accordance with the provisions of this Act and for a lawful purpose,—

(a) for which the Data Principal has given her consent; or

(b) for certain legitimate uses.

(2) For the purposes of this section, the expression "lawful purpose" means any purpose which is not expressly forbidden by law.

Understanding Section 4: The Gateway Provision

Section 4 of the Digital Personal Data Protection Act, 2023 is arguably the most foundational provision of the entire legislation. It establishes the fundamental legal principle that governs all personal data processing in India: no processing without a lawful ground.

The Core Principle

[recovered from the vector store — section4.html p.2]

itive obligation regime. Unlike a permissive framework where everything is allowed unless prohibited, the DPDPA establishes that personal data processing is prohibited unless it falls within one of the two specified grounds AND serves a lawful purpose.

This provision represents a paradigm shift in Indian data protection law, moving from sector-specific regulations to a comprehensive, rights-based framework that applies across all sectors and all forms of personal data processing.

Legislative Intent and Policy Objectives

The legislative intent behind Section 4 is multi-fold:

1. Individual Autonomy

Empowering Data Principals with control over their personal data by requiring either their consent or a legitimate justification for processing.

2. Legal Certainty

Providing clear, unambiguous grounds for processing, eliminating interpretive confusion and regulatory arbitrariness.

3. Balance of Interests

Balancing individual privacy rights with legitimate business, governmental, and societal needs through the "legitimate uses" ground.
4. Accountability

Creating an accountability mechanism where Data Fiduciaries must justify their processing activities under one of the specified grounds.

The Two Grounds for Processing

Section 4(1) establishes a binary framework for lawful processing. Every processing activity must fall under one (and only one) of these two grounds:

Ground 1: Consent

Section 4(1)(a)

"for which the Data Principal has given her consent"

Key Characteristics:

Voluntary and informed

Specific to purpose

Freely given

Unambiguous indication

Withdrawable at any time

Typical Use Cases:

Marketing communications

Personalized services

Optional features

Data sharing with third parties

Behavioral analytics

Ground 2: Legitimate Uses

Section 4(1)(b)

"for certain legitimate uses"

Key Characteristics:

Defined in Section 7 of DPDPA

No consent required

Public or institutional interest

Necessary for specified purposes

Subject to safeguards

Typ

[recovered from the vector store — section4.html p.3]

ical Use Cases:

Legal compliance

Government functions

Medical emergencies

Employment relationships

Fraud prevention

⚠️ Critical Compliance Point

Every processing activity must be justified under one of these two grounds. There is no third option, no "implied consent," no "business necessity" outside legitimate uses, and no "industry practice" exception. If your processing doesn't fit into either ground, it is unlawful under DPDPA.

Understanding "Lawful Purpose" - Section 4(2)
Section 4(2) provides a crucial definition that applies to both grounds of processing. It defines "lawful purpose" as:

"any purpose which is not expressly forbidden by law"

Legal Analysis of "Lawful Purpose"

This definition employs a negative formulation—defining lawfulness by what it is NOT rather than what it IS. This approach has significant implications:

The Permissive Interpretation

By defining lawful purpose negatively, Section 4(2) creates a presumption of lawfulness. Unless a specific law expressly forbids a purpose, that purpose is considered lawful for data processing. This is a more liberal approach compared to requiring explicit legal authorization for each purpose.
What Constitutes "Expressly Forbidden by Law"?

