

## Section 17 DPDPA

Exemptions. 17.(1) The provisions of Chapter II, except sub-sections (1) and (5) of section 8, and those of Chapter III and section 16 shall not apply where—

- (a) the processing of personal data is necessary for enforcing any legal right or claim; (b) the processing of personal data by any court or tribunal or any other body in India which is entrusted by law with the performance of any judicial or quasi-judicial or regulatory or supervisory function, where such processing is necessary for the performance of such function; (c) personal data is processed in the interest of prevention, detection, investigation or prosecution of any offence or contravention of any law for the time being in force in India; (d) personal data of Data Principals not within the territory of India is processed pursuant to any contract entered into with any person outside the territory of India by any person based in India;
- (e) the processing is necessary for a scheme of compromise or arrangement or merger or amalgamation of two or more companies or a reconstruction by way of demerger or otherwise of a company, or transfer of undertaking of one or more company to another company, or involving division of one or more companies, approved by a court or tribunal or other authority competent to do so by any law for the time being in force; and
- (f) the processing is for the purpose of ascertaining the financial information and assets and liabilities of any person who has defaulted in payment due on account of a loan or advance taken from a financial institution, subject to such processing being in accordance with the provisions regarding disclosure of information or data in any other law for the time being in force. Explanation.—For the purposes of this clause, the expressions “default” and “financial institution” shall have the meanings respectively assigned to them in sub-sections (12) and (14) of section 3 of the Inso

[recovered from the vector store — section17.html p.2]

X, an individual, takes a loan from Y, a bank. X defaults in paying her monthly loan repayment instalment on the date on which it falls due. Y may process the personal data of X for ascertaining her financial information and assets and liabilities.

(2) The provisions of this Act shall not apply in respect of the processing of personal data—

(a) by such instrumentality of the State as the Central Government may notify, in the interests of sovereignty and integrity of India, security of the State, friendly relations with foreign States, maintenance of public order or preventing incitement to any cognizable offence relating to any of these, and the processing by the Central Government of any personal data that such instrumentality may furnish to it; and

(b) necessary for research, archiving or statistical purposes if the personal data is not to be used to take any decision specific to a Data Principal and such processing is carried on in accordance with such standards as may be prescribed.

(3) The Central Government may, having regard to the volume and nature of personal data processed, notify certain Data Fiduciaries or class of Data Fiduciaries, including startups, as Data Fiduciaries to whom the provisions of section 5, sub-sections (3) and (7) of section 8 and sections 10 and 11 shall not apply.

Explanation.—For the purposes of this sub-section, the term “startup” means a private limited company or a partnership firm or a limited liability partnership incorporated in India, which is eligible to be and is recognised as such in accordance with the criteria and process notified by the department to which matters relating to startups are allocated in the Central Government.

(4) In respect of processing by the State or any instrumentality of the State, the provisions of sub-section (7) of section 8 and sub-section (3) of section 12 and, where such processing is for a

[recovered from the vector store — section17.html p.3]

purpose that does not include making of a decision that affects the Data Principal, sub-section (2) of section 12 shall not apply.

(5) The Central Government may, before expiry of five years from the date of commencement of this Act, by notification, declare that any provision of this Act shall not apply to such Data Fiduciary or classes of Data Fiduciaries for such period as may be specified in the notification.

Applicable DPDP Rule 2025

Rule 15: Exemption from Act for Research, Archiving or Statistical Purpose

← Section 16 DPDPA

Section 18 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 17 of the Digital Personal Data Protection Act, 2023

"No rule without exception, but exceptions must not swallow the rule." - Legal Maxim  
Section 17(1). Nothing contained in this Act shall apply to—

processing of personal data necessary for such person as may be notified by the Central Government in the interest of sovereignty and integrity of India, security of the State, friendly relations with foreign States, maintenance of public order or preventing incitement to any cognizable offence relating to any of these;

processing of personal data made available by such person voluntarily for any public benefit or public service and for such purpose, as may be notified by the Central Government;

processing of personal data necessary for the purpose of prevention, detection, investigation or prosecution of any offence or contravention of any law for the time being in force;

processing of personal data in the interest of such person or such class of persons in the course of any judicial proceeding or for the purpose of exercising any right or claim before any

[recovered from the vector store – section17.html p.4]

court or tribunal as may be notified by the Central Government;

Section 17(2). Nothing contained in section 5, section 6, section 7 and section 8 shall apply to—

processing of personal data for the purposes of research, archiving or statistical purposes, subject to such safeguards as may be notified by the Central Government for ensuring that the identity of the Data Principal cannot be inferred from such data;

processing of publicly available personal data.

