

[recovered from the vector store — section12.html p.1]

Section 12 DPDPA

Right to correction and erasure of personal data.

12.(1) A Data Principal shall have the right to correction, completion, updating and erasure of her personal data for the processing of which she has previously given consent, including consent as referred to in clause (a) of section 7, in accordance with any requirement or procedure under any law for the time being in force.

(2) A Data Fiduciary shall, upon receiving a request for correction, completion or updating from a Data Principal,—

(a) correct the inaccurate or misleading personal data;

(b) complete the incomplete personal data;

(c) update the personal data.

(3) A Data Principal shall make a request in such manner as may be prescribed to the Data Fiduciary for erasure of her personal data, and upon receipt of such a request, the Data Fiduciary shall erase her personal data unless retention of the same is necessary for the specified purpose or for compliance with any law for the time being in force.

Applicable DPDP Rule 2025

Rule 13: Rights of Data Principals

← Section 11 DPDPA

Section 13 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 12 of the Digital Personal Data Protection Act, 2023

"To err is human; to correct is divine. To erase is your right." - Adapted from Alexander Pope

Section 12 - Right to Correction and Erasure of Personal Data

Statutory Text

Section 12(1). The Data Principal shall have the right to correction, completion, updating and erasure of her personal data.

Section 12(2). A Data Principal, who has consented to the processing of her personal data by a Data Fiduciary, shall have the right to—

correct such personal data that is inaccurate or m

[recovered from the vector store — section12.html p.2]

is leading;

complete such personal data that is incomplete; and

update such personal data where there is any change therein,

in a Data Fiduciary's records in such manner as may be prescribed.

Section 12(3). Where correction, completion or updating of personal data is carried out by the Data Fiduciary pursuant to any request made by the Data Principal under sub-section (2), the Data Fiduciary shall—

intimate such correction, completion or updating to all other Data Fiduciaries and Data Processors with whom the Data Fiduciary has shared such personal data, in such manner as may be prescribed;

take reasonable steps to ensure that the Data Fiduciaries and Data Processors so intimated, shall carry out such correction, completion or updating in their respective records, as applicable, in such manner as may be prescribed; and

intimate to the Data Principal the details of all other Data Fiduciaries and Data Processors with whom she may herself seek correction, completion or updating in such manner as may be prescribed.

Section 12(4). A Data Principal, who has consented to the processing of her personal data by a Data Fiduciary, shall have the right to request erasure of her personal data by the Data Fiduciary in such manner as may be prescribed.

Section 12(5). Nothing in this section shall be construed as requiring the Data Fiduciary to alter or erase any personal data if—

such alteration or erasure is not feasible or involves disproportionate effort from its Data Fiduciary;
or

such personal data is retained as mandated by any law for the time being in force or may be necessary for compliance with any judgment or order of any court or tribunal or other judicial or quasi-judicial authority.

Applicable DPDP Rules 2025:

Rule 13: Rights of Data Principals (procedures for correction, erasure requests)

Table of Contents

Executive Summary: The Rights of Rectification & Deletion

Philosophical Foundations: Dignity & Autonomy

Constitutional Framework: Reputation & Lib

[recovered from the vector store — section12.html p.3]

Section 12(3): Ripple Effect Obligations

Section 12(5): Exceptions to Correction/Erasure

Comparative Analysis: DPDPA vs GDPR "Right to be Forgotten"

Practical Compliance Guidance

1. Executive Summary: The Rights of Rectification & Deletion

Section 12 recognizes a fundamental truth: data about you should be accurate, and you should be able to delete it when you no longer want it processed. This section grants Data Principals FOUR distinct rights:

Right | What It Means | Example | Section

CORRECTION | Fix wrong/misleading data | Name misspelled as "Jon" instead of "John" | 12(2)(a)

COMPLETION | Add missing data | Apartment number missing from address | 12(2)(b)

UPDATING | Change outdated data | Old phone number, moved to new city | 12(2)(c)

ERASURE | Delete data entirely | "I want my account and all data deleted" | 12(4)

🔗 The Data Accuracy Imperative

Why Accuracy Matters:

Scenario 1: Credit Scoring

Bank's database shows: "Loan Default: Yes"

Reality: You never defaulted. It's someone else with similar name. Impact: Denied loans, credit cards, housing for YEARS. Without Section 12: You're powerless to fix it. With Section 12: You can demand correction + bank must fix it with all entities they shared it with. Scenario 2: Medical Records

Hospital records show: "Allergic to Penicillin"

Reality: You're NOT allergic. Wrong patient's data. Impact: Denied life-saving antibiotic in emergency. Without Section 12: Error persists, potentially fatal. With Section 12: Correction right can save your life. The Stakes: Inaccurate data isn't just annoying - it can destroy opportunities, damage reputation, or literally kill you. 1.1 The Ripple Effect: Section 12(3)'s Innovation

Section 12(3) is a game-changer. It's not enough to correct data with one Data Fiduciary. The correction must ripple through the entire data ecosystem.