Purposes Expressly Forbidden by Law Include:

Criminal Activities | Processing data for committing fraud, identity theft, money laundering, terrorism, or any criminal offense
Prohibited Discrimination | Using data to discriminate based on caste, religion, race, sex in ways prohibited by the Constitution or specific laws
Violating Statutory Prohibitions | Purposes that violate specific prohibitions in laws like IT Act, Indian Penal Code, or sector-specific regulations
Child Safety Violations | Processing children's data in ways forbidden by POCSO Act or child protection laws
Constitutional Violations | Purposes that infringe fundamental rights in ways not saved by reasonable restrictions

Example: Lawful vs. Unlawful Purposes

✅ Lawful Purposes (Not Expressly

[recovered from the vector store — section4.html p.4]

Forbidden):

Marketing: Using email addresses to send promotional content (with consent under Section 4(1)(a))

Credit Scoring: Processing financial data to assess creditworthiness for lending decisions

Personalization: Analyzing browsing behavior to recommend products

Research: Using anonymized health data for medical research (subject to appropriate safeguards)

 Unlawful Purposes (Expressly Forbidden):

Phishing: Collecting banking credentials to commit financial fraud (forbidden under IPC, IT Act)

Illegal Surveillance: Tracking individuals without lawful authority in violation of privacy rights

Caste Discrimination: Using caste data to deny services or employment (forbidden under Constitution and specific laws)

Creating Deepfakes: Processing biometric data to create non-consensual intimate images (forbidden under IT Act Section 66E)

Important Distinction: Lawful Purpose vs. Lawful Ground

Having a "lawful purpose" (Section 4(2)) is necessary but not sufficient.
You must BOTH:

Have a lawful purpose (not expressly forbidden), AND

Have a lawful ground (consent OR legitimate use)

Example: Sending marketing emails may be a lawful purpose (not forbidden), but you still need consent (Section 4(1)(a)) to make the processing lawful. Ground 1: Consent - Section 4(1)(a)

Consent is the primary ground for processing personal data under the DPDPA. When processing is based on consent, the Data Principal exercises their autonomy by making an informed choice about whether to allow the processing. Consent Under DPDPA: Detailed Requirements

While Section 4(1)(a) establishes consent as a ground, Section 6 of DPDPA elaborates on the attributes and requirements of valid consent. For Section 4 purposes, consent must be:

Five Pillars of Valid Consent

1. Free Consent

Given voluntarily, without coercion, deception, or making the service conditional on consent for unrelated processing

2. Informed Consent

Based on clear notice (Section 5) about what data is being collect

[recovered from the vector store — section4.html p.5]

5. Withdrawable Consent

Data Principal can withdraw consent as easily as it was given

When to Use Consent as the Lawful Ground

 Use Consent For

 Marketing and promotional communications

 Optional personalization features

 Sharing data with third parties for non-essential purposes

 Behavioral tracking and profiling

 Processing beyond what's necessary for service delivery

 Cross-border data transfers (where consent is chosen)

 Secondary uses of data not covered by original purpose

 Don't Rely on Consent For

 Core service delivery (use contract performance instead)

 Legal compliance requirements

 Employee data processing (use employment relationship)

 Medical emergencies (use vital interests)

 Fraud prevention and security

 Processing where genuine choice cannot be given

 Government functions and public tasks

Practical Example: E-commerce Platform

Scenario: ShopEasy, an e-commerce platform, processes customer data for various purposes.
 Consent-Based Processing:

Email marketing: Sending promotional offers and new product announcements → Requires consent

Product recommendations: Analyzing purchase history to suggest products → Requires consent

Social media integration: Sharing purchases on social platforms → Requires consent

Third-party analytics: Sharing data with marketing agencies → Requires consent

 Legitimate Use Processing (No Consent Required):

Order processing: Using address and payment details to fulfill orders → Performance of contract

Customer support: Processing queries and complaints → Performance of contract

Fraud detection: Monitoring suspicious transactions → Security and fraud prevention

Tax compliance: Retaining transaction records → Legal obligation

Implementation: ShopEasy provides separate consent

[recovered from the vector store — section4.html p.6]

checkboxes for each consent-based purpose and clearly explains which processing occurs regardless of consent for service delivery.

