

7. A Data Fiduciary may process personal data of a Data Principal for any of following uses, namely:—

(a) for the specified purpose for which the Data Principal has voluntarily provided her personal data to the Data Fiduciary, and in respect of which she has not indicated to the Data Fiduciary that she does not consent to the use of her personal data. Illustrations.
(I) X, an individual, makes a purchase at Y, a pharmacy. She voluntarily provides Y her personal data and requests Y to acknowledge receipt of the payment made for the purchase by sending a message to her mobile phone. Y may process the personal data of X for the purpose of sending the receipt. (II) X, an individual, electronically messages Y, a real estate broker, requesting Y to help identify a suitable rented accommodation for her and shares her personal data for this purpose. Y may process her personal data to identify and intimate to her the details of accommodation available on rent. Subsequently, X informs Y that X no longer needs help from Y. Y shall cease to process the personal data of X;
(b) for the State and any of its instrumentalities to provide or issue to the Data Principal such subsidy, benefit, service, certificate, licence or permit as may be prescribed, where--

(i) she has previously consented to the processing of her personal data by the State or any of its instrumentalities for any subsidy, benefit, service, certificate, licence or permit; or

(ii) such personal data is available in digital form in, or in non-digital form and digitised subsequently from, any database, register, book or other document which is maintained by the State or any of its instrumentalities and is notified by the Central Government,

subject to standards followed for processing being in accordance with the policy issued by the Central Government or any law for the time being in force for governance of personal data

[recovered from the vector store — section7.html p.2]

X. a pregnant woman, enrolls herself on an app or website to avail of government's maternity benefits programme, while consenting to provide her personal data for the purpose of availing of such benefits. Government may process the personal data of X processing to determine her eligibility to receive any other prescribed benefit from the government;

(c) for the performance by the State or any of its instrumentalities of any function under any law for the time being in force in India or in the interest of sovereignty and integrity of India or security of the State;

(d) for fulfilling any obligation under any law for the time being in force in India on any person to disclose any information to the State or any of its instrumentalities, subject to such processing being in accordance with the provisions regarding disclosure of such information in any other law for the time being in force;

(e) for compliance with any judgment or decree or order issued under any law for the time being in force in India, or any judgment or order relating to claims of a contractual or civil nature under any law for the time being in force outside India;

(f) for responding to a medical emergency involving a threat to the life or immediate threat to the health of the Data Principal or any other individual;

(g) for taking measures to provide medical treatment or health services to any individual during an epidemic, outbreak of disease, or any other threat to public health;

(h) for taking measures to ensure safety of, or provide assistance or services to, any individual during any disaster, or any breakdown of public order.

Explanation.—For the purposes of this clause, the expression “disaster” shall have the same meaning as assigned to it in clause (d) of section 2 of the Disaster Management Act, 2005; or

(i) for the purposes of employment or those related to safeguarding the employer from loss or liability, such as prev

[recovered from the vector store — section7.html p.3]

ention of corporate espionage, maintenance of confidentiality of trade secrets, intellectual property, classified information or provision of any service or benefit sought by a Data Principal who is an employee.

Applicable DPDP Rule 2025

Rule 7: Notice given by Data Fiduciary to Data Principal

← Section 6 DPDP

Section 8 DPDP →

DPDP

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 7 of the Digital Personal Data Protection Act, 2023

"Privacy is not for sale, and human rights should not be compromised out of fear or greed." - Edward Snowden

Section 7 - Certain Legitimate Uses

Statutory Text

Section 7. A Data Fiduciary may process personal data of a Data Principal for any of following purposes, namely:—

Voluntary Provision: For the specified purpose for which the Data Principal has voluntarily provided her personal data to the Data Fiduciary and in respect of which she has not indicated that she does not consent to the use of her personal data.

State Benefits: For the State and any of its instrumentalities to provide or issue to the Data Principal such subsidy, benefit, service, certificate, licence or permit as may be prescribed, where—

(i) she has previously consented to the processing of her personal data by the State or any of its instrumentalities for any subsidy, benefit, service, certificate, licence or permit; or

(ii) such personal data is available in digital form in, or in non-digital form and digitised subsequently from, any database, register, book or other document which is maintained by the State or any of its instrumentalities and is notified by the Central Government.