How It Works:

You request

[recovered from the vector store — section12.html p.4]

t correction: "My name is spelled wrong"

Data Fiduciary A corrects it

Data Fiduciary A must notify: All other Data Fiduciaries and Processors they shared your data with

Those entities must correct it too

You're informed: Of all entities, so you can verify correction happened

Why Revolutionary: In the pre-DPDPA world, you'd have to chase down every single entity individually. Now, one correction request cascades through the entire system.

2. Philosophical Foundations: Dignity & Autonomy

2.1 Immanuel Kant: Dignity Requires Truth

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 Data Correction: If everyone's data were perpetually wrong and uncorrectable, society would collapse (no trust in databases, records, identities). Therefore, there must be a right to correction. Dignity Connection: To be defined by FALSE information is to have your dignity violated. Section 12 restores dignity by ensuring data reflects truth. 2.2 John Locke: Property in One's Person

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

Data as Extension of Person: Data about you is an extension of your person. If you have property rights in your person, you have rights in your data - including the right to ensure it's accurate and the right to delete it. 2.3 Viktor Mayer-Schönberger: Delete

Mayer-Schönberger, "Delete: The Virtue of Forgetting in the Digital Age" (2009):

Argued that human forgetting is a feature, not a bug.
Digital permanence (inability to delete) threatens:

Personal growth: Past mistakes follow forever

Social trust: No second chances

Innovation: Fear of permanent record stifles risk-taking

Section 12(4) implements erasure right - digital approximation of human forgetting.

2.4 Academic Research on Data Accuracy

Key Studies:

Federal Trade Commission (2012) - Report on credit reporting accuracy.

Found 26% of credit reports conta

[recovered from the vector store — section12.html p.5]

in errors, 5% had errors serious enough to affect lending decisions.

Proposition: Without correction rights, error rates would be even higher.

Gellman & Dixon (2013) - "Data Brokers: A Call for Transparency and Accountability"

Documented pervasive errors in data broker databases, with no easy way for individuals to correct them.

Section 12 addresses these documented problems.

3. Constitutional Framework: Reputation & Liberty

3.1 Right to Reputation (Article 21)

Vishwanath Agrawal v. Sarla Vishwanath Agrawal, (2012) 7 SCC 288

Supreme Court: "The right to reputation is an inseparable aspect of Article 21 of the Constitution.

Reputation is an inseparable part of the right to life and right to live with dignity."

Connection to Section 12: Inaccurate data damages reputation. Right to correction protects reputation by ensuring data is truthful.

3.2 Puttaswamy: Informational Control

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

Recognized informational self-determination as core of privacy.

Three Pillars:

Right to control WHO gets data (Consent - Section 6)

Right to know WHAT is being done (Access - Section 11)

Right to correct and delete (Correction & Erasure - Section 12)

4. Section 12(1): Four Rights Overview

Statutory Language: "The Data Principal shall have the right to correction, completion, updating and erasure of her personal data."

This is the umbrella provision - declaring four rights that are detailed in subsequent subsections.

4.1 Distinction: Correction vs. Completion vs. Updating

Right | When to Use | Example | Result

CORRECTION | Data is WRONG | Name: "Rajesh Kumar" → Should be "Rajesh Gupta" | Replace wrong with right

COMPLETION | Data is INCOMPLETE | Address: "123 Main St" → Missing: "Apt 4B" | Add missing information

UPDATING | Data WAS right, now OUTDATED | Phone: "+91-98765-43210" → New: "+91-99876-54321" | Replace old with new

ERASURE | Don't want data processed anymore | "Delete my entire acc

[recovered from the vector store – section12.html p.6]

5. Section 12(2): Right to Correction

Statutory Language: "A Data Principal, who has consented to the processing of her personal data by a Data Fiduciary, shall have the right to—(a) correct such personal data that is inaccurate or misleading; (b) complete such personal data that is incomplete; and (c) update such personal data where there is any change therein..."

