

[recovered from the vector store — section15.html p.1]

Section 15 DPDPA

Duties of Data Principal.

15.A Data Principal shall perform the following duties, namely:—

- (a) comply with the provisions of all applicable laws for the time being in force while exercising rights under the provisions of this Act;
- (b) to ensure not to impersonate another person while providing her personal data for a specified purpose;
- (c) to ensure not to suppress any material information while providing her personal data for any document, unique identifier, proof of identity or proof of address issued by the State or any of its instrumentalities;
- (d) to ensure not to register a false or frivolous grievance or complaint with a Data Fiduciary or the Board; and
- (e) to furnish only such information as is verifiably authentic, while exercising the right to correction or erasure under the provisions of this Act or the rules made thereunder.

Applicable DPDP Rule 2025

Rule 13: Rights of Data Principals

← Section 14 DPDPA
Section 16 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

Comprehensive Legal Interpretation of Section 15 of the Digital Personal Data Protection Act, 2023

"With great rights come great responsibilities." - Uncle Ben (data protection version)

Section 15 - Duties of Data Principal

Statutory Text

Section 15. The Data Principal shall—

comply with all applicable laws for the time being in force while exercising her rights under this Act;

not register a false or frivolous grievance or complaint with the Data Fiduciary or the Board, as the case may be;

not impersonate another person while providing her personal data for any document, unique identifier, proof of identity or proof of address;

not suppress any material information while providing her perso

[recovered from the vector store — section15.html p.2]

nal data for any document, unique identifier, proof of identity or proof of address, if such suppression is prohibited by law; and

furnish only such information, as is verifiably authentic, while exercising the right to correction or erasure under this Act.

Table of Contents

Executive Summary: Rights Come With Duties

Philosophical Foundations: Reciprocal Obligations

Constitutional Framework: Fundamental Duties

Section 15(a): Comply With All Applicable Laws

Section 15(b): No False or Frivolous Grievances

Section 15(e): Provide Verifiably Authentic Information

Consequences of Violating Duties

Comparative Analysis: Duties in Other Jurisdictions

1. Executive Summary: Rights Come With Duties

Sections 4-14 give Data Principals powerful rights. Section 15 says: "Don't abuse them."

This is the "responsibility clause" - balancing individual rights with societal interests and preventing system abuse. [??](#) The Balance Principle

The Rights You Get (Sections 4-14):

Right to consent-based processing (Section 4)

Right to notice (Section 5)

Right to withdraw consent (Section 6)

Right to access your data (Section 11)

Right to correction and erasure (Section 12)

Right to grievance redressal (Section 13)

Right to nominate (Section 14)

The Duties You Owe (Section 15):

Comply with other laws while exercising rights

Don't file false/frivolous complaints

Don't impersonate others

Don't suppress legally required information

Provide truthful information for corrections

Why Both Are Necessary:

Without duties, rights would be abused:

Criminals would use erasure to destroy evidence

Trolls would spam complaint systems

Fraudsters would impersonate others with impunity

People would make false correction claims

Entire data protection system would collapse

With duties, rights remain enforceable and effective.

[recovered from the vector store — section15.html p.3]

uence

15(a) Comply with laws | Don't use DPDPA rights to break other laws | Using erasure right to destroy evidence of tax fraud | Rights denied + prosecution under violated law

15(b) No frivolous complaints | Don't spam grievance systems | Filing 100 identical fake complaints | Complaints dismissed + possible defamation case + penalty

15(c) No impersonation | Don't pretend to be someone else | Using fake Aadhaar to open bank account | Criminal prosecution (IPC Sections 416-419)

15(d) No suppression | Don't hide legally required information | Omitting criminal record when applying for job that legally requires disclosure | Application rejected + possible fraud case

15(e) Authentic info | Correction requests must be truthful | Claiming you never had criminal conviction when you did | Correction denied + possible fraud case

2. Philosophical Foundations: Reciprocal Obligations

2.1 Immanuel Kant: Duty Ethics (Deontology)

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

Application to Section 15:

Test: What if EVERYONE abused data rights?

If everyone filed false complaints → grievance system collapses

If everyone impersonated others → trust in digital identity collapses

If everyone used erasure to destroy evidence → justice system collapses

If everyone made false correction claims → data accuracy meaningless

Conclusion: Such behavior cannot be universalized. Therefore, you have a DUTY not to behave this way.

Kant's Principle: Treat people as ends, not means.

Using data rights to manipulate or harm others treats them as means to your ends. Section 15 prohibits this.

2.2 Social Contract Theory (Rousseau, Locke, Hobbes)

Core Idea: Rights exist within a social contract. You get rights FROM society, you owe duties TO society.