Applicable DPDP Rules 2025:

Rule 6: Exemptions for Certain Categories of Processing

Rule 7: Safeguards for Research and Archiving

Table of Contents

Executive Summary: When DPDPA Doesn't Apply

Philosophical Foundations: Public Good vs Individual Rights

Constitutional Framework: Reasonable Restrictions

Section 17(1)(a): National Security & Public Order

Section 17(1)(b): Voluntary Public Benefit

Section 17(1)(c): Crime Prevention & Prosecution

Section 17(2)(b): Publicly Available Data

Preventing Exemption Abuse

Comparative Analysis: GDPR, CCPA Exemptions

1. Executive Summary: When DPDPA Doesn't Apply

Section 17 carves out exemptions - situations where DPDPA's stringent requirements DON'T apply.

?? Understanding Exemptions

What Exemptions Mean:

Normally, processing personal data requires:

? Notice (Section 5)

? Consent (Section 6)

? Limited purpose (Section 4)

? Security (Section 8)

? All other DPDPA protections

With Exemptions:

Some or ALL of these requirements are WAIVED for specific purposes.

Why Exemptions Exist:

Certain legitimate activities would be impossible if DPDPA fully applied:

National Security: Can't notify terrorists you're tracking them

Crime Investigation: Can't get suspect's consent to investigate them

Research: Academic research requires data analysis without individual consent

Journalism: Public interest reporting would be stifled by consent requirements

Two Types of Exemptions in S

[recovered from the vector store — section17.html p.5]

ection 17:

Complete Exemption (17(1)): ENTIRE Act doesn't apply

Partial Exemption (17(2)): Only Sections 5-8 don't apply (but Sections 11-15 still apply)

### 1.1 Complete vs Partial Exemptions

Exemption | Scope | What Doesn't Apply | What Still Applies

17(1)(a) National Security | COMPLETE | ENTIRE Act | Nothing - full exemption

17(1)(b) Public Benefit | COMPLETE | ENTIRE Act | Nothing - full exemption

17(1)(c) Crime Investigation | COMPLETE | ENTIRE Act | Nothing - full exemption

17(1)(d) Judicial Proceedings | COMPLETE | ENTIRE Act | Nothing - full exemption

17(2)(a) Research/Statistics | PARTIAL | Sections 5, 6, 7, 8 (Notice, Consent, Purpose, Security) |

Sections 11-15 (Access, Correction, Grievance, Nomination, Duties) still apply

17(2)(b) Public Data | PARTIAL | Sections 5, 6, 7, 8 | Sections 11-15 still apply

## 2. Philosophical Foundations: Public Good vs Individual Rights

### 2.1 Jeremy Bentham: Utilitarianism

Greatest Happiness Principle: "The greatest good for the greatest number."

Application to Exemptions:

Individual privacy rights sometimes must yield to collective good:

National Security: Protecting millions > individual privacy

Crime Prevention: Public safety > criminal's privacy

Research: Medical breakthroughs benefiting humanity > individual control

Section 17 implements utilitarian balance.

### 2.2 John Stuart Mill: Harm Principle

Mill's Principle: "The 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."

Application: Privacy rights can be restricted to prevent harm:

17(1)(a): Prevent harm to nation

17(1)(c): Prevent harm from crime

### 2.3 Ronald Dworkin: Rights as Trumps (But Not Absolute)

Concept: Individual rights normally "trump" collective interests BUT rights aren't absolute.

Section 17 recognizes: Privacy is fundamental right (Puttaswamy) but subject to reasonable restrictions for compelling state interests.

[recovered from the vector store — section17.html p.6]

able Restrictions

### 3.1 Article 19 & Reasonable Restrictions

Article 19(1)(a): Right to freedom of speech and expression

Article 19(2): Reasonable restrictions in interests of sovereignty, security, public order, etc.