5.1 Right to Correct "Inaccurate or Misleading" Data

❓ Correction Scenarios

Scenario 1: Misspelled Name

Current Data: Name: "Jon Smith"

Actual: Name: "John Smith"

Request: "Please correct my name spelling from Jon to John"

Result: Data Fiduciary must correct ❓

Scenario 2: Wrong Birth Date

Current Data: DOB: "15/03/1985"

Actual: DOB: "15/03/1995"

Request: "My birth year is wrong - should be 1995, not 1985"

Result: Data Fiduciary must correct ❓

Scenario 3: Incorrect Transaction Status

Current Data: "Payment Failed"

Actual: Payment succeeded (bank confirms)

Request: "Transaction shows failed but actually succeeded"

Result: Data Fiduciary must correct ❓

Scenario 4: Misleading Incomplete Information

Current Data: "Complaint Filed: Customer Quality Issue"

Missing Context: Complaint was resolved, customer satisfied, withdrawal requested

Request: "Please add resolution details - complaint was resolved"

Result: Data Fiduciary must complete/correct ❓

5.2 What is "Misleading" Data?

"Misleading" includes technically accurate data that gives false impression.

❓❓ Misleading Data Examples

Example 1: Selective Recording

Data: "Customer complained about product quality"

What's Missing: "...but later withdrew complaint after explanation"

Why Misleading: Partial truth creates false negative impression

Correction Right: ? You can demand complete context

Example 2: Outdated Criminal Record

Data: "Arrested for shoplifting, 2015"

What's Missing: "Charges dropped, case dismissed, innocent"

Why Misleading: Arrest ≠ guilt. Record without outcome is mislead

[recovered from the vector store — section12.html p.7]

ng.

Correction Right: ? You can demand completion with outcome

5.3 Burden of Proof: Who Proves Accuracy?

Critical Question: If you claim data is wrong, who has burden to prove it?

Answer: You (Data Principal) must provide evidence that data is inaccurate.

Practical Examples:

Claim | Evidence Required | Likely Result

"My name is misspelled" | Aadhaar card, passport, official ID | ? Correction granted

"I never made this purchase" | Bank statement (no charge), alternate evidence | ? Correction likely if proof solid

"I paid this bill" | Payment receipt, bank confirmation | ? Correction granted

"I don't like this review" | No evidence it's inaccurate, just dislike | ? Correction denied (opinion, not inaccuracy)

6. Section 12(3): Ripple Effect Obligations

This is Section 12's most powerful provision. When Data Fiduciary corrects your data, they must:

6.1 Three Mandatory Actions

Action 1: Intimate Other Data Fiduciaries/Processors (12(3)(a))

Tell everyone you shared data with about the correction. Action 2: Take Reasonable Steps for Downstream Correction (12(3)(b))

Ensure those entities also correct it in their records. Action 3: Inform Data Principal (12(3)(c))

Tell you WHO has your data, so you can verify corrections. ? The Correction Cascade in Action

Scenario: Credit Score Error

Step 1: You discover error

Your credit report shows: "Loan Default 2023"

Reality: No default. You paid on time. Bank error. Step 2: You request correction

Email to Bank: "Section 12 correction request - I never defaulted on loan account XYZ. See attached payment proofs."

Step 3: Bank corrects its records

Bank verifies, corrects internal database. Step 4: Bank notifies downstream entities (Section 12(3)(a))

Bank emails:

Credit Bureau A

Credit Bureau B

Credit Rating Agency C

Data Analytics Company D

"Correction: Customer Account XYZ - No default occurred.

[recovered from the vector store — section12.html p.8]

r databases to remove default record.

Step 6: Bank informs you (Section 12(3)(c))

"Your correction has been processed. We have notified:

CIBIL (Credit Bureau A)

Experian (Credit Bureau B)

CRIF High Mark (Credit Rating Agency C)

Data Analytics Pvt Ltd (Company D)"

"You may contact them directly to verify correction."

Step 7: You verify

Check your credit reports - error corrected everywhere!

Why This Matters: Without Section 12(3), you'd have to individually contact Bank, then CIBIL, then Experian, then High Mark, then Analytics company... Taking MONTHS. Section 12(3) does it automatically.

6.2 "Reasonable Steps" Standard

What are "reasonable steps"?