State Functions: For the performance by the State or any of its instrumentalities of any function under any law for t

[recovered from the vector store — section7.html p.4]

he time being in force in India or in the interest of sovereignty and integrity of India or security of the State. Legal Disclosure: For fulfilling any obligation under any law for the time being in force in India on any person to disclose any information to the State or any of its instrumentalities, subject to such processing being in accordance with the provisions regarding disclosure of such information in any other law for the time being in force. Judicial Compliance: For compliance with any judgment or decree or order issued under any law for the time being in force in India, or any judgment or order relating to claims of a contractual or civil nature under any law for the time being in force outside India. Medical Emergency: For responding to a medical emergency involving a threat to the life or immediate threat to the health of the Data Principal or any other individual. Public Health: For taking measures to provide medical treatment or health services to any Data Principal during an epidemic, outbreak of disease or any other threat to public health.

Disaster Management: For taking measures to ensure safety of, or provide assistance or services to, any Data Principal during any disaster or any breakdown of public order. Employment: For the purposes of employment or those related to safeguarding the employer from loss or liability, such as prevention of corporate espionage, maintenance of confidentiality of trade secrets, intellectual property, classified information or provision of any service or benefit sought by a Data Principal who is an employee. Table of Contents

Executive Summary: The Consent-Privacy Dialectic

Philosophical Foundations: Social Contract Theory

Constitutional Framework: Puttaswamy Judgment

Section 7(a): Voluntary Provision Analysis

Section 7(b): State Benefits and Digital Welfare

Section 7(c): State Functions and Sovereignty

Section 7(d): Legal Disclosure Obligations

[recovered from the vector store — section7.html p.5]

Section 7 of the Digital Personal Data Protection Act, 2023 represents the legislative answer to perhaps the most profound question in modern data protection law: When can personal data be processed without explicit consent?

As the ancient Greek philosopher Heraclitus observed, "The only constant in life is change." Section 7 acknowledges that in our dynamic digital society, requiring explicit consent for every data processing activity would create an impossibly rigid framework that would:

Paralyze emergency response systems during medical crises

Cripple government welfare delivery mechanisms

Make employment relationships administratively unworkable

Prevent law enforcement from functioning effectively

🔍 The Consent Conundrum: A Philosophical Thought Experiment

Imagine if every time a paramedic needed to check your medical records during a heart attack, they first had to obtain your written consent. Or picture a scenario where firefighters rescuing you from a burning building must first ask permission to access your apartment's floor plan.

The absurdity is obvious, yet it illustrates Section 7's fundamental principle: Some processing activities are so inherently necessary, legitimate, or time-critical that requiring consent would be counterproductive, impractical, or even dangerous. "The reasonable man adapts himself to the world: the unreasonable one persists in trying to adapt the world to himself. Therefore all progress depends on the unreasonable man." - George Bernard Shaw

Section 7 is the DPDPA's "reasonable" provision - acknowledging that absolute consent requirements would be "unreasonable" in certain contexts.

1.1 Key Characteristics of Section 7

Closed List (Not Open-Ended): Un

[recovered from the vector store — section7.html p.6]

like GDPR's Article 6(1)(f) "legitimate interests" which requires a balancing test, Section 7 provides a numerus clausus (closed list) of precisely nine categories. This approach reflects the civil law tradition rather than common law's more flexible approach. No Balancing Test Required: If your processing falls within one of the nine categories, you don't need to conduct an elaborate balancing exercise between your interests and the Data Principal's rights. The legislature has already performed that balancing act. Necessity Still Applies: Just because processing falls within Section 7 doesn't mean you can process any data you want. The processing must still be necessary for the specified purpose.