If consent obtained as the basis for processing under Section 4(1)(a) is invalid (fails to meet Section 6 requirements), the entire processing becomes unlawful. This can result in:

Financial penalties under Section 33 of DPDPA

Requirement to cease processing immediately

Data Principal rights enforcement through Data Protection Board

Ground 2: Legitimate Uses - Section 4(1)(b)

The second ground for processing personal data is "certain legitimate uses" as specified in Section 7 of the DPDPA. This ground recognizes that in many situations, obtaining consent is either impractical, impossible, or would undermine important public or private interests.

Legitimate uses represent a carefully calibrated exception to the consent requirement. They are not a broad "legitimate interest" standard (as in GDPR), but rather a closed list of specific circumstances where processing without consent is justified by law.

Categories of Legitimate Uses (Section 7 DPDPA)
Legitimate Use Category | Description | Examples
State Functions (Section 7(a)) | Processing by the State or instrumentality of State for specified functions, services, benefits, licenses, permits, or certificates | Aadhaar verification, passport issuance, welfare scheme implementation
Legal Rights/Claims (Section 7(b)) | Processing necessary for compliance with any law or for instituting, pursuing, defending legal claims | Litigation records, regulatory filings, statutory record-keeping
Court Orders (Section 7(c)) | Processing for compliance with any judgment, decree, or order of any Court or Tribunal in India | Discovery in litigation, compliance with court-mandated disclosures
Medical Emergency (Section 7(d)) | Processing to

[recovered from the vector store — section4.html p.7]

provide medical treatment or health services during medical emergency | Emergency room treatment, ambulance services, epidemic response
Disaster Response (Section 7(e)) | Processing to respond to any breakdown of public order | Natural disaster relief, public safety during emergencies
Employment (Section 7(f)) | Processing by employer for recruitment, termination, provision of service/benefit, or verification of attendance | Payroll, attendance, performance evaluation, background verification
Safety and Security (Section 7(g)) | Processing for ensuring safety and security, including preventing/detecting unlawful activity and ensuring network security | CCTV surveillance, fraud prevention, cybersecurity monitoring
Business Transfer (Section 7(h)) | Processing for mergers, acquisitions, demergers, or other business restructuring | Due diligence in M&A, asset transfers, corporate reorganizations
Publicly Available (Section 7(i)) | Processing of personal data made publicly available by Data Principal or under any law | Public social media posts, government gazette publications
Other Prescribed Uses (Section 7(j)) | Any other legitimate use as may be prescribed by the Central Government | To be specified in DPDP Rules
Unlike consent (which can be obtained for any lawful purpose), legitimate uses are strictly limited to the categories specified in Section 7. Organizations cannot invoke "business necessity" or "legitimate interest" outside these enumerated categories.

Key Principles for Legitimate Use Processing

Compliance Requirements for Legitimate Uses

Necessity Test: Processing must be genuinely necessary for the legitimate use, not merely convenient or beneficial

Proportionality: Collect only the minimum data required for the specific legitimate use

Purpose Limitation: Data collected under legitimate use cannot be repurposed for other activities

Transparency: While consent is not required, reasonable transparency about processing is still

[recovered from the vector store — section4.html p.8]

Security: Enhanced security measures appropriate to the sensitivity and volume of data

Documentation: Maintain clear records of the legitimate use basis and necessity justification

Review Mechanism: Regularly review whether processing still meets legitimate use criteria

Scenario: CarePlus Hospital receives an unconscious patient in the emergency room at 2 AM.

Processing Under Legitimate Use (Section 7(d) - Medical Emergency):

Patient identification: Checking ID cards, calling emergency contacts

Medical records access: Retrieving past medical history from hospital database

Blood type verification: Processing biometric/health data for treatment

Insurance verification: Contacting insurance provider for coverage confirmation

Medication administration: Recording and administering medications

Why No Consent Required: Medical emergency legitimate use (Section 7(d)) allows processing without consent when obtaining consent is impossible or would delay critical care.