Rousseau (The Social Contract, 1762): "Each of us puts his person and all his power in common under the supreme direction of the general will."

[recovered from the vector store — section15.html p.4]

Application:

Society gives you data rights (Sections 4-14)

In exchange, you must not abuse them (Section 15)

This reciprocity maintains social order

Locke's State of Nature: Without duties, we'd have "state of nature" - chaos where everyone pursues self-interest without restraint.

2.3 Aristotle: Virtue Ethics

Concept: Virtue is the mean between two extremes.

Application to Data Rights:

Deficiency: Never exercising your rights (letting others exploit you)

VIRTUE (Golden Mean): Exercising rights responsibly, with integrity

Excess: Abusing rights, weaponizing them against others

Section 15 promotes the virtuous mean - responsible exercise of rights.

3. Constitutional Framework: Fundamental Duties

3.1 Article 51A: Fundamental Duties

Article 51A (added by 42nd Amendment, 1976): Lists fundamental duties of every citizen.

Selected Duties:

(a) To abide by the Constitution and respect its ideals and institutions

(c) To uphold and protect the sovereignty, unity and integrity of India

(h) To develop scientific temper, humanism and the spirit of inquiry and reform

(j) To strive towards excellence in all spheres of individual and collective activity

Section 15 as Statutory Duties: Similar to Article 51A, Section 15 imposes specific duties related to data protection.

Parallel:

Article 51A = General civic duties

Section 15 = Specific data-related duties

Both balance rights with responsibilities

3.2 Rights-Duties Nexus in Indian Jurisprudence

Ranganath Misra v. Union of India, (2003) 2 SCC 747:

"While Part III of the Constitution deals with fundamental rights, Part IV-A dealing with fundamental duties emphasizes that while the citizens have fundamental rights, they also have certain fundamental duties."

Application: While DPDPA Part 3 gives rights, Part 4 (including Section 15) imposes duties. Consistent with constitutional structure.

4. Section 15(a): Comply With All Applicable Laws

Statutory Language: "comply with all applicable laws for the time b

[recovered from the vector store — section15.html p.5]

ing in force while exercising her rights under this Act"

Core Principle: DPDPA rights are not a license to break OTHER laws.

Example 1: Evidence Destruction (IPC Section 201)

Scenario: You're under investigation for tax fraud. Tax authorities have requested your financial records. You use Section 12(4) erasure right to delete all financial data from your bank's systems.

IPC Section 201 - Causing disappearance of evidence of offence

Income Tax Act, 1961 - Obstruction of tax proceedings

Consequence: Erasure request DENIED under Section 12(5)(b) (legal retention requirement) + Criminal prosecution + Imprisonment up to 7 years

Example 2: Money Laundering (PMLA Violation)

Scenario: You open bank account using fake identity (violating KYC norms). When bank questions irregularities, you submit Section 12 "correction" request claiming your fake details are "corrections."

Prevention of Money Laundering Act, 2002

Consequence: Correction denied + Account frozen + PMLA investigation + Imprisonment up to 7 years

Example 3: Defamation Through False Complaints (IPC Section 499)

Scenario: You dislike a company. You file Section 13 grievance falsely accusing them of selling your data to criminals (knowing this is false) to damage their reputation.

IPC Section 500 - Punishment for defamation

Consequence: Grievance dismissed + Defamation case by company + Imprisonment up to 2 years or fine

Example 4: Obstruction of Investigation (IPC Section 186)

Scenario: Police investigating cybercrime request your data from social media platform. You use Section 12 to request erasure of evidence b

[recovered from the vector store — section15.html p.6]

efore police can access it.

Laws Violated:

IPC Section 186 - Obstructing public servant

Information Technology Act provisions

Consequence: Erasure denied (ongoing investigation) + Obstruction charges + Imprisonment up to 3 months or fine up to ₹500 + Extended investigation

4.3 Legitimate vs Illegitimate Use

Scenario | Legitimate Use? | Reasoning

Deleting old social media posts for privacy | ☒ LEGITIMATE | No legal obligation to retain, no investigation, pure privacy interest

Correcting wrong birth date in records | ☒ LEGITIMATE | Accuracy right, no law violated

Deleting email after receiving court summons | ☒ ILLEGITIMATE | Evidence destruction, obstruction of justice

Requesting erasure of arrest record after charges dropped | ☒ LEGITIMATE | No conviction, privacy interest strong

Requesting erasure of conviction record (still within legal retention period) | ☒ ILLEGITIMATE | Criminal records must be retained per law

Filing complaint about actual data breach | ☒ LEGITIMATE | Genuine grievance

Filing false complaint to extort money | ☒ ILLEGITIMATE | Extortion (IPC Section 384)

5. Section 15(b): No False or Frivolous Grievances

Statutory Language: "not register a false or frivolous grievance or complaint with the Data Fiduciary or the Board, as the case may be"

Two Prohibited Types:

FALSE: Complaints that are knowingly untrue

FRIVOLOUS: Complaints that lack any serious purpose, are vexatious, or made to harass

5.1 What is "False" Complaint?

Definition: Complaint based on facts you KNOW to be untrue.