Data Fiduciary must:

- ☐ Send formal notification to downstream entities
 - ☐ Follow up if no response
 - ☐ Use contractual mechanisms to require downstream correction
 - ☐ Keep records of notification
 - ☐ Not required: Physically monitor downstream entities' databases
 - ☐ Not required: Guarantee correction if downstream entity refuses (but must report this)
7. Section 12(4): Right to Erasure

Statutory Language: "A Data Principal, who has consented to the processing of her personal data by a Data Fiduciary, shall have the right to request erasure of her personal data by the Data Fiduciary..."

This is India's version of the "Right to be Forgotten" - though DPDPA doesn't use that term.

7.1 What is "Erasure"?

Erasure = Permanent deletion + inability to reconstruct.

Action | Counts as Erasure? | Explanation

Permanent deletion from all systems | ☒ YES | True erasure

Deletion from production, remains in backup (deleted from backup within 90 days) | ☒ YES | Reasonable approach - backups eventually erased

Anonymization (data de-identified, can't be linked back) | ☒ YES | Functionally equivalent to erasure

Moving to "inactive" folder but still accessible | ☐ NO | Not deleted, just hidden

Deletion from main DB but remains in logs | ☐ ☐ DEPENDS | If logs are temporary (30 days), OK. If permanent logs, NOT erasure

"Soft dele

[recovered from the vector store — section12.html p.9]

te" (flagged as deleted, still in database) | ❌ NO | Still exists, just marked deleted

7.2 When Can You Request Erasure?

❓ Valid Erasure Requests

Scenario 1: Purpose Fulfilled

"I completed my purchase. You no longer need my data."

Fiduciary Response: ❓ Must erase (unless legal retention requirement)

Scenario 2: Consent Withdrawn

"I withdraw my consent for marketing. Delete my data."

Fiduciary Response: ❓ Must erase marketing data (can retain transaction data if legally required)

Scenario 3: Service No Longer Wanted

"I'm closing my account. Delete everything."

Fiduciary Response: ❓ Must erase (except data with legal retention requirement)

Scenario 4: Data No Longer Relevant

"This browsing history from 5 years ago - please delete it."

Fiduciary Response: ❓ Should be deleted under Section 9(1)(b) anyway

7.3 Erasure is Not "Delete and Forget"

Important: Section 12(4) gives you right to request erasure. Data Fiduciary must evaluate request against exceptions in Section 12(5).

8. Section 12(5): Exceptions to Correction/Erasure

Data Fiduciary can REFUSE correction/erasure if:

8.1 Exception #1: Disproportionate Effort (12(5)(a))

Statutory Language: "such alteration or erasure is not feasible or involves disproportionate effort from its Data Fiduciary"

❓❓ Proportionality Analysis

Proportionate (Must Comply):

Correcting name in standard database field

Deleting customer account

Updating email address

Erasing browsing history

Disproportionate (Can Refuse):

Editing your face out of 10,000 photos taken at public event

Removing your name from printed, distributed physical books

Reconstructing years of archived data from backup tapes to find and delete one record

Correcting data scattered across 500 legacy systems with no integration

Borderline Cases:

Deleting data from 5 interconnected systems: Proportionate (modern architecture should handle this)

Correcting data that requires manual review of 1000s of records: Depends (was Data Fiduciary negligence)

[recovered from the vector store — section12.html p.10]

nt in creating such system?)

Key Principle: Data Fiduciary cannot claim "disproportionate effort" if the difficulty is due to their own poor data management practices.

8.2 Exception #2: Legal Retention Requirement (12(5)(b))

Statutory Language: "such personal data is retained as mandated by any law for the time being in force or may be necessary for compliance with any judgment or order of any court or tribunal..."

❓ When Erasure Cannot Happen

Legal Retention Requirements:

1. Tax Records (Income Tax Act)

Retention Period: 6 years

Your Request: "Delete my payment records from 2 years ago"

Fiduciary Response: ❓ Cannot erase (legal requirement)

2. Company Financial Records (Companies Act)

Retention Period: 8 years

Your Request: "Delete my invoice from 2023"

Fiduciary Response: ❓ Cannot erase until 2031

3. KYC Documents (PMLA)

Retention Period: 5 years after account closure

Your Request: "Close my bank account and delete my KYC immediately"

Fiduciary Response: ❓ Account closed, but KYC retained for 5 years

4. Ongoing Litigation

Situation: You're party to lawsuit, your data is evidence

Your Request: "Delete data related to this contract dispute"

Fiduciary Response: ❓ Cannot erase (court may need evidence)

5. Criminal Investigation

Situation: Police investigating fraud, your transaction data is evidence

Your Request: "Delete my transaction history"

Fiduciary Response: ❓ Cannot erase (may be required for prosecution)

8.3 Partial Erasure Solution

Smart Approach: Delete what can be deleted, retain only what's legally required.

