[recovered from the vector store — section11.html p.1]

Section 11 DPDPA

Right to access information about personal data. 11.(1) The Data Principal shall have the right to obtain from the Data Fiduciary to whom she has previously given consent, including consent as referred to in clause (a) of section 7 (hereinafter referred to as the said Data Fiduciary), for processing of personal data, upon making to it a request in such manner as may be prescribed,—

(a) a summary of personal data which is being processed by such Data Fiduciary and the processing activities undertaken by that Data Fiduciary with respect to such personal data; (b) the identities of all other Data Fiduciaries and Data Processors with whom the personal data has been shared by such Data Fiduciary, along with a description of the personal data so shared; and

(c) any other information related to the personal data of such Data Principal and its processing, as may be prescribed.
(2) Nothing contained in clause (b) or clause (c) of sub-section (1) shall apply in respect of the sharing of any personal data by the said Data Fiduciary with any other Data Fiduciary authorised by law to obtain such personal data, where such sharing is pursuantto a request made in writing by such other Data Fiduciary for the purpose of prevention or detection or investigation of offences or cyber incidents, or for prosecution or punishment of offences. Applicable DPDP Rule 2025

Rule 13: Rights of Data Principals

← Section 10 DPDPA

Section 12 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 11 of the Digital Personal Data Protection Act, 2023

"Knowledge is power. Information is liberating." - Kofi Annan

Section 11 - Right to Access Information About Personal Data

Sta

[recovered from the vector store — section11.html p.2]

Section 11(1). The Data Principal shall have the right to obtain from the Data Fiduciary to whom she has previously given consent, including consent as referred to in clause (a) of section 7 (hereinafter referred to as the said Data Fiduciary), for processing of personal data, upon making to it a request in such manner as may be prescribed,—

a summary of personal data which is being processed by such Data Fiduciary and the processing activities undertaken by that Data Fiduciary with respect to such personal data;

the identities of all other Data Fiduciaries and Data Processors with whom the personal data has been shared by such Data Fiduciary, along with a description of the personal data so shared; and

any other information related to the personal data of such Data Principal and its processing, as may be prescribed.
Section 11(2). Nothing contained in clause (b) or clause (c) of sub-section (1) shall apply in respect of the sharing of any personal data by the said Data Fiduciary with any other Data Fiduciary authorised by law to obtain such personal data, where such sharing is pursuant to a request made in writing by such other Data Fiduciary for the purpose of prevention or detection or investigation of offences or cyber incidents, or for prosecution or punishment of offences.

Applicable DPDP Rules 2025:

Rule 13: Rights of Data Principals (manner of making requests, timeline for response, format of information)

Table of Contents

[recovered from the vector store — section11.html p.3]

Section 11 is the "transparency cornerstone" of the DPDPA. It gives Data Principals the fundamental right to ask: "What do you know about me?"

This isn't just paperwork - it's informational self-determination in action.  The Knowledge Asymmetry Problem

The Old World (Pre-DPDPA):

Data Fiduciary knows:

What data they have about you

How they're using it

Who they're sharing it with

How long they're keeping it

What algorithms are processing it

Data Principal (You) knows:

...Nothing. You gave your data years ago

You have no idea what they've done with it

You're kept in the dark

Result: Massive power imbalance. Companies know everything about you; you know nothing about what they know. The New World (Section 11):

Data Principals can demand answers:

"Show me what data you have about me"

"Tell me what you're doing with my data"

"Who have you shared my data with?"

Result: Symmetry restored. Knowledge = Power. Transparency = Accountability.
1.1 The Three Pillars of Access Rights

Subsection | What You Can Request | Purpose | Penalty for Non-Compliance
11(1)(a) | Summary of your data + processing activities | Know WHAT data exists & HOW it's used | Up to ₹200 crores (Schedule Item 3)
11(1)(b) | Who your data has been shared with | Know WHO has your data | Up to ₹200 crores (Schedule Item 3)
11(1)(c) | Other prescribed information | Future-proofing provision | Up to ₹200 crores (Schedule Item 3)

1.2 Critical Limitation: Consent-Based Only

Key Text: "The Data Principal shall have the right to obtain from the Data Fiduciary to whom she has previously given consent..."