Parallel to Section 17: Privacy right (Article 21) also subject to reasonable restrictions for:

Sovereignty and integrity of India [17(1)(a)]

Security of State [17(1)(a)]

Public order [17(1)(a)]

Prevention of offences [17(1)(c)]

### 3.2 Puttaswamy's Three-Pronged Test

K.S. Puttaswamy v. Union of India (2017) established test for restricting privacy:

Legality: Restriction must have legislative mandate

Legitimate Aim: Must serve legitimate state interest

Proportionality: Means must be proportionate to objective

Section 17 satisfies test:

☐ Legality: Parliamentary statute (DPDPA)

☐ Legitimate Aim: National security, crime prevention, judicial proceedings, public benefit, research

☐ Proportionality: Exemptions narrowly tailored (must be "necessary," "for specified purpose")

### 4. Section 17(1)(a): National Security & Public Order

Statutory Language: "processing of personal data necessary for such person as may be notified by the Central Government in the interest of sovereignty and integrity of India, security of the State, friendly relations with foreign States, maintenance of public order or preventing incitement to any cognizable offence relating to any of these"

#### 4.1 Scope of Exemption

Five Grounds:

Sovereignty and integrity of India

Security of the State

Friendly relations with foreign States

Maintenance of public order

Preventing incitement to cognizable offence

☐ National Security Exemption Examples

☐ LEGITIMATE Uses:

Example 1: Intelligence Agencies

Entity: R&AW, IB, CBI

Processing: Monitoring suspected terrorists' communications, travel patterns, financial transactions

Why Exempt: Cannot notify suspects, cannot obtain consent, necessary for national security

Safeguard: Must be "necessary" - proportionality requirement

Examp

[recovered from the vector store — section17.html p.7]

le 2: Border Security

Entity: BSF, ITBP

Processing: Biometric data of people crossing borders, facial recognition at checkpoints

Why Exempt: Security of State

Example 3: Counter-Terrorism

Entity: NIA, Police

Processing: Social media monitoring for radicalization, travel bookings of suspects

Why Exempt: Preventing incitement to cognizable offences (terrorism)

Example 4: Diplomatic Intelligence

Entity: Ministry of External Affairs, intelligence wings

Processing: Data about foreign diplomats, suspected spies

Why Exempt: Friendly relations with foreign States, Security of State

?? QUESTIONABLE Uses (Potential Abuse):

Example 1: Political Surveillance

Scenario: Ruling party uses "national security" exemption to monitor opposition politicians

Problem: Not actually "necessary" for security - this is political abuse

Safeguard: Judiciary can review if exemption misused

Example 2: Journalist Monitoring

Scenario: Monitoring investigative journalists under guise of "public order"

Problem: Chills free speech, not genuine security threat

Safeguard: "Necessary" requirement + judicial review

4.2 "Such Person as May Be Notified"

Key Phrase: Central Government must NOTIFY which entities can claim this exemption.

Likely Notified Entities:

Intelligence Bureau (IB)

Research & Analysis Wing (R&AW)

Central Bureau of Investigation (CBI)

National Investigation Agency (NIA)

Directorate of Revenue Intelligence (DRI)

Border Security Force (BSF)

Military Intelligence

NOT automatically exempt: Regular police, state agencies (unless notified)

## 5. Section 17(1)(b): Voluntary Public Benefit

Statutory Language: "processing of personal data made available by such person voluntarily for any public benefit or public service and for such purpose, as may be notified by the Central Government"

### 5.1 Three Requirements

Voluntarily provided: Data Principal gave data willingly

Public benefit/public service: Processing serves public good

Notified purpose: Central Government s

[recovered from the vector store – section17.html p.8]

pecifies which purposes qualify

#### Public Benefit Exemption Examples

##### Example 1: Disaster Relief

Scenario: Earthquake strikes. Citizens voluntarily register on government portal with contact details, location, needs.

Processing: Government shares data with relief agencies to coordinate rescue

Why Exempt: Voluntarily provided + public benefit (disaster relief)

Result: No need for formal consent, notice procedures

##### Example 2: COVID Contact Tracing

Scenario: People voluntarily install contact tracing app (Aarogya Setu)

Processing: Government uses location data to identify potential COVID exposures

Why Exempt: Voluntarily provided + public service (public health)

##### Example 3: Blood Donor Registry

Scenario: People voluntarily register as blood donors with government database

Processing: Government/hospitals contact them when blood needed

Why Exempt: Voluntarily provided + public benefit (saving lives)

##### Example 4: Missing Persons Database

Scenario: Family voluntarily submits details of missing person

Processing: Police/NGOs share information to aid search

Why Exempt: Voluntarily provided + public service

#### 5.2 "Voluntarily" - Critical Qualifier

Truly Voluntary Means:

Free choice (not coerced)

Clear understanding of purpose

Can withdraw

NOT Voluntary:

Mandatory government forms

Required for accessing benefits

Coerced by circumstances

#### 6. Section 17(1)(c): Crime Prevention & Prosecution

Statutory Language: "processing of personal data necessary for the purpose of prevention, detection, investigation or prosecution of any offence or contravention of any law for the time being in force"

##### 6.1 Four Stages of Criminal Justice

Prevention: Proactive measures to stop crime

Detection: Discovering that crime occurred

Investigation: Gathering evidence, identifying culprits

Prosecution: Legal proceedings against accused

❓ Law Enforcement Exemption Scenarios

Prevention:

Police analyze crime patterns to deploy patrols

Monitoring known offenders' mo

[recovered from the vector store — section17.html p.9]

vements

Surveillance of high-crime areas

Detection:

CCTV footage analysis after crime

Analyzing financial transactions for fraud detection

Data mining to identify suspicious patterns

Investigation:

Accessing suspect's phone records

Obtaining bank statements

Collecting DNA/biometric data

Email/social media content review

Prosecution:

Using collected data as evidence in court

Witness protection data

Maintaining criminal records

6.2 "Necessary" Requirement

"Necessary" = Proportionality Test

Not every police request is "necessary." Courts will examine:

Is processing essential for stated purpose?

Are less intrusive alternatives available?

Is extent of processing proportionate to crime's severity?

?? Proportionality Analysis

? PROPORTIONATE:

Scenario: Murder investigation - Police obtain suspect's phone location data for day of murder

Analysis: Serious crime + narrow temporal scope + directly relevant = proportionate

?? DISPROPORTIONATE:

Scenario: Traffic challan case - Police demand 5 years of suspect's complete browsing history

Analysis: Minor offence + excessive scope + not relevant = disproportionate

? PROPORTIONATE:

Scenario: Terrorism investigation - Intelligence agencies monitor suspect's communications

Analysis: Grave threat + necessary for prevention = proportionate

## ?? DISPROPORTIONATE:

Scenario: Mass surveillance of all citizens "just in case"

Analysis: Dragnet surveillance + no specific suspicion = disproportionate

7. Section 17(1)(d): Judicial Proceedings

Statutory Language: "processing of personal data in the interest of such person or such class of persons in the course of any judicial proceeding or for the purpose of exercising any right or claim before any court or tribunal"

7.1 Scope: Court Proceedings & Legal Rights

### ?? Judicial Proceedings Exemption

Covers:

1. Evidence in Litigation

Parties can present personal data as evidence without consent requirements

Example: Divorce case - presenting spouse's bank statement

[recovered from the vector store — section17.html p.10]

s, emails as evidence of infidelity/hidden assets

## 2. Discovery/Disclosure

Legal obligation to disclose documents in litigation

Example: Employment discrimination case - employer must disclose employee records

## 3. Witness Testimony

Witnesses can testify about others' personal information

Example: Witness describes accused's behavior, movements (personal data)

## 4. Court Records

Court judgments often contain personal data of parties

Example: Published judgment includes names, facts about parties

## 5. Legal Advice & Representation

Lawyers processing client data to provide legal services

Example: Lawyer reviews client's contracts, financial records to advise on dispute

## 6. Arbitration & Tribunals

Similar exemption for arbitral proceedings, quasi-judicial bodies

Example: Consumer forum, labor tribunal, tax tribunal proceedings

## 7.2 Balancing with Court Confidentiality

Important: Exemption doesn't override court rules on confidentiality/sealing records.

Courts can still:

Seal sensitive documents

Hold in-camera proceedings

Redact personal data from public judgments

Issue gag orders

Section 17(1)(d) means: DPDPA doesn't ADD extra barriers to using data in court, but existing legal protections remain.

## 8. Section 17(2)(a): Research & Statistics

Statutory Language: "processing of personal data for the purposes of research, archiving or statistical purposes, subject to such safeguards as may be notified by the Central Government for ensuring that the identity of the Data Principal cannot be inferred from such data"

Type: PARTIAL exemption (only Sections 5-8 don't apply)

### 8.1 Three Purposes

Research: Scientific, academic, medical research

Archiving: Historical preservation, cultural heritage

Statistical: Government statistics, economic data, surveys

#### 🔍 Research Exemption Examples

Medical Research:

Scenario: Cancer research institute analyzes patient records from hospitals to identify cancer patterns

Without Exemption: Would need consent from every patient

[recovered from the vector store — section17.html p.11]

t (impossible for historical data, deceased patients)