Post-Emergency: Once patient regains consciousness and emergency is over, hospital must obtain consent for:

Sharing medical records with family members

Legitimate Use Boundary: Employment Data Processing
Company: TechCorp India, a software development company with 500 employees

Challenge: Determining which employee data processing requires consent vs. falls under legitimate use

Analysis Under Section 7(f) - Employment:

Recruitment: Processing candidate resumes, conducting background checks

Payroll: Bank account details, PAN, tax information

Attendance: Biometric attendance, work hours tracking

Performance: Work performance reviews, project assignments

Benefits: Health insurance enrollment, provident fund

Termination: Exit formalities, final settlement

Marketing: Using employee testimonials in

[recovered from the vector store — section4.html p.9]

company marketing

Social Events: Sharing personal contact information for unofficial social gatherings

Wellness Programs: Optional health tracking apps or fitness challenges

Alumni Networks: Adding to company alumni database post-employment

References: Providing employment references to third parties

Outcome: TechCorp implemented a dual-track consent system - automatic legitimate use processing for employment essentials, separate consent mechanism for optional/promotional uses.

Key Learning: Section 7(f) covers employment relationship essentials, but extends only to what is reasonably necessary for that relationship. Optional benefits and non-essential uses require consent.

Practical Implementation Examples

Example 1: Fintech Lending Platform - Dual Ground Processing

Company: QuickLoan, a digital lending platform

Processing Activity: Loan application and disbursement
Section 4(1)(b) - Legitimate Use Basis:

Credit Assessment | Processing credit bureau data, bank statements (Section 7(b) - necessary for contract performance)
KYC Verification | Aadhaar, PAN verification (Section 7(b) - legal compliance under PMLA)
Fraud Prevention | Device fingerprinting, IP tracking (Section 7(g) - safety and security)
Legal Records | Retaining loan agreements (Section 7(b) - legal compliance under RBI regulations)

Section 4(1)(a) - Consent Required:

Cross-sell Products | Marketing insurance, investment products via email/SMS
Behavioral Analysis | Tracking app usage patterns for personalization beyond credit assessment
Third-party Sharing | Sharing data with partner merchants for co-branded offers

Compliance Approach: QuickLoan's application clearly separates essential processing (with legitimate use justification) from optional processing (with granular consent checkboxes).

Example 2: EdTech Platform - Student Data Processing

Company: LearnBright, online education platform for K-12 students

Special Consideration: Processing children's data (under 18 years)

□□ Paren

[recovered from the vector store — section4.html p.10]

For children under 18, consent must be obtained from parents/guardians (Section 9 DPDPA). This applies to all consent-based processing under Section 4(1)(a).

Course Delivery: Processing student name, class, academic progress (necessary for service delivery)

Assessment: Recording test scores, assignments (educational contract performance)

Safety: Monitoring for inappropriate content, cyberbullying (Section 7(g) - safety)

Legal Compliance: Maintaining educational records as required by education authorities

Behavioral Tracking: Analyzing learning patterns for personalized recommendations

Video Recording: Recording live class sessions for later viewing

Third-party Tools: Using external assessment or collaboration tools

Marketing: Sending information about additional courses or programs

Implementation: LearnBright requires verified parental consent before enrollment, with separate consent modules for optional features.

Example 3: Social Media Platform - Multiple Processing Purposes

Platform: ConnectIndia, a social networking platform

Complexity: Diverse processing purposes requiring different legal grounds
Processing Activity | Legal Ground | Rationale
Account creation and authentication | Legitimate Use | Necessary for service delivery (contract performance)
Content moderation for illegal content | Legitimate Use | Section 7(b) - legal compliance (IT Act intermediary obligations)
Security monitoring for hacking attempts | Legitimate Use | Section 7(g) - network security
Processing publicly posted content | Legitimate Use | Section 7(i) - made publicly available by Data Principal
Algorithmic feed curation | Consent | Optional personalization feature
Targeted advertising | Consent | Not necessary for service, requires explicit consent
Sharing data with third-party advertisers | Consent | Third-party disclosure requires consent
Location tracking for nearby friends | C

[recovered from the vector store — section4.html p.11]

onsent | Optional feature, sensitive data

Compliance Challenge: ConnectIndia must clearly segregate core platform functions (legitimate use) from optional, consent-based features, ensuring users can opt out of consent-based processing without losing access to essential features.