This means:

 Section 11 applies when you CONSENTED to processing

 Section 11 does NOT apply to Section 7 processing (legitimate uses without consent) - EXCEPT Section 7(a)

 Section 11 Applicability Matrix

Processing Basis | Section 11 Applies? | Explanation

Section 4 - Consent | ☑ YES | You consented → You can request access

[recovered from the vector store — section11.html p.4]

loyer employee | ? YES | Explicitly included in 11(1)

Section 7(b) - State functions | ? NO | No consent given

Section 7(c) - Legal obligation | ? NO | No consent given

Section 7(d) - Medical emergency | ? NO | No consent given

Section 7(e)-(j) | ? NO | Legitimate uses without consent

Practical Impact: If government processes your Aadhaar data for welfare schemes (Section 7(b)), you CANNOT use Section 11 to request access. Use RTI Act instead.

2. Philosophical Foundations: Transparency & Accountability

2.1 John Stuart Mill: Information as Liberty

Mill, On Liberty (1859): "If all mankind minus one, were of one opinion, and only one person were of the contrary opinion, mankind would be no more justified in silencing that one person, than he, if he had the power, would be justified in silencing mankind."

Data Protection Application: Information asymmetry = silencing. When organizations know everything about you but you know nothing about what they know, you're effectively silenced in the data relationship. Section 11 restores voice by giving Data Principals the right to demand transparency.

2.2 Louis Brandeis: Sunlight as Disinfectant

Justice Louis Brandeis (1914): "Sunlight is said to be the best of disinfectants; electric light the most efficient policeman."

Section 11 Implementation:

Sunlight = Transparency: Data Fiduciaries must disclose what they're doing

Disinfectant = Accountability: Knowing they must disclose deters bad practices

Policeman = Enforcement: Access requests enable Data Principals to detect violations

2.3 Amartya Sen: Development as Freedom

Sen, Development as Freedom (1999): Argued that freedom requires capability - not just absence of constraints, but positive ability to act.

Data Protection Parallel:

Negative Right: "Don't process my data without consent" (Section 4)

Positive Right: "Show me what you're doing with my data" (Section 11)

Section 11 provides the capability to exercise control - not just the abstract right.

2.4 Aca

[recovered from the vector store — section11.html p.5]

demic Research on Access Rights

Key Studies:

Urban et al. (2020) - "The Unwanted Sharing Economy: An Analysis of Cookie Syncing and User Transparency" ACM CCS.

Found that even technically sophisticated users couldn't understand what companies knew about them without explicit disclosure requirements.

Harkous et al. (2018) - "PriBots: Conversational Privacy with Chatbots" SOUPS.

Demonstrated that conversational, accessible privacy information (like Section 11 summaries) dramatically increased user understanding.

Sanchez Chamorro et al. (2020) - "Do Cookie Banners Respect my Choice?" IEEE S&P.

Found that without access rights, users couldn't verify whether their choices were actually being respected.

Section 11 implements these findings: Access enables verification, verification enables trust.
3. Constitutional Framework: Right to Information

3.1 Puttaswamy: Informational Autonomy

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

⁉ Puttaswamy on Informational Self-Determination

Justice D.Y. Chandrachud (Para 164):

"Informational privacy is a facet of the right to privacy. The dangers to privacy in an age of information can originate not only from the State but from non-state actors as well. We commend the Union government to examine and put into place a robust regime for data protection."

Three Components of Informational Privacy:

Right to control: Decide who gets your data (Section 6 - Consent)

Right to know: Know what's being done with your data (Section 11 - Access)

Right to correct: Fix wrong data (Section 12 - Correction)

Section 11 is the legislative implementation of the "right to know" component.

3.2 Article 21: Know Thyself (Digitally)

Supreme Court has held that Article 21 (right to life) includes right to know about oneself.

Mr. X v. Hospital Z, (1998) 8 SCC 296: Court held patient has right to medical information about themselves.