1.2 The Nine Pathways to Consent-Free Processing

Subsection | Category | Primary Beneficiary | Typical Use Cases

7(a) | Voluntary Provision | Private Sector | E-commerce receipts, Real estate enquiries

7(b) | State Benefits | Government | Aadhaar-based welfare, Digital certificates

7(c) | State Functions | Government | National security, Law enforcement

7(d) | Legal Disclosure | Both | Tax compliance, Regulatory reporting

7(e) | Judicial Compliance | Both | Court orders, Arbitral awards

7(f) | Medical Emergency | Healthcare | ER treatment, Unconscious patients

7(g) | Public Health | Healthcare | Contact tracing, Vaccination drives

7(h) | Disaster Management | Emergency Services | Natural disasters, Rescue operations

7(i) | Employment | Private Sector | HR management, Trade secret protection

2. Philosophical Foundations: Social Contract Theory

To truly understand Section 7, we must first grapple with a fundamental philosophical question that has occupied legal theorists since the Enlightenment: What is the proper relationship between individual autonomy and collective good?

2.1 The Social Contract and Data Processing

Thomas Hobbes, in *Leviathan* (1651), argued that individuals surrender certain freedoms to the sovereign in exchange for security and order. Jean-Jacque

[recovered from the vector store — section7.html p.7]

s Rousseau later refined this in The Social Contract (1762), proposing that legitimate political authority requires the consent of the governed.

Section 7 represents a modern incarnation of this social contract theory in the data protection context:

🔗 The Data Protection Social Contract

We, the Data Principals, agree that:

In emergencies (medical, disaster), our privacy can be breached to save lives

The State may process our data to deliver welfare benefits efficiently

Our employers may monitor certain activities to protect legitimate business interests

Courts may order disclosure to ensure justice

In exchange, we expect:

Such processing to be strictly necessary and proportionate

Appropriate safeguards against abuse

Accountability and transparency from Data Fiduciaries

Judicial oversight and remedies for violations

"Man is born free, and everywhere he is in chains. Those who think themselves the masters of others are indeed greater slaves than they." - Jean-Jacques Rousseau

Section 7's genius lies in acknowledging that sometimes we must accept certain "chains" (restrictions on absolute privacy) to prevent greater slavery (chaos, inefficiency, inability to deliver essential services).

2.2 Kant's Categorical Imperative

Immanuel Kant's famous Categorical Imperative asks: "Act only according to that maxim whereby you can, at the same time, will that it should become a universal law."

Applied to Section 7: Would we want to live in a world where:

Paramedics cannot access medical records during emergencies? (Section 7(f))

Police cannot investigate crimes effectively? (Section 7(c))

Governments cannot deliver welfare efficiently? (Section 7(b))

Employers cannot protect trade secrets? (Section 7(i))

The answer is clearly "no" - which justifies these legitimate uses as ethical imperatives, not just legal permissions.

2.3 Utilitarian Calculus

Jeremy Bentham and John Stuart Mill's utilitarianism provides another lens. Mill wrote in On Liberty (1859): "Th

[recovered from the vector store — section7.html p.8]

e only purpose for which power can be rightfully exercised over any member of a civilized community, against his will, is to prevent harm to others."

Section 7 embodies this principle - processing without consent is permitted only when necessary to prevent harm or deliver essential services.

Benefit to Society (lives saved, welfare delivered, justice administered) > Cost to Individual Privacy (temporary processing without explicit consent)

2.4 Academic Research on Consent Fatigue

Modern research validates Section 7's approach. Key studies include:

1. Adjerid et al. (2013) - "Sleights of Privacy: Framing, Disclosures, and the Limits of Transparency" in Proceedings of the Ninth Symposium on Usable Privacy and Security (SOUPS). Found that users suffer from "consent fatigue" - when faced with too many consent requests, they stop reading them carefully.
2. Acquisti & Grossklags (2005) - "Privacy and Rationality in Individual Decision Making" IEEE Security & Privacy, 3(1), 26-33. Demonstrated that individuals systematically misunderstand privacy risks and make irrational decisions when providing consent.
3. Barocas & Nissenbaum (2014) - "Big Data's End Run around Procedural Privacy Protections" Communications of the ACM, 57(11), 31-33. Argued that notice-and-consent regimes are fundamentally broken in the big data era.

Section 7's Lesson: When consent becomes meaningless due to overuse, alternative legal bases become not just permissible but necessary for a functional data protection regime.