Case Study 1: HealthTech Startup - Balancing Innovation and Compliance

Company: VitalAI, an AI-powered health monitoring startup

Product: Wearable device and app for continuous health tracking with AI-driven insights

VitalAI initially took a blanket consent approach with a single checkbox: "I agree to VitalAI processing my health data for service delivery, personalization, research, and partner collaborations."

Bundled consent violates specificity requirement (Section 6)

Failed to distinguish between processing grounds under Section 4(1)(a) and (b)

Unclear lawful purpose for each processing activity

No clear mechanism for granular consent withdrawal

 Legitimate Use Processing (No Consent):

Device Functionality: Heart rate, steps, sleep tracking for displaying personal health metrics (necessary for device function)
Safety Alerts: Abnormal heart rate detection and emergency notifications (Section 7(d) - medical emergency prevention)

Device Security: User authentication, device pairing (Section 7(g) - security)

 Consent-Based Processing (Granular Consent):

AI Health Insights: "Allow VitalAI to analyze your health data using AI to provide personalized health recommendations" (separate consent)

Research Use: "Contribute anonymized health data to medical research studies" (separate consent)

Healthcare Provider Sharing: "Share health data with your doctor through our Doctor Connect feature" (separate consent with specific doctor selection)

Insurance Integration: "Share fitness data with insurance partners for premium discounts" (separate consent)

[recovered from the vector store — section4.html p.12]

8% of users enabled AI insights (high opt-in when consent is genuine)

Only 23% opted into insurance sharing (demonstrating importance of granular consent)

Zero compliance issues in first year post-implementation

Key Learning: Distinguishing between legitimate use and consent-based processing, with granular consent options, actually improves user experience and trust while ensuring compliance.

Case Study 2: Retail Chain - CCTV Surveillance Legal Basis Challenge

Company: MegaMart, a large retail chain with 200 stores across India

Issue: Determining lawful ground for CCTV surveillance and facial recognition

CCTV Recording: Continuous video surveillance in stores

Facial Recognition: Identifying known shoplifters

Customer Analytics: Analyzing foot traffic patterns, dwell time

Marketing Use: Creating customer personas based on demographics

Ground: Legitimate Use - Section 7(g) (safety and security)

Rationale: Theft prevention, staff safety, incident investigation

Requirements: Clear signage informing about CCTV surveillance, retention limited to 90 days unless needed for investigation

 Activity 2: Facial Recognition for Security
Ground: Legitimate Use - Section 7(g) (preventing unlawful activity)

Rationale: Identifying known shoplifters, preventing repeat theft

Requirements: Database limited to individuals with proven shoplifting history, regular review and deletion, heightened security measures for biometric data

Ground: Consent Required - Section 4(1)(a)

Rationale: Foot traffic analysis and dwell time tracking go beyond security necessity and constitute business analytics

Requirements: Cannot rely on legitimate use; must obtain explicit consent or use anonymized data that doesn't identify individuals

[recovered from the vector store — section4.html p.13]

ired - Section 4(1)(a)

Rationale: Using CCTV footage to infer customer demographics for marketing is not a legitimate use

Alternative: Use voluntary surveys or loyalty program data with consent instead

Final Implementation: MegaMart maintains CCTV under Section 7(g), implements clear signage, limits facial recognition to security purposes only, and abandoned plans for marketing analytics using CCTV data without explicit consent.

Key Learning: Section 7(g) safety and security legitimate use is narrowly construed—it covers genuine security needs but doesn't extend to business intelligence or marketing purposes.