Extension to Digital Context: If you have right to know your medical data, you certainl

[recovered from the vector store — section11.html p.6]

y have right to know your digital data.

3.3 Right to Information Act, 2005 - Parallel Principle

RTI Act gives citizens right to information from public authorities. Section 11 extends this principle to private sector data processing.

Common Philosophy:

RTI: "The state serves the people; people have right to know what state does"

Section 11: "Data Fiduciaries hold data in trust; Data Principals have right to know what Fiduciaries do"

4. Scope of Section 11: Who Can Request?

4.1 "The Data Principal"

Who qualifies?

 You (individual whose data is being processed)

 Your parent (if you're under 18)

 Your guardian (if you have disability affecting capacity)

 Your nominee (after your death, for limited purposes)

 NOT random third parties

 NOT competitors seeking company information

4.2 "To Whom She Has Previously Given Consent"

This is a critical limitation. You can only request access from Data Fiduciaries to whom you:

Gave explicit consent under Section 6, OR

Provided deemed consent under Section 7(a) (employment context)

Cannot request from:

Data Fiduciaries processing under Section 7(b)-(j) (legitimate uses)

Data Fiduciaries you never interacted with

Data brokers who obtained your data from others (unless you originally consented to that sharing)

5. Section 11(1)(a): Summary of Personal Data & Processing Activities

Statutory Language: "a summary of personal data which is being processed by such Data Fiduciary and the processing activities undertaken by that Data Fiduciary with respect to such personal data"

This subsection has TWO components:

5.1 Component 1: Summary of Personal Data

What must be disclosed:

 Compliant "Summary of Personal Data" Response

Example: E-Commerce Platform

Your Personal Data Summary

Request Date: January 9, 2025

Data Fiduciary: ShopEasy India Pvt. Ltd.

1. IDENTITY DATA:

Name: Rajesh Kumar Sharma

Email: rajesh.sharma@email.com

Phone: +91-98765-43210

Date of Birth: March 15, 1985

[recovered from the vector store — section11.html p.7]

ping Address: Flat 202, Palm Heights, MG Road, Pune - 411001

Billing Address: Same as shipping

3. FINANCIAL DATA:

Payment Method: HDFC Credit Card (ending 4567)

Note: We do NOT store full card details. Tokenized reference only.

4. TRANSACTION DATA:

Total Orders: 47

Order Value Range: ₹250 - ₹12,500

Last Order: December 28, 2024

Order Categories: Electronics (15), Books (12), Clothing (10), Home & Kitchen (10)

5. USAGE DATA:

Account Created: March 10, 2020

Last Login: January 8, 2025

Device Types: Mobile (Android), Desktop (Windows)

IP Address Range: Pune region

6. PREFERENCE DATA:

Product Categories You Browse: Tech gadgets, programming books

Email Preferences: Promotional emails (opted in), Order updates (mandatory)

Language: English
7. CUSTOMER SERVICE DATA:

Support Tickets: 3 (all resolved)

Chat Transcripts: Available upon request

Data Retention: Your data will be retained until 2 years after last purchase, or until you request deletion, whichever is earlier.

Why This is Compliant:

 Comprehensive but summarized (not raw database dump)

 Organized by category

 Clear and understandable language

 Shows what data exists

5.2 Component 2: Processing Activities

"...and the processing activities undertaken by that Data Fiduciary..."

This means: "What are you DOING with my data?"

 Compliant "Processing Activities" Response

Processing Activities for Your Data

1. ORDER FULFILLMENT:

Purpose: Process and deliver your orders

Data Used: Name, address, phone, order details, payment info

Processing Type: Automated order management system

Retention: 7 years (tax and warranty purposes)

2. CUSTOMER COMMUNICATION:

Purpose: Send order updates, delivery notifications, customer support

Data Used: Email, phone, order details

Processing Type: Automated email/SMS system

Retention: Duration of customer relationship

[recovered from the vector store — section11.html p.8]

ences

Processing Type: Encrypted database storage

Retention: Until account deletion

4. FRAUD PREVENTION:

Purpose: Detect and prevent fraudulent transactions

Data Used: Transaction patterns, device info, IP address

Processing Type: Automated risk scoring algorithms

Retention: 3 years

5. PERSONALIZATION:

Purpose: Show relevant product recommendations (only with your consent)