Example:

Your Request: "Delete my account and all data"

Fiduciary Analysis:

Profile information (name, photo, bio): ⓘ Can delete

Browsing history: ⓘ Can delete

Preference settings: ⓘ Can delete

Transaction records from last 3 years: ⓘ Must retain for tax compliance (6 years)

KYC documents: ⓘ Must retain (PMLA requirement)

Fiduciary Response:

"We have deleted your profile, browsing history, and preferences. However,

[recovered from the vector store — section12.html p.11]

we must retain transaction records (tax law) and KYC documents (PMLA) for [X years]. These will be deleted automatically when retention period expires."

This is compliant - erase what can be erased, document why remainder is retained.

9. Comparative Analysis: DPDPA vs GDPR "Right to be Forgotten"

Aspect | India (DPDPA Sec 12) | EU (GDPR Art 16, 17)

Right Name | Right to Correction and Erasure | Right to Rectification & Right to be Forgotten (Erasure)

Scope | Consent-based processing | All processing (wider scope)

Correction Right | ☒ Yes (12(2)) | ☒ Yes (Art 16)

Completion Right | ☒ Explicit (12(2)(b)) | ☒ Yes (Art 16)

Updating Right | ☒ Explicit (12(2)(c)) | ☒ Covered under rectification

Erasure Right | ☒ Yes (12(4)) | ☒ Yes (Art 17)

Ripple Effect | ☒ Mandatory (12(3) - must notify downstream) | ☒ Similar (Art 19 - communicate to recipients)

Exceptions | 2: Disproportionate effort, Legal retention | 6 exceptions (freedom of expression, legal claims, public interest, etc.)

Search Engine Delisting | Not explicit in DPDPA | ☒ Yes (Google Spain case established this)

Public Interest Exception | Not explicit | ☒ Yes (journalism, public interest research exempt)

9.1 The Google Spain Case: Right to be Forgotten

Google Spain v. AEPD and Mario Costeja González, CJEU C-131/12 (2014)

Facts: Spanish citizen's decades-old debt was searchable on Google. He requested Google delist the search results.

Holding: EU citizens have right to request search engines remove links to information about them if information is "inadequate, irrelevant, or excessive."

DPDPA Position: Section 12 doesn't explicitly address search engines. However:

If search engine is Data Fiduciary (processing user data), Section 12 applies

If search engine merely links to others' content, unclear

Likely will require judicial interpretation or future amendment

10. Practical Compliance Guidance

10.1 Sample Correction Request

☒ Correction Request Template

Subject: Section 12 DPDPA Correction Request -

[recovered from the vector store — section12.html p.12]

I am writing to exercise my right to correction under Section 12(2) of the Digital Personal Data Protection Act, 2023.

Evidence: Please see attached [Aadhaar card/Passport/other official document] showing correct date of birth.

Please also notify all Data Fiduciaries and Data Processors with whom you have shared my data, and provide me with their identities so I can verify correction.

I look forward to your response within 30 days as required by Rule 13.

Subject: Section 12(4) DPDPA Erasure Request - [Your Name]

I am writing to exercise my right to erasure under Section 12(4) of the Digital Personal Data Protection Act, 2023.

I request complete erasure of all my personal data from your systems, including:

All other personal data you hold about me

Reason for Request: [Optional: "I no longer use your services" / "Purpose of processing has been fulfilled" / "I withdraw my consent"]

You may retain data required by law (please specify retention period)

Erasure may take up to 90 days for backup systems

Please confirm erasure within 30 days and provide details of any data retained due to legal requirements.

10.3 Compliance Checklist for Data Fiduciaries

[recovered from the vector store — section12.html p.13]

CORRECTION INFRASTRUCTURE:

- ☐ System to receive correction requests
- ☐ Identity verification before making changes
- ☐ Data correction workflows
- ☐ Evidence evaluation procedures
- ☐ Downstream notification system (12(3))
- ☐ Correction tracking and logging

ERASURE INFRASTRUCTURE:

- ☐ Data deletion capabilities across all systems
- ☐ Backup erasure procedures
- ☐ Anonymization capabilities (alternative to deletion)
- ☐ Legal retention period tracking
- ☐ Partial erasure workflows
- ☐ Deletion verification mechanisms