Case Study 3: Government Digital Service - Public Function Data Processing

Agency: State Transport Department's DigiDL portal (Digital Driving License)

Objective: Digitization of driving license application and renewal process

Processing Activities:

Collecting applicant personal data (name, DOB, address, photo)

Biometric verification (fingerprints)

Medical fitness certificates

Verification of supporting documents

Integration with traffic violation database

SMS notifications for application status

Section 4 Analysis for Government Processing:
Section 7(a) - State Functions

ALL core processing activities fall under Section 7(a) as they are for "issuance of license or permit" - an expressly enumerated State function.

Implication: No consent required from applicants for any data processing necessary for license issuance.

However, Transparency Required:

While Section 7(a) eliminates consent requirement, Section 8 still requires:

Clear privacy notice explaining what data is collected and why

Data accuracy obligations

Security safeguards

Retention limitations (data retained only as long as license is valid + statutory period)

Consent Still Required For:

Optional Services: Using biometric data for Aadhaar-based authentication (if made optional)

Third-party Sharing: Sharing license data with insurance companies for premium verification

Value-

[recovered from the vector store — section4.html p.14]

added Services: Sending promotional messages about safe driving courses

Implementation Approach: DigiDL portal displays clear notice that data collection is for license issuance (State function, no consent needed), but provides separate opt-in checkboxes for optional services. Key Learning: Government processing under Section 7(a) is broad for enumerated State functions, but doesn't extend to optional or commercial activities. Compliance Framework: Implementing Section 4

Step-by-Step Compliance Methodology

Step 1: Data Mapping

Inventory all personal data processing activities across your organization - what data, from whom, for what purpose, how long retained

Step 2: Purpose Classification

For each processing activity, clearly define and document the specific purpose. Ensure each purpose is lawful (not expressly forbidden by law)

Step 3: Ground Determination

Determine whether each processing activity falls under consent (Section 4(1)(a)) or legitimate use (Section 4(1)(b)). Document the rationale

Step 4: Mechanism Design

For consent-based processing: Design compliant consent mechanisms.
For legitimate use: Document necessity justification and implement appropriate safeguards

Step 5: Documentation

Create and maintain comprehensive records of processing activities, legal grounds, consent records, and compliance assessments

Step 6: Ongoing Review

Regularly review processing activities, legal grounds, and compliance status. Update as business operations evolve

Decision Tree: Choosing the Right Legal Ground

Section 4 Legal Ground Decision Framework

 Question 1: Is the purpose expressly forbidden by law?

→ If YES: Processing is unlawful regardless of ground (STOP)

→ If NO: Proceed to Question 2

 Question 2: Does it fall under Section 7 legitimate uses?

→ If YES: Check if processing is NECESSARY for that legitimate use

- If necessary: Use Section 4(1)(b) - Legitimate Use
- If not necessary: Proceed to Question 3

→ If NO: Proceed to Question 3

[recovered from the vector store — section4.html p.15]

Question 3: Can you obtain valid consent?

→ If YES: Use Section 4(1)(a) - Consent (ensure compliance with Section 6)

→ If NO: Processing is not permissible under DPDPA (STOP)

If there's significant power imbalance (employer-employee, government-citizen), consent may not be freely given. Prefer legitimate use if available.

Pitfall 1: "Implied Consent" or "Deemed Consent"

Issue: Assuming that use of service implies consent for all processing

Why it fails: Section 6 requires explicit, unambiguous consent. Continued use of service doesn't equal consent for processing beyond what's necessary for service delivery

Compliant approach: Obtain explicit consent for optional processing; rely on legitimate use for essential processing

Pitfall 2: Overreliance on Legitimate Use

Issue: Stretching legitimate use categories to avoid seeking consent

Why it fails: Legitimate uses are narrowly construed and require genuine necessity

Example of abuse: Claiming "safety and security" (Section 7(g)) as ground for marketing analytics

Compliant approach: Use legitimate use only when genuinely necessary; obtain consent for optional or business-oriented processing
Issue: Making service access conditional on consent for unrelated processing