3. Constitutional Framework: The Puttaswamy Judgment

Section 7 cannot be understood without reference to the landmark judgment in Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1, where the Supreme Court of India declared privacy a fundamental right under Article 21 of the Constitution.

3.1 The Puttaswamy Three-Prong Test

The Supreme Court held that any infringement of the right to privacy must meet three criteria:

?? The Constitutional Trinity: Puttaswa

[recovered from the vector store — section7.html p.9]

1. LEGALITY - The action must be sanctioned by law

☐ Section 7 satisfies this - it's part of a democratically enacted statute

2. LEGITIMATE AIM - The action must pursue a legitimate state aim

☐ Section 7's purposes (medical emergencies, public health, state functions) are textbook legitimate aims

3. PROPORTIONALITY - The means must be proportionate to the objective

? This is where Section 7 requires careful application

Relevant Extract from Puttaswamy (Para 180, Justice Chandrachud):

"An invasion of life or personal liberty must meet the three-fold requirement of (i) legality, which postulates the existence of law; (ii) need, defined in terms of a legitimate state aim; and (iii) proportionality which ensures a rational nexus between the objects and the means adopted to achieve them."

3.2 Proportionality Doctrine

The proportionality test has deep roots in German constitutional law (Verhältnismäßigkeitsprinzip), refined by the Federal Constitutional Court over decades. It comprises four sub-tests:

Legitimate Aim - Is the objective important enough?

Suitability - Does the measure actually advance the objective?

Necessity - Is there no less intrusive alternative?

Proportionality Stricto Sensu - Do benefits outweigh harms?

☐ Proportionality Example: Hospital Processing Under Section 7(f)

Scenario: Unconscious patient arrives at ER after car accident. Hospital wants to access medical records.

Legitimate Aim: ☐ Saving patient's life (Section 7(f) - medical emergency)

Suitability: ☐ Accessing medical records (allergies, blood type, existing conditions) directly helps treatment

Necessity: ☐ Patient is unconscious; cannot provide consent; no time for delays

Proportionality S.S.: ☐ Benefit (potentially saving life) vastly outweighs cost (temporary access to health records)

Conclusion: Processing is constitutional and lawful under Section 7(f). Counter-Example (FAILS test): Same hospital wants to access patient's social m

[recovered from the vector store — section7.html p.10]

edia history and shopping preferences "just in case it's relevant." This FAILS necessity (not required for treatment) and proportionality.

3.3 Indian Case Law Post-Puttaswamy

Justice K.S. Puttaswamy (Retd.) v. Union of India, (2019) 1 SCC 1 (Aadhaar Validation): While upholding Aadhaar's validity, the Court imposed strict conditions. Relevant for Section 7(b) - State benefits.

Key holdings:

Aadhaar cannot be made mandatory for bank accounts, mobile phones

Private entities cannot demand Aadhaar (except for Section 7(b) welfare delivery)

Purpose limitation strictly enforced - data collected for one benefit cannot be used for unrelated purposes without consent

Navtej Singh Johar v. Union of India, (2018) 10 SCC 1: While primarily about LGBTQ+ rights, the judgment reinforced that privacy protections extend to all aspects of personal autonomy.

4. Section 7(a): Voluntary Provision - The Implied Consent Paradox

Statutory Text: "For the specified purpose for which the Data Principal has voluntarily provided her personal data to the Data Fiduciary and in respect of which she has not indicated that she does not consent to the use of her personal data."

4.1 The Three Elements of Section 7(a)

❓ Dissecting Section 7(a): Three Essential Elements

Element 1: VOLUNTARY PROVISION

The Data Principal must affirmatively provide data to the Data Fiduciary. This excludes:

Data scraped from public sources

Data inferred or derived (e.g., credit scores, psychometric profiles)

Data obtained from third parties

Element 2: SPECIFIED PURPOSE

The purpose must be clear and specific at the time of provision. Vague purposes like "business operations" or "improving services" won't suffice.

Element 3: NO INDICATED OBJECTION

The Data Principal must not have explicitly said "don't use my data for this purpose." Note the double-negative construction - it's an opt-out mechanism, not opt-in.