☒ False vs Mistaken Complaints

FALSE Complaint (Violates 15(b)):

"Company sold my data to advertisers" - when you KNOW they didn't, you're making it up to harm them

Result: ☒ Violation of Section 15(b) + Possible defamation case

MISTAKEN Complaint (Does NOT violate 15(b)):

"Company sold my data to advertisers" - you genuinely believe this happened based on receiving targeted ads, but actually it's contextual advertising, not data sale

Result: ☒ NOT a vi

[recovered from the vector store — section15.html p.7]

olation (honest mistake, good faith belief)

Key Distinction: Intent and Knowledge

False = Knowing it's untrue + filing anyway (bad faith)

Mistaken = Believing it's true + filing (good faith)

Good Faith Defense: If you genuinely believed the complaint was true, even if wrong, you did NOT violate Section 15(b). 5.2 What is "Frivolous" Complaint?

Definition: Complaint that:

Has no legal basis or merit

Is vexatious (intended to annoy/harass)

Lacks any serious purpose

Wastes system resources

?? Frivolous Complaint Examples

? FRIVOLOUS #1: Spam Complaints

Filing 100 identical complaints to same Data Fiduciary/Board about same issue that's already been addressed

Why Frivolous: Wastes resources, no serious purpose, harassment

? FRIVOLOUS #2: Unreasonable Demands

"I want you to delete the fact that I bought your product from your financial records"

Why Frivolous: Legally impossible (tax records must be maintained), no merit

? FRIVOLOUS #3: Vague Dissatisfaction

"I don't like your company, so I'm filing complaint"

Why Frivolous: No specific violation alleged, just dislike

? FRIVOLOUS #4: Already Resolved

Company already addressed your complaint satisfactorily.

You file 10 more complaints about same issue. Why Frivolous: Matter closed, no new information, harassment

? NOT FRIVOLOUS #1: Persistent Legitimate Complaint

Company claims they fixed data breach, but you have evidence they didn't. You follow up persistently. Why NOT Frivolous: Legitimate unresolved issue, not harassment

? NOT FRIVOLOUS #2: Novel Legal Issue

Your complaint raises new, untested legal question about data rights. Why NOT Frivolous: Serious legal purpose, even if outcome uncertain

6. Section 15(c): No Impersonation

Statutory Language: "not impersonate another person while providing her personal data for any document, unique identifier, proof of identity or proof of address"

Core Prohibition: Don't pretend to be someone else when providing identity information.

6.1 What is "

[recovered from the vector store — section15.html p.8]

❓ Impersonation Violations

Example 1: Fake Aadhaar

Using forged Aadhaar card with someone else's details to open bank account

Violation: Section 15(c) + IPC Section 419 (cheating by personation)

Penalty: Imprisonment up to 3 years + fine

Example 2: Identity Theft for Credit Card

Using stolen PAN and address proof to apply for credit card in victim's name

Violation: Section 15(c) + IPC Section 66C (identity theft under IT Act)

Penalty: Imprisonment up to 3 years + fine up to ₹1 lakh

Example 3: Celebrity Impersonation

Creating social media account pretending to be famous person, using their photos/details

Violation: Section 15(c) + IPC Section 416 (cheating by personation)

Penalty: Imprisonment up to 3 years + fine

Example 4: Exam Fraud

Taking online exam using someone else's credentials and identity documents

Violation: Section 15(c) + IPC Section 419 + exam fraud statutes

Penalty: Imprisonment + exam ban

Example 5: Job Application Fraud

Using fake degrees and someone else's credentials to apply for job

Violation: Section 15(c) + IPC Section 420 (cheating)

Penalty: Imprisonment up to 7 years + fine

6.2 Legitimate Name Variations vs Impersonation

Situation | Impersonation? | Explanation

Using nickname instead of legal name | ❓ NO | Still your identity, just informal version

Using maiden name after marriage | ❓ NO | Your legitimate previous name

Using stage name (actor, author) | ❓ NO | Legitimate professional name

Using someone else's Aadhaar | ❓ YES | Different person's identity document

Creating fake ID with celebrity's name | ❓ YES | Clear impersonation

Using parent's documents as your own | ❓ YES | Different person, even if family

7. Section 15(d): No Material Suppression

Statutory Language: "not suppress any material information while providing her personal data for any document, unique identifier, proof of identity or proof of address, if such suppression i

[recovered from the vector store — section15.html p.9]

s prohibited by law"

Key Phrase: "if such suppression is prohibited by law"

This means: You can't hide information that law **REQUIRES** you to disclose.