Example: "Accept all cookies and marketing emails or you cannot create an account"

Why it fails: Violates "freely given" requirement of consent (Section 6)

Compliant approach: Separate essential processing (legitimate use) from optional processing (granular consent)

Issue: Using data collected for one purpose for a different purpose without fresh legal ground

Example: Collecting email for order confirmation, later using it for marketing without new consent

Why it fails: Violates purpose limitation principle; new purpose requires new legal ground

Compliant approach: Either seek fresh consent for new purpose or anony

[recovered from the vector store — section4.html p.16]

Section 4 Compliance Checklist

Comprehensive data inventory completed with all processing activities documented

Each processing activity mapped to specific, lawful purpose

Legal ground (consent or legitimate use) determined and documented for each activity

For consent-based processing: Compliant consent mechanisms implemented per Section 6

For legitimate use processing: Necessity justification documented and reviewed

Purpose limitation controls in place to prevent purpose creep

Granular consent options provided (no bundled consent for unrelated purposes)

Clear separation between essential and optional processing

Privacy notices accurately reflect legal grounds for processing

Consent withdrawal mechanisms as easy as consent grant

Regular audits scheduled to review continued validity of legal grounds

Training provided to relevant staff on Section 4 requirements

Incident response procedures account for processing without valid legal ground

Documentation maintained for demonstrating compliance to Data Protection Board

Integration with Other DPDPA Provisions

Section 3 | Obligations of Data Fiduciary - Section 4 grounds must be established before any obligations arise
Section 5 | Notice - Required before seeking consent under Section 4(1)(a)

Section 6 | Consent - Elaborates attributes of valid consent for Section 4(1)(a) processing

Section 7 | Legitimate Uses - Defines specific legitimate uses referenced in Section 4(1)(b)

Section 8 | General Obligations - Apply to all processing regardless of legal ground

Section 11 | Rights of Data Principal - Must be respected for all Section 4 compliant processing

Section 33 | Penalties - Processing without valid Section 4 ground triggers penalty provisions

Frequently Asked Questions

Q1: Can I use both grounds (consent and legitimate use) for the same processing activity?

Answer: No. Each processing activity should rely on ONE legal ground. You

[recovered from the vector store — section4.html p.17]

cannot use legitimate use as a "backup" if consent is withdrawn. Choose the appropriate ground based on the nature and necessity of processing.

Exception: Different aspects of a broader activity may use different grounds. For example, account creation (legitimate use for authentication) and personalized recommendations (consent for analytics).

Q2: What happens if I relied on legitimate use but later realize consent was needed?

Answer: This is a serious compliance issue. You should:

Immediately cease the processing activity

Conduct a compliance audit to identify extent of non-compliance

Obtain valid consent from affected Data Principals before resuming

Consider voluntary disclosure to Data Protection Board if breach is significant

Review all other legitimate use processing to prevent similar issues

Preventive Measure: Always conduct legal ground assessment before commencing new processing activities.

Q3: Does Section 4 apply to processing of publicly available data?

Answer: Yes, Section 4 applies, BUT Section 7(i) provides a legitimate use ground for data "made publicly available by the Data Principal."
Only applies to data the Data Principal themselves made public (not data made public by others)

Processing must respect the context in which data was made public

Doesn't permit scraping data for purposes incompatible with original disclosure

General data protection principles (accuracy, security, retention) still apply

Example: Can process public social media posts for sentiment analysis, but cannot create detailed private profiles for sale to third parties.

Q4: How do I determine if a purpose is "expressly forbidden by law"?

Answer: A purpose is expressly forbidden if:

Criminal law: Purpose constitutes or facilitates a crime (fraud, theft, criminal intimidation)

Statutory prohibition: Specific law prohibits the activity (e.g., discriminatory profiling forbidden by anti-discrimination laws)

[recovered from the vector store — section4.html p.18]

e infringes fundamental rights without justifiable restriction

Sectoral regulation: Industry-specific law prohibits the purpose (e.g., SEBI forbidding certain uses of insider information)

Not "expressly forbidden": Purposes that are merely unethical, controversial, or commercially disadvantageous but not legally prohibited.