Data Used: Browsing history, purchase history

Processing Type: Machine learning recommendation engine

Your Control: You can opt out in settings

Retention: 1 year of activity

6. ANALYTICS:

Purpose: Improve website performance and user experience

Data Used: Aggregated, anonymized usage data

Processing Type: Statistical analysis

Note: Individual-level data not used for analytics
7. LEGAL COMPLIANCE:

Purpose: Comply with tax, accounting, consumer protection laws

Data Used: Transaction records, invoices

Processing Type: Record keeping

Retention: As required by law (typically 7 years)

Why This is Compliant:

 Lists each processing activity

 Explains purpose of each activity

 Specifies what data is used for what purpose

 Indicates retention periods

 Notes where user control exists

5.3 What is NOT Required: Raw Data Dump
Section 11(1)(a) requires a "summary" - not a complete raw database export.

 Over-Compliance vs.  Appropriate Compliance

 Over-Compliance (Not Required):

Every server log entry (millions of lines)

Every cookie value with timestamps

Every API call with technical parameters

Raw database schema with technical column names

Why Excessive: Overwhelming, not useful, defeats purpose of "summary"

 Appropriate Compliance:

Organized summary of data categories

Clear explanation of processing activities

Plain language, not technical jargon

Comprehensible to ordinary person

Why Sufficient: Meets statutory "summary" requirement, enables informed decisions

Legal Standard: Reasonable person test - would a reasonable Data Principal understand what data e

[recovered from the vector store — section11.html p.9]

6. Section 11(1)(b): Data Sharing Disclosure

Statutory Language: "the identities of all other Data Fiduciaries and Data Processors with whom the personal data has been shared by such Data Fiduciary, along with a description of the personal data so shared"

This is the "Who knows about me?" disclosure.

6.1 Two Required Elements

IDENTITIES: Names of all entities data was shared with

DESCRIPTION: What specific data was shared with each entity

 Compliant Data Sharing Disclosure

Data Sharing Report

Your data has been shared with the following entities:

1. DELIVERY PARTNERS (Data Processors)

Entities:

BlueDart Express Ltd.

Delhivery Pvt. Ltd.

Ecom Express Ltd.

Data Shared: Name, delivery address, phone number, order details

Purpose: To deliver your orders

Legal Basis: Necessary for service performance (your consent)

Data Transfer Date Range: March 2020 - December 2024

2. PAYMENT GATEWAY (Data Processor)

Entity: RazorPay Software Pvt. Ltd.

Data Shared: Transaction amount, order ID, email (card details handled directly by gateway, not by us)

Purpose: Process payments

Legal Basis: Necessary for service performance

Data Transfer Date Range: March 2020 - Present
3. CUSTOMER SERVICE PLATFORM (Data Processor)

Entity: Freshdesk Inc. (USA - adequate data protection measures in place)

Data Shared: Name, email, phone, support ticket content

Purpose: Manage customer support inquiries

Legal Basis: Your consent (accepted when using support)

Data Transfer Date Range: March 2020 - Present

4. CLOUD HOSTING PROVIDER (Data Processor)

Entity: Amazon Web Services India Pvt. Ltd.

Data Shared: All account data (stored on their servers)

Purpose: Data hosting and infrastructure

Legal Basis: Necessary for service provision

Security: Encrypted storage, data residency in India

Data Transfer Date Range: March 2020 - Present

5. MARKETING PARTNER (Data Fiduciary)

Entity: EmailMarketing Pro Ltd.