With Exemption: Can process WITHOUT consent IF data is de-identified

Safeguard: Must anonymize data so individual patients cannot be re-identified

Scenario: University researchers analyze social media data to study political polarization

Without Exemption: Need consent from millions of users

With Exemption: Can analyze IF data is aggregated/anonymized

Scenario: Census data, economic surveys, unemployment statistics

Without Exemption: Each respondent would need full DPDPA notice/consent

With Exemption: Can collect and analyze for statistical purposes with de-identification

Scenario: National Archives preserving government records, historical documents

Without Exemption: Would need to redact all personal data or obtain consent (impractical)

With Exemption: Can preserve with appropriate access controls

## 8.2 The Critical Safeguard: De-Identification

Requirement (Rule 7): "Identity of the Data Principal cannot be inferred from such data"

Technique | Description | Example

Anonymization | Irreversibly remove identifying info | Remove names, addresses, ID numbers, replace with random codes

Aggregation | Report only grouped statistics | "25% of respondents aged 25-35" (not individual ages)

Pseudonymization | Replace identifiers with pseudonyms | "Patient A", "Patient B" instead of real names

Data Masking | Obscure parts of data | Phone: "XXXXX-43210", DOB: "XX/XX/1990"

Generalization | Reduce precision | Exact address → City only, Exact age → Age range

Noise Addition | Add random variations | Differential privacy techniques

Challenge: Seemingly anonymous data can sometimes be re-identified by combining datasets.

Famous Example: Netflix Prize dataset (2007)

Netflix released "anonymized" movie ratings for research competition

Researchers cross-referenced with IMDb public reviews

[recovered from the vector store — section17.html p.12]

## 9. Section 17(2)(b): Publicly Available Data

Statutory Language: "processing of publicly available personal data"

Type: PARTIAL exemption (only Sections 5-8 don't apply)

### 9.1 What is "Publicly Available"?

Definition: Personal data that is legitimately accessible to the public.

🔍 Publicly Available Data Examples

🔍 CLEARLY Public:

Company Directors: Listed on MCA website (Ministry of Corporate Affairs)

Property Records: Public land registries

Court Judgments: Published by courts (unless sealed)

Government Officials: Names, offices, contact info on official websites

Academic Publications: Author names, affiliations

Patents/Trademarks: Inventor/applicant names

Electoral Rolls: Voter lists (public in India)

🔍 ARGUABLY Public (Context-Dependent):

Social Media Profiles: Public profiles (but not private posts)

News Articles: Information published in media

Professional Directories: LinkedIn public profiles, doctor directories

Phone Directories: Yellow Pages (if people opted in)

🔍 NOT Public:

Data Breaches: Stolen data posted online ≠ "publicly available"

Private Messages: Even if leaked

Hacked Databases: Unlawfully obtained data remains protected

Inferred Data: Data scraped and aggregated from multiple sources to create profile

### 9.2 Limitations on Processing Public Data

Important: Just because data is public doesn't mean you can do ANYTHING with it.

Section 17(2)(b) exempts Sections 5-8 BUT Sections 11-15 STILL APPLY:

Section | Applies to Public Data? | Implication

Section 5 (Notice) | 🚫 Exempted | Don't need to provide notice when processing public data

Section 6 (Consent) | 🚫 Exempted | Don't need consent to process public data

Section 7 (Purpose) | 🚫 Exempted | Can use public data for different purposes

Section 8 (Security) | 🚫 Exempted | But best practice still to secure it

[recovered from the vector store — section17.html p.13]

APPLIES | Data Principal can still request access to how you're using their public data

Section 12 (Correction) | ? APPLIES | Data Principal can request correction if you have wrong public data

Section 13 (Grievance) | ? APPLIES | Data Principal can file complaints about your processing

## 10. Preventing Exemption Abuse

### 10.1 Narrow Interpretation Principle

Legal Principle: Exemptions to rights must be narrowly construed.

Supreme Court Precedent:

State of U.P. v. Jeet S. Bisht, (2007) 6 SCC 586:

"Exceptions to a right must be narrowly interpreted. The right is the rule; exception is an exception."

Application to Section 17: When in doubt, DPDPA protections apply. Exemptions don't expand.

### 10.2 Judicial Review of Exemptions

Courts Can Review:

Was processing truly "necessary"?

Was exemption properly invoked?

Was there less intrusive alternative?

Was proportionality maintained?