4.2 Official Illustrations from DPDPA

Illustration I (Pharmacy Receipt):

"X, an individual, ma

[recovered from the vector store — section7.html p.11]

kes a purchase at Y, a pharmacy. She voluntarily provides Y her personal data and requests Y to acknowledge receipt of the payment made for the purchase by sending a message to her mobile phone. Y may process the personal data of X for the purpose of sending the receipt."

- ☐ Voluntary: X affirmatively provides phone number
- ☐ Specified Purpose: Sending payment receipt (clear and narrow)
- ☐ No Objection: X's request implies she wants this processing
- ☐ Use phone number for marketing/promotional SMS
- ☐ Share phone number with third-party advertisers
- ☐ Build customer profile linking purchases to demographics
- ☐ Use number for loyalty program enrollment without separate consent

"X, an individual, electronically messages Y, a real estate broker, requesting Y to help identify a suitable rented accommodation for her and shares her personal data for this purpose. Y may process her personal data to identify and intimate to her the details of accommodation available on rent. Subsequently, X informs Y that X no longer needs help from Y. Y shall cease to process the personal data of X."

Key Insight: Section 7(a) is NOT perpetual. When the purpose ceases (X found accommodation elsewhere) or Data Principal objects, processing must stop immediately.

The Conundrum: If I voluntarily give my phone number to receive a receipt, haven't I implicitly consented to that use? What makes Section 7(a) different from Section 6 consent?

Aspect | Section 6 Consent | Section 7(a) Voluntary Provision

Nature | Explicit, affirmative action | Implicit from conduct

Mechanism | Opt-in (must affirmatively agree) | Opt-out (assumed unless objection)

Formality | Requires Section 5 notice, clear affirmative action | Less formal - inferred from provision and context

Withdrawal | Section 6(5) - formal withdrawal process | Simple objection sufficient

[recovered from the vector store — section7.html p.12]

Purpose Scope | Can be broader, multiple purposes | Tightly limited to specific purpose of provision

The Philosophical Answer: Section 7(a) recognizes what philosopher J.L. Austin called "speech acts" - actions that perform a function merely by being stated. When you give your phone number for a receipt, your action (providing number) combined with context (requesting receipt) creates an implicit authorization that's narrower and more situation-specific than formal consent. 4.4 Practical Scenarios: When to Use Section 7(a) vs Section 6

📌 Real-World Scenario Matrix

Scenario 1: E-Commerce Order Confirmation

Customer places order, provides email for order confirmation. Use: 📌 Section 7(a) - Voluntary provision, specified purpose

Scenario 2: Newsletter Subscription

Website offers newsletter, asks visitor to provide email. Use: 📌 Section 6 Consent Required - Marketing/promotional use

Scenario 3: Restaurant Reservation

Diner provides phone number for reservation confirmation. Use: 📌 Section 7(a) - Limited to reservation management

Scenario 4: Fitness App - Health Data

User uploads health metrics to track fitness progress.
Use: 📌📌 Section 6 Consent Preferred - Health data is sensitive

Scenario 5: Social Media Platform

User uploads photos, videos, posts to share. Use: 📌📌 Section 6 Consent Required - Processing scope (algorithmic recommendations, ad targeting) extends beyond immediate purpose

5. Section 7(b): State Benefits - The Digital Welfare State

Statutory Text: "For the State and any of its instrumentalities to provide or issue to the Data Principal such subsidy, benefit, service, certificate, licence or permit as may be prescribed..."

5.1 The Aadhaar Connection

Section 7(b) is intimately connected to India's Aadhaar ecosystem. The Aadhaar Act, 2016 allows Aadhaar-based delivery of benefits, and Section 7(b) provides the data protection legal basis for such delivery under DPDPA.

📌 Understanding the Aadhaar-DPDPA Relationship

Aadhaar Act, 2016:

[recovered from the vector store — section7.html p.13]

Section 7(b) DPDPA: Provides data protection legal basis for State to process Aadhaar and other personal data when delivering benefits. Official Illustration: "X, a pregnant woman, enrolls herself on an app or website to avail of government's maternity benefits program, while consenting to provide her personal data for the purpose of availing of such benefits. After X is granted maternity benefits, the Government may process the personal data of X for determining her eligibility to receive any other prescribed benefit from the government."