Data Shared: Email address, name, product pr

[recovered from the vector store — section11.html p.10]

eferences (only because you opted in to promotional emails)

Purpose: Send promotional offers

Your Control: You can opt out anytime in email preferences

Data Transfer Date Range: June 2020 - Present

Note: This is the ONLY third-party we share data with for marketing purposes
6. NO OTHER SHARING

We have NOT shared your data with:

 Data brokers

 Advertising networks (we don't do behavioral targeting)

 Social media platforms

 Credit rating agencies

 Any other third parties

Why This is Compliant:

 Names every entity (both Data Fiduciaries and Processors)

 Describes what data was shared with each

 Explains purpose of sharing

 Notes legal basis

 Indicates user control where applicable

 Explicitly states what was NOT shared (for clarity)

6.2 Data Processors vs. Data Fiduciaries: Why Distinction Matters

Entity Type | Relationship | Example | Disclosure Requirement
Data Processor | Processes on your behalf, per your instructions | Cloud hosting provider, email service | Must disclose
Data Fiduciary | Processes for their own purposes, independent relationship | Marketing partner, affiliate | Must disclose
Your Employee | Works for you, accesses data as part of job | Customer service rep, IT admin | Not required (internal access, not "sharing")
7. Section 11(1)(c): Other Prescribed Information

Statutory Language: "any other information related to the personal data of such Data Principal and its processing, as may be prescribed"

This is a future-proofing provision - allows government to add disclosure requirements via Rules as technology evolves.

7.1 Currently Prescribed Information (Rule 13)

DPDP Rules 2025, Rule 13 prescribes additional disclosures:

Data Retention Period: How long each category of data will be kept

Cross-Border Transfers: Countries where data is transferred (if applicable)

Automated Decision-Making: If algorithms are used for decisions affecting the Data Principal

Data Protection Officer Contact: (For SDFs) How to

[recovered from the vector store — section11.html p.11]

contact DPO

Grievance Officer Contact: How to file complaints

Data Breach History: Whether Data Principal's data was involved in any breaches (if yes, details)

7.2 Potential Future Prescribed Information

As technology evolves, government may prescribe disclosure of:

AI training usage (was your data used to train AI models?)

Biometric processing details

Genetic data processing

IoT device data collection specifics

Brain-computer interface data (neurotechnology)

Metaverse/VR behavioral data
8. Section 11(2): Law Enforcement Exception

Statutory Language: "Nothing contained in clause (b) or clause (c) of sub-section (1) shall apply in respect of the sharing of any personal data by the said Data Fiduciary with any other Data Fiduciary authorised by law to obtain such personal data, where such sharing is pursuant to a request made in writing by such other Data Fiduciary for the purpose of prevention or detection or investigation of offences or cyber incidents, or for prosecution or punishment of offences."

This is the "national security and law enforcement" exception. 8.1 What This Means

Normal Situation:

You request access under Section 11(1)(b)

Data Fiduciary must disclose WHO they shared your data with

Exception under 11(2):

If Data Fiduciary shared your data with law enforcement (police, CBI, NIA, etc.) for investigation/prosecution

They do NOT have to disclose this sharing

□□ Why the Exception Exists

Scenario: Police investigating financial fraud. Step 1: Police send written request to bank: "We're investigating fraud. Share transaction data for Account No. 123456789."

Step 2: Bank shares data with police (legally required to comply).
Step 3: Suspect (account holder) submits Section 11 access request: "Who have you shared my data with?"

Without Exception: Bank must disclose: "We shared your data with Police Station XYZ." Suspect knows they're under investigation. Destroys evidence, flees country. With Exception (Section 11(2)): Bank does NOT

[recovered from the vector store — section11.html p.12]

have to disclose police sharing. Investigation integrity preserved.

Why Necessary: Prevents tipping off suspects, protects investigation confidentiality.

Exception applies ONLY if ALL conditions met:

Authorized by Law: Receiving entity must be legally empowered to get data (police, courts, regulators with legal authority)

Written Request: Request must be in writing (not verbal)

Investigation of offences/cyber incidents

Actual Law Enforcement Context: Not just any government request

Private company requests data via court subpoena in civil lawsuit.

Exception Applies? □ NO - not criminal investigation

Tax department requests data for routine tax assessment.

Exception Applies? □ NO - routine compliance, not investigation

SEBI requests data during market surveillance.