Best Practice: When in doubt, seek legal counsel for purposes involving sensitive data or novel use cases.

Q5: Can I process children's data under legitimate use without parental consent?

Answer: Yes, BUT with important caveats:
Section 9 Interaction: Section 9 requires verifiable parental consent for processing children's data, BUT this applies only to consent-based processing under Section 4(1)(a). Legitimate use processing (Section 4(1)(b)) of children's data:

Does NOT require parental consent

Must genuinely fall within Section 7 legitimate use categories

Requires enhanced safeguards appropriate to child data

Must serve the child's best interests where applicable

Example: School processing student data for educational administration (Section 7 - necessary for service delivery) doesn't require parental consent, but school offering optional personalization features (consent-based) does require parental consent. Q6: What if consent is withdrawn - can I continue processing under legitimate use?

Answer: No. This is a critical compliance error called "ground switching."

The Rule: If you chose consent as the legal ground and consent is withdrawn, you MUST stop processing. You cannot retroactively claim legitimate use as an alternative ground. Why: The choice of legal ground must be made upfront based on the nature and necessity of processing.
Legitimate use requires genuine necessity, not just business preference. Allowing ground switching would undermine consent's value. Proper Approach: If processing serves dual purposes (e.g., fraud prevention AND marketing), clearly separate them from the start - use legitimate use for fraud prev

[recovered from the vector store — section4.html p.19]

ention, consent for marketing. Then withdrawal of marketing consent doesn't affect fraud prevention processing. Q7: How does Section 4 apply to cross-border data transfers?

Answer: Section 4 establishes the grounds for processing, including cross-border transfers. However:

For Consent-Based Transfers (Section 4(1)(a)):

Consent must specifically cover the cross-border transfer

Notice must identify recipient countries/regions

Data Principal must understand implications of transfer

For Legitimate Use Transfers (Section 4(1)(b)):

Transfer must be necessary for the legitimate use purpose

Example: Transferring employee data to foreign parent company for payroll (Section 7(f) employment)

Additional Requirements: Cross-border transfers may be subject to additional restrictions or requirements under Section 16 and future rules.
Summary: Section 4 at a Glance

 Core Principle

All personal data processing requires BOTH a lawful purpose AND one of two legal grounds (consent or legitimate use)

 Binary Framework

Only two grounds: Consent (Section 4(1)(a)) or Legitimate Uses (Section 4(1)(b)) - no third option exists

 Lawful Purpose

Defined negatively: any purpose not expressly forbidden by law is lawful (permissive approach)

 Closed List

Legitimate uses are limited to categories in Section 7 - cannot be expanded by interpretation

 Key Takeaway: Section 4 is the gateway provision that must be satisfied before any personal data processing. Without a valid legal ground under Section 4, all processing is unlawful regardless of how well other DPDPA requirements are met. Organizations must conduct rigorous legal ground assessments for each processing activity and document their compliance with Section 4's dual requirements: lawful purpose + appropriate legal ground. Related Provisions

Section 7: Certain Legitimate Uses →

Detailed enumeration of legitimate use categories

 Disclaimer

This interpretation is provided for educational and informational purpose

[recovered from the vector store — section4.html p.20]

s only and does not constitute legal advice. While every effort has been made to ensure accuracy, the Digital Personal Data Protection Act, 2023, and the DPDP Rules, 2025, are subject to interpretation by competent authorities and courts. Organizations should consult qualified legal counsel for specific compliance guidance tailored to their operations. Section 4 requirements may evolve through regulatory guidance, judicial interpretation, and amendments. The author and DPDPA.com assume no liability for actions taken based on this information.