Key Insight: This illustration shows "consent creep" - data provided for one benefit (maternity) can be used for other benefits without fresh consent. This is simultaneously efficiency-promoting and privacy-concerning.

5.2 What Qualifies as "Benefits, Services, Certificates"?

Category | Examples | Data Typically Processed

Subsidy | LPG subsidy, Food subsidy, Fertilizer subsidy | Income details, Family size, Consumption data

Benefit | Pension, Scholarship, Maternity benefits, Disability benefits | Age, Health records,

Educational records, Employment history

Service | Passport, Healthcare (CGHS), Public education | Identity documents, Address proof, Medical history

Certificate | Birth certificate, Death certificate, Caste certificate, Income certificate | Family details, Hospital records, Land records

Licence | Driving licence, Arms licence, Professional licences | Qualifications, Criminal records, Biometric data

Permit | Building permit, Trade licence, Environmental clearances | Property details, Business information, Financial records

5.3 The "Benefit Creep" Concern

?? The "Benefit Creep" Dilemma

Efficiency Argument (Pro):

Reduces duplicative data collection

Auto-enrollment in benefits Data Principal is entitled to

Reduces administrative burden

Minimizes fraud (cross-refe

[recovered from the vector store — section7.html p.14]

rencing across schemes)

Privacy Argument (Con):

Undermines purpose limitation principle

Creates detailed welfare profiles

Potential for surveillance and social scoring

Risk of function creep beyond welfare to law enforcement, taxation

The Balancing Act: Puttaswamy requires proportionality. Use of maternity benefit data to determine eligibility for childcare support? Probably proportionate. Use of same data to profile fertility patterns for demographic studies without further consent? Likely disproportionate.

Recommended Safeguard: Government should establish categories of related benefits where cross-use is permissible (e.g., "Family Welfare Category"). Cross-category use should require fresh consent.

6. Section 7(c): State Functions and Sovereignty

Statutory Text: "For the performance by the State or any of its instrumentalities of any function under any law for the time being in force in India or in the interest of sovereignty and integrity of India or security of the State."

6.1 Scope of State Functions

Section 7(c) is the broadest and potentially most concerning provision. It covers:

Law Enforcement: Police investigations, criminal prosecutions

National Security: Intelligence gathering, counter-terrorism

Tax Administration: Income tax assessments, GST compliance

Regulatory Functions: RBI banking supervision, SEBI market regulation

Judicial Functions: Court proceedings, enforcement of judgments

Critical Safeguards Required

While Section 7(c) permits broad state processing, Puttaswamy's proportionality doctrine still applies:

Processing must be for a specific state function, not general surveillance

Only necessary data should be processed

Procedural safeguards must exist (judicial warrants, oversight mechanisms)

Data retention should be limited to what's legally required

6.2 "Sovereignty and Integrity" - Defining the Undefined

The terms "sovereignty and integrity of India" and "security of the State" are borrowed from Article 19(2) of the C

[recovered from the vector store — section7.html p.15]

onstitution, which permits reasonable restrictions on fundamental rights.

Supreme Court Guidance: In *S.R. Bommai v. Union of India* (1994) 3 SCC 1, the Court held that "security of State" refers to serious and aggravated forms of public disorder, not mere law and order problems.

Application to Section 7(c): Processing under "security of State" should be limited to:

Terrorism and insurgency matters

Espionage and foreign interference

War and external aggression threats

Organized crime threatening state institutions

It should NOT cover routine law enforcement or administrative convenience.

7. Sections 7(d) - 7(i): Remaining Legitimate Uses

7.1 Section 7(d): Legal Disclosure Obligations

Purpose: Enables compliance with statutory disclosure requirements (tax returns, regulatory filings, audit requirements). Example: Banks must disclose suspicious transactions to Financial Intelligence Unit under PMLA; companies must file annual returns with ROC. 7.2 Section 7(e): Judicial Compliance

Purpose: Permits processing pursuant to court orders, arbitral awards, or foreign judgments. Example: Discovery orders in litigation, asset attachment orders, family court custody proceedings. 7.3 Section 7(f): Medical Emergency

Purpose: Life-threatening situations requiring immediate medical intervention. Example: Unconscious accident victim at ER; accessing medical history to prevent drug allergies; emergency blood transfusion. When Does "Emergency" End?