RIPPLE EFFECT COMPLIANCE (12(3)):

- ☐ Registry of all downstream Data Fiduciaries/Processors
- ☐ Contractual obligations for downstream correction
- ☐ Automated notification system
- ☐ Follow-up procedures if no response
- ☐ Documentation of notifications sent
- ☐ System to inform Data Principal of downstream entities

EXCEPTION HANDLING:

- ☐ Legal retention requirements documented
- ☐ Proportionality assessment procedures
- ☐ Process to explain refusals to Data Principals
- ☐ Partial erasure capabilities
- ☐ Annual review of retained data

TIMELINE COMPLIANCE:

- ☐ 30-day response deadline tracking
- ☐ Automated acknowledgments
- ☐ Escalation for complex requests

❓ Progress updates to Data Principals

10.4 Common Section 12 Violations

❓ Top 15 Correction/Erasure Violations

1. Ignoring Correction Requests

❓ No response to correction request

Penalty: ₹200 crores

2. Refusing Valid Corrections

❓ "We don't need to fix it" (when data is clearly wrong)

Penalty: ₹200 crores

3. No Downstream Notification

❓ Correcting data but not telling entities you shared with

Penalty: ₹200 crores (violates 12(3))

4. Fake Erasure

❓ "Deleted" but data still exists in systems

Penalty: ₹200 crores

5. Excessive Retention

❓ Claiming "legal requirement" when none exists

Penalty: ₹200 crores

6. No Evidence Evaluation

❓ Refusing correction without evaluating evidence

Penalty: ₹200 crores

7. Delaying Correction

❓ Taking 6 months to fix simple spelling error

Penalty: ₹200 crores

[recovered from the vector store — section12.html p.14]

ncomplete Erasure

❓ Deleting account but keeping browsing history

Penalty: ₹200 crores

9. No Downstream Follow-Up

❓ Notifying once, never checking if correction happened

Penalty: ₹200 crores (fails "reasonable steps")

10. Retaliation

❓ Degrading service after correction request

Penalty: ₹200 crores

11. False Disproportionality Claim

❓ "Too difficult" when it's standard database update

Penalty: ₹200 crores

12. Charging Fees

❓ "Pay ₹5000 to correct your data"

Penalty: ₹200 crores (correction should be free)

13. Requiring Excessive Proof

❓ "Provide notarized affidavit to fix spelling error"

Penalty: ₹200 crores (unreasonable burden)

14. Backup Excuse Forever

❓ "We can't delete from backups" (never deleted)

Penalty: ₹200 crores (reasonable time: 90 days max)

15. No Communication

❓ Not informing Data Principal about downstream entities

Penalty: ₹200 crores (violates 12(3)(c))

11. Conclusion: The Power to Correct and Delete

Section 12 gives Data Principals two fundamental powers:

The power to ensure truth: Correction rights ensure data about you is accurate

The power to be forgotten: Erasure rights let you exit the digital record

These aren't just technical rights - they're essential to human dignity.

"To be defined by falsehoods is to have your identity stolen. To have no ability to erase your past is to have no ability to change your future."

Section 12 protects both: the right to truth and the right to move on.

Key Principles to Remember:

Four Rights: Correction, Completion, Updating, Erasure

Ripple Effect: Corrections cascade to all downstream entities (12(3))

Burden of Proof: You must prove data is wrong (reasonable standard)

True Erasure: Not just "soft delete" - permanent removal

Two Exceptions: Disproportionate effort, Legal retention

Partial Erasure: Delete what can be deleted, retain only legally required

30-Day Timeline: Same as other data rights

Section 12 recognizes that control over your data includes the power to fix i

[recovered from the vector store — section12.html p.15]

t and the power to end it.

Comprehensive Legal Interpretation Complete

Section 12 DPDPA 2023 - Right to Correction and Erasure of Personal Data

🔍 Four distinct rights explained

🔍 Ripple effect obligations (12(3))

🔍 Philosophical foundations (Kant, Locke, Mayer-Schönberger)

🔍 Constitutional framework (reputation, Puttaswamy)

🔍 Correction vs completion vs updating clarified

🔍 True erasure standards

🔍 Two exceptions analyzed

🔍 GDPR comparison (Google Spain case)

🔍 Sample request templates

🔍 Compliance checklists

🔍 15 common violations

© 2026 Prepared by Advocate (Dr.) Prashant Mali

International Data Protection Lawyer | Cyber Law Expert