7.1 What is "Material Information"?

Material = Significant, relevant, could affect decision.

Not material: Trivial details that don't matter.

7.2 When is Suppression "Prohibited by Law"?

☐ Legally Required Disclosures

1. Criminal Record (When Legally Required)

Context: Applying for jobs in law enforcement, judiciary, sensitive positions

Required Disclosure: Criminal convictions, pending cases

Suppression Prohibited: ☐ YES (various employment laws)

2. Financial Liabilities (Loans, Insolvency)

Context: Applying for new loan, credit card

Required Disclosure: Existing loans, defaults, insolvency proceedings

Suppression Prohibited: ☐ YES (banking regulations)

3. Medical Conditions (Insurance)

Context: Buying health/life insurance

Required Disclosure: Pre-existing diseases, medical history

Suppression Prohibited: ☐ YES (Insurance Act, 1938)

4. Conflict of Interest (Government Employment)

Context: Applying for government position

Required Disclosure: Relatives in government, business interests

Suppression Prohibited: ☐ YES (conduct rules)

5. Dual Citizenship (Certain Contexts)

Context: Government jobs, defense contracts

Required Disclosure: Foreign citizenship, OCI status

Suppression Prohibited: ☐ YES (security clearance requirements)

6. Personal Preferences (Most Contexts)

Context: E-commerce, social media

Required Disclosure: Usually **NONE**

Suppression Prohibited: ☐ NO (you have privacy right)

7.3 General Privacy vs Specific Disclosure Requirements

Key Principle: Section 15(d) does NOT override your general privacy rights. It only applies when specific law requires disclosure.

Example:

Shopping website asks: "What's your income?" → You can refuse (no legal requirement to disclose)

Bank asks for income proof for loan → You must provide (banking regulations require it)

[recovered from the vector store — section15.html p.10]

ide Verifiably Authentic Information

Statutory Language: "furnish only such information, as is verifiably authentic, while exercising the right to correction or erasure under this Act"

Applies To: Section 12 correction and erasure requests. Core Requirement: When requesting correction, provide TRUE facts with proof. 8.1 What is "Verifiably Authentic"?

Verifiable = Can be proven true through evidence. Authentic = Genuine, not fake.

☑ Compliant Correction Requests

Example 1: Name Correction

Claim: "My name is misspelled as 'Jon' should be 'John'"

Evidence: Aadhaar card showing "John"

Verifiable? ☑ YES

Result: Correction granted

Example 2: Birth Date Correction

Claim: "My birth year is wrong - 1995, not 1985"

Evidence: Birth certificate + Passport showing 1995

Verifiable? ☑ YES

Result: Correction granted

Example 3: Transaction Correction

Claim: "This payment shows 'Failed' but actually succeeded"

Evidence: Bank statement showing successful debit + Payment confirmation email

Verifiable? ☑ YES

Result: Correction granted

☑ Non-Compliant Correction Requests

Example 1: False Criminal Record Claim

Claim: "I was never convicted of theft, please correct your records"

Reality: You WERE convicted (court records exist)

Evidence Provided: None, or fabricated documents

Verifiable? ☑ NO (False claim)

Result: ☑ Correction denied + Violates Section 15(e) + Possible fraud case

Example 2: Age Manipulation

Claim: "I'm 25, not 35, please correct"

Reality: All official documents show 35

Evidence Provided: Fake documents

Verifiable? ☐ NO (False claim)

Result: ☐ Correction denied + Violates Section 15(e)

Example 3: Loan Default Denial

Claim: "I never defaulted on loan, please erase this record"

Reality: Bank has records of default, legal notices sent

Evidence Provided: None or insufficient

Verifiable? ☐ NO (False claim)

Result: ☐ Erasure denied + Violates Section 15(e)

[recovered from the vector store — section15.html p.11]

lated | Immediate Consequence | Additional Consequences

15(a) - Using rights to break laws | Rights request denied | Prosecution under violated law (IPC, PMLA, etc.)