Critical Question: Once patient regains consciousness and is stable, Section 7(f) no longer applies. Hospital must obtain consent for ongoing treatment and data processing. Best Practice: Obtain retroactive consent at earliest opportunity; explain what data was accessed during emergency.

7.4 Section 7(g): Public Health Measures

Purpose: Epidemic/pandemic response, disease outbreak control. Example: COVID-19 contact tracing, Aarogya Setu app, vaccination certificate generation, epidemic surveillance. 7.5 Section 7(h):

[recovered from the vector store — section7.html p.16]

Disaster Management

Purpose: Natural disasters, public order breakdowns requiring emergency response.

Example: Flood rescue operations using location data, earthquake victim identification, riot control and evacuation.

7.6 Section 7(i): Employment Purposes

Purpose: Employee data processing for employment relationship and protecting employer interests.

Permitted Uses:

Payroll processing and tax deduction

Performance management and appraisals

Background verification

Trade secret protection

Prevention of corporate espionage

Workplace safety and security

Section 7(i) Controversies

The Debate: Section 7(i) has been criticized as overly broad, potentially enabling invasive employee surveillance.

Concerns:

Email monitoring

Biometric attendance beyond what's necessary

Social media monitoring

Location tracking of employees

Recommended Approach: Employers should still obtain consent for non-essential processing. Use Section 7(i) only for genuinely necessary employment functions.

8. Comparative Analysis: DPDPA Section 7 vs GDPR Article 6

8.1 Fundamental Philosophical Difference

Aspect | DPDPA Section 7 | GDPR Article 6

Approach | Closed list (9 specific categories) | Open principles (6 lawful bases with interpretation flexibility)

Legitimate Interests | No general legitimate interests basis | Article 6(1)(f) - Balancing test between controller and data subject interests

Contractual Necessity | Not included (must use consent or Section 7(a)) | Article 6(1)(b) - Processing necessary for contract performance

Predictability | Higher - clear whether processing fits category | Lower - requires case-by-case balancing for legitimate interests

Flexibility | Lower - cannot adapt to new scenarios easily | Higher - legitimate interests can cover novel situations

8.2 Why No "Legitimate Interests"?

GDPR's Article 6(1)(f) "legitimate interests" is the most commonly used basis in Europe (after consent). It allows controllers to process data when:

Controller has a legi

[recovered from the vector store — section7.html p.17]

itimate interest

Processing is necessary for that interest

Data subject's interests don't override controller's interests

Why India Rejected This:

Abuse Potential: Concern that Indian companies would over-rely on "legitimate interests" to bypass consent

Enforcement Complexity: Balancing test requires sophisticated regulatory oversight

Legal Certainty: Closed list provides more certainty for compliance

Cultural Preference: Indian legal tradition favors specific rules over broad principles

9. DPDP Rules 2025: Operationalizing Section 7

9.1 Second Schedule - Standards for State Processing

The DPDP Rules 2025 Second Schedule specifies standards for processing under Section 7(b) by State and its instrumentalities:

Intimation Requirement: State must provide intimation to Data Principal about the processing

Contact Information: Must provide business contact information for queries

Transparency: Even though consent not required, transparency obligations remain

9.2 Fourth Schedule - Children's Data Exemptions

Fourth Schedule specifies situations where Section 7 processing doesn't require parental consent verification for children's data:

State benefits and services

Medical emergencies

Judicial compliance

10. Practical Compliance Guidance for Organizations

10.1 Decision Tree: Which Legal Basis to Use?

🔍 Legal Basis Selection Framework

Step 1: Is this for a state benefit, emergency, or state function?

→ YES: Check Section 7(b), (c), (f), (g), (h)

→ NO: Go to Step 2

Step 2: Did Data Principal voluntarily provide data for a specific, limited purpose?