Cannot Hide Behind Exemptions:

Claiming "national security" doesn't immunize from all scrutiny

Courts apply proportionality test

Exemptions must be invoked in good faith

### 10.3 Safeguards Against Abuse

#### ?? Built-In Safeguards

##### 1. Notification Requirement

Central Government must NOTIFY which entities can claim exemption [17(1)(a), (b), (d)]

Not a blank check - specific entities only

##### 2. Purpose Limitation

Exemption only for SPECIFIED purpose

Can't claim crime investigation then use data for unrelated purposes

##### 3. Necessity Test

"Necessary" appears repeatedly - processing must be essential

Judicial review enforces this

##### 4. Partial Exemptions

Research/public data get PARTIAL exemption only (17(2))

Still subject to access, correction, grievance rights

#### 5. De-Identification for Research

Research exemption conditioned on anonymization

Can't claim research then use identifiable data for other purposes

#### 6. Data Protection Board Oversight

Board can investigate complaints even for exempt processing

Can report abuses to Parliament

#### 7. Parliamentary Accountability

Government must jus

[recovered from the vector store — section17.html p.14]

## Comparative Analysis: GDPR, CCPA Exemptions

Exemption Type | India (DPDPA) | EU (GDPR) | California (CCPA)  
National Security | ? Complete (17(1)(a)) | ? Complete (Art 23) | ? Exempt  
Crime Investigation | ? Complete (17(1)(c)) | ? Complete (Art 23) | ? Exempt  
Judicial Proceedings | ? Complete (17(1)(d)) | ? Complete (Recital 73) | ? Exempt  
Research/Statistics | Partial (17(2)(a)) | Partial (Art 89) | Partial exemption  
Public Data | Partial (17(2)(b)) | ? Can process (Recital 50) | ? Can process  
Journalism | Not explicit (may be under 17(1)(b)) | ? Explicit (Art 85) | ? Explicit  
Household/Personal | Not explicit | ? Explicit (Art 2(2)(c)) | ? Explicit  
Employment | Section 7(a) (not exemption, special ground) | Special rules (Art 88) | Partial exemption

### 11.1 Notable Differences

GDPR has explicit journalism exemption (Art 85):

Balances data protection with freedom of expression

Media/artistic expression gets special treatment

India's DPDPA:

No explicit journalism exemption

May fall under "public benefit" [17(1)(b)] if government notifies

Or may not be exempt at all (concerning for press freedom)

This is potential concern: Investigative journalism often processes personal data without consent.  
DPDPA may inadvertently chill journalism.

Section 17 recognizes that privacy rights, while fundamental, are not absolute.

Certain societal interests - national security, justice, research, public benefit - sometimes outweigh individual privacy.

"No right is absolute. The art of governance lies in balancing competing rights and interests."

Section 17 attempts this balance - protecting privacy while enabling legitimate public functions.

Key Principles:

Exemptions are Exceptions: Rule is protection, exemption is narrow exception

Necessity Requirement: Exemption only when processing is truly necessary

Proportionality: Extent of exemption must be p

[recovered from the vector store — section17.html p.15]

proportionate to purpose

Safeguards Remain: Even exempt processing subject to some oversight

Judicial Review: Courts can review if exemptions are abused

Narrow Construction: When in doubt, privacy prevails

The Six Exemptions:

17(1)(a): National security, public order (COMPLETE)

17(1)(b): Voluntary public benefit (COMPLETE)

17(1)(c): Crime prevention/prosecution (COMPLETE)

17(1)(d): Judicial proceedings (COMPLETE)

17(2)(a): Research/statistics (PARTIAL - with de-identification)

17(2)(b): Public data (PARTIAL - access rights remain)

Section 17 ensures DPDPA is workable in the real world while maintaining core privacy protections.

Comprehensive Legal Interpretation Complete

Section 17 DPDPA 2023 - Exemptions

🔍 Complete vs partial exemptions explained

🔍 Six exemption categories analyzed

🔍 National security & public order scope

🔍 Crime prevention & prosecution framework

🔍 Judicial proceedings exemption

🔍 Research with de-identification safeguards

🔍 Public data processing rules

🔍 Abuse prevention mechanisms

🔍 Proportionality & necessity tests

🔍 GDPR & CCPA comparison

🔍 Philosophical foundations (Bentham, Mill, Dworkin)

© 2026 Prepared by Advocate (Dr.) Prashant Mali

International Data Protection Lawyer | Cyber Law Expert