15(b) - False/frivolous complaints | Complaint dismissed | Possible defamation case + Vexatious litigant designation + Board may refuse future complaints

15(c) - Impersonation | Service denied / Account suspended | IPC Sections 416-419 (imprisonment up to 3 years) + IT Act Section 66C (identity theft)

15(d) - Suppression | Application rejected / Service denied | Possible fraud case + Contractual breach + Blacklisting

15(e) - False correction claims | Correction/erasure denied | IPC Section 177 (furnishing false information) + Possible fraud case

9.2 Good Faith Defense

CRITICAL SAFEGUARD: Section 15 targets bad faith violations. Good faith mistakes/errors are NOT violations:

☐ Good Faith Defense Examples

Scenario 1: Mistaken Complaint

You filed complaint believing company violated your rights. Investigation shows they didn't. You genuinely believed they did.

Result: ☐ NOT a violation of 15(b) - honest mistake, good faith

Scenario 2: Document Error

You provided what you believed was correct ID, but turns out it had administrative error from issuing authority. Result: ☐ NOT a violation of 15(c) - you didn't intentionally impersonate

Scenario 3: Misunderstanding Legal Requirement

You didn't disclose something because you genuinely didn't know law required it. Result: ☐ NOT a violation of 15(d) - lack of knowledge, not intentional suppression

Scenario 4: Reasonable Belief in Correction

You request correction believing data is wrong based on your records. Turns out your records were mistaken. Result: ☐ NOT a violation of 15(e) - reasonable belief, not false claim

Burden of Proof: Accuser must prove bad faith (intentional violation). If you can show good faith, no violation.

10. Comparative Analysis: Duties in Other Jurisdictions

Jurisdiction | Data Principal Duties/Obligations

India (DPDPA)

[recovered from the vector store — section15.html p.12]

| • Explicit duties section (Section 15) • Five specific duties • Balances rights with responsibilities
EU (GDPR) | • NO explicit "duties" section • Implicit: rights must be exercised in good faith •
Controllers can refuse manifestly unfounded/excessive requests (Art 12)
UK (UK GDPR) | • Similar to EU GDPR • No explicit duties • Good faith implied
USA (CCPA) | • NO explicit duties • Businesses can deny requests if unverifiable • No bad faith
prevention provision
Singapore (PDPA) | • NO explicit duties section • Focuses on organization obligations
South Africa (POPIA) | • Data subjects must provide accurate info (implicit) • No comprehensive duties
section

India's Approach is Unique:

☐ Most explicit duties section globally

☐ Balances individual rights with societal interests

☐ Prevents system abuse proactively

☐ Aligned with Indian constitutional tradition (Fundamental Duties in Article 51A)

Why GDPR Doesn't Have Explicit Duties:

European legal tradition emphasizes individual rights more strongly

Relies on general principles of good faith (civil law concept)

Controllers can refuse unreasonable requests (built-in safeguard)

India's Approach Advantage: Clarity.

Data Principals know exactly what they can/cannot do.

11. Conclusion: Rights & Responsibilities in Balance

Section 15 completes the DPDPA framework by recognizing a fundamental truth: Rights without responsibilities lead to chaos.

"Freedom is not the absence of commitments, but the ability to choose - and commit myself to - what is best for me." - Paulo Coelho

Section 15 ensures data rights remain meaningful by preventing their abuse.

The Five Duties - Final Summary:

Comply with laws (15(a)): Don't use data rights to break other laws

No frivolous complaints (15(b)): Don't spam or abuse grievance systems

No impersonation (15(c)): Don't pretend to be someone else

No suppression (15(d)): Don't hide legally required information

Authentic information (15(e)): Correction requests must be truthful

[recovered from the vector store — section15.html p.13]

Remember:

- ☑ Good faith mistakes are OK - Section 15 targets intentional bad actors, not honest errors
- ☑ Your rights remain strong - Duties don't diminish rights, they protect them from abuse
- ☑ Balance is key - Exercise rights responsibly, and they'll remain effective for everyone

Section 15 ensures the DPDPA system works for everyone by preventing the few from ruining it for the many.

Comprehensive Legal Interpretation Complete

Section 15 DPDPA 2023 - Duties of Data Principal

- ☑ Five duties comprehensively analyzed
- ☑ Philosophical foundations (Kant, Rousseau, Aristotle)
- ☑ Constitutional framework (Article 51A parallel)
- ☑ 30+ violation examples with consequences
- ☑ Good faith defense explained
- ☑ Legitimate vs illegitimate use clarified
- ☑ Material information requirements
- ☑ False vs mistaken complaints distinguished
- ☑ Global comparison (GDPR, CCPA, PDPA)
- ☑ Practical guidance for compliance

© 2026 Prepared by Advocate (Dr.) Prashant Mali

International Data Protection Lawyer | Cyber Law Expert