→ YES: Consider Section 7(a) (but be conservative)

→ NO: Go to Step 3

Step 3: Is this for employment management or employer protection?

→ YES: Consider Section 7(i)

→ NO: Go to Step 4

Step 4: None of the above?

→ Must obtain Section 6 consent

10.2 Documentation Requirements

Even when using Section 7, organizations should document:

Legal Basis Assessment: Why this processing qualifies under specific

[recovered from the vector store — section7.html p.18]

Section 7 subsection

Necessity Justification: Why this specific data is necessary

Proportionality Analysis: How you've minimized privacy impact

Alternative Consideration: Why consent-based processing wasn't feasible

Retention Policy: How long data will be kept and why

10.3 Common Mistakes to Avoid

❑ Common Section 7 Compliance Errors

❑ Mistake 1: Using Section 7(a) for marketing

❑ Correct: Always use Section 6 consent for marketing

❑ Mistake 2: Assuming employment covers all employee data

❑ Correct: Section 7(i) is limited to necessary employment functions

❑ Mistake 3: Processing beyond specified purpose under 7(a)

❑ Correct: Purpose must be narrow and specific

❑ Mistake 4: Ignoring proportionality requirements

❑ Correct: Section 7 doesn't eliminate necessity and proportionality

❑ Mistake 5: Not documenting legal basis

❑ Correct: Maintain detailed records of Section 7 reliance

10.4 Board-Level Considerations

Boards of Directors should:

Review and approve policies on when to use Section 7 vs consent

Ensure conservative interpretation of Section 7 to minimize regulatory risk

Monitor complaints about Section 7 processing

Conduct annual legal basis audits

Engage external counsel for Section 7 interpretations

Section 7 of the DPDPA represents a carefully calibrated balance between individual privacy rights and societal necessities. By providing nine specific categories of consent-free processing, the legislature has:

❑ Enabled essential government functions and emergency responses

❑ Facilitated legitimate business operations

❑ Maintained constitutional compliance with Puttaswamy principles

❑ Provided legal certainty through a closed list approach

However, Section 7 is not a blank check. The proportionality doctrine, purpose limitation, and necessity principles continue to apply. Data Fiduciaries must exercise Section 7 powers responsibly, always asking:

"Is this processing truly necessary, proportionate, and in alignment with

[recovered from the vector store — section7.html p.19]

the specific Section 7 category I'm invoking?"

As Justice Chandrachud wrote in Puttaswamy: "Privacy is not surrendered by the individual under a contract. Nor can such a surrender be the condition precedent to the enjoyment of non-privacy related benefits."

Section 7 embodies this principle - it permits processing without consent only when absolutely necessary, not as a matter of contractual convenience or business preference. [🔗](#) Key Takeaways for Compliance

Default to Consent: When in doubt, use Section 6 consent rather than stretching Section 7

Document Everything: Maintain detailed records of Section 7 reliance and necessity justifications

Regular Audits: Periodically review whether Section 7 processing is still necessary

Purpose Limitation: Don't expand processing beyond original Section 7 justification

Proportionality: Always apply Puttaswamy's three-prong test

Transparency: Even without consent, be transparent about processing

Conservative Interpretation: When Section 7 is ambiguous, choose the privacy-protective reading

Comprehensive Legal Interpretation Complete

This interpretation covers all nine subsections of Section 7 DPDPA, 2023, with constitutional analysis, philosophical foundations, case law references, and practical guidance.

[🔗](#) 9 comprehensive subsection analyses

[🔗](#) Puttaswamy judgment constitutional framework

[🔗](#) Philosophical foundations (Kant, Rousseau, Mill)

[🔗](#) 50+ practical scenarios and examples

[🔗](#) GDPR comparative analysis

[🔗](#) Academic research references (Acquisti, Barocas, Adjerd)

[🔗](#) DPDP Rules 2025 interpretation

[🔗](#) Corporate compliance toolkit

© 2025 Prepared by Advocate (Dr.) Prashant Mali

International Data Protection Lawyer | Cyber Law Expert

This interpretation is provided for educational purposes and does not constitute legal advice. Organizations should consult qualified legal counsel for specific compliance guidance tailored to their operations.