Exception Applies? □□ DEPENDS - If part of investigation into market manipulation (offence), then YES. If routine inspection, then NO.

Company shares data with affiliate for marketing.

Exception Applies? □ NO - not law enforcement

8.3 Exception Limited to 11(1)(b) and (c) Only

Important: Section 11(2) exception applies ONLY to subsections (b) and (c).
□ Can hide that data was shared with law enforcement (11(1)(b) exception)

□ Can withhold other prescribed info related to investigation (11(1)(c) exception)

□ CANNOT hide what personal data exists or processing activities (11(1)(a) still applies)

Practical Effect: Even under investigation, you can still see WHAT data the Fiduciary has and WHAT they're doing wit

[recovered from the vector store — section11.html p.13]

9. The Access Request Process (Rule 13)

9.1 How to Make a Section 11 Request

Rule 13 prescribes the manner of making requests:

 Step-by-Step Access Request Process

Step 1: Verify Your Identity

Data Fiduciary can request identity verification to ensure request is from actual Data Principal (not imposter).
Acceptable Methods:

Login to your account (if you have one)

Aadhaar OTP

Registered email/phone verification

Answer security questions

Step 2: Submit Request

Methods:

Online form on Data Fiduciary's website/app

Email to designated data protection contact

Written letter (postal mail)

Through grievance officer contact published under Section 9(1)(c)

Information to Include:

Your name

Contact details

Account identifier (if applicable)

Specific information requested (11(1)(a), (b), (c), or all)

Preferred format for response (email, postal mail, downloadable file)

Step 3: Wait for Response

Timeline (Rule 13):

Acknowledgment: Within 7 days

Full Response: Within 30 days

Extension (if complex): Additional 30 days with justification (total 60 days max)

Step 4: Receive Information

Data Fiduciary must provide information in:

Commonly used format (PDF, DOC, Excel)

Plain language

Structured, easy to understand

Free of charge (first request)

Step 5: Review & Act

After receiving information, you can:

Request correction (Section 12) if data is wrong

Request erasure (Section 13) if no longer needed

Withdraw consent (if you want to stop processing)

File complaint with Data Protection Board if response inadequate

9.2 Frequency of Requests

Rule 13 Limitation:

First request in 12 months: FREE

Subsequent requests in same 12 months: Data Fiduciary may charge reasonable fee

Rationale: Prevents abuse (repeated frivolous requests), but ensures everyone gets at least one free access per year.

[recovered from the vector store — section11.html p.14]

ta Fiduciary Response Obligations

10.1 What Data Fiduciary MUST Do

Obligation | Requirement | Timeline | Penalty for Non-Compliance
Acknowledge | Confirm receipt of request | Within 7 days | Up to ₹200 crores
Verify Identity | Ensure requester is actual Data Principal | Before responding | Data security obligation
Respond | Provide requested information | Within 30 days (extendable to 60) | Up to ₹200 crores
Format | Commonly used, structured format | Upon response | Up to ₹200 crores
Language | Plain, understandable language | Upon response | Up to ₹200 crores
Free (First Request) | No charge for first annual request | N/A | Up to ₹200 crores

10.2 What Data Fiduciary CANNOT Do

 Prohibited Responses

1. Ignore Request

 "We received your request but we're too busy to respond."

Penalty: ₹200 crores

2. Delay Beyond Timeline

 Responding after 60 days without valid justification.

Penalty: ₹200 crores

3. Provide Incomprehensible Data

 Raw database dump with technical jargon, no explanation.

Penalty: ₹200 crores (fails "summary" requirement)

4. Charge Excessive Fees

 ₹10,000 fee for access request.

Penalty: ₹200 crores (unreasonable fee)
5. Refuse Without Valid Reason

 "We don't have to comply with this request" (when Section 11 clearly applies).

Penalty: ₹200 crores

6. Incomplete Response

 Disclosing only some data, hiding other processing activities.

Penalty: ₹200 crores

7. Retaliation

 Closing user's account because they made access request.

Penalty: ₹200 crores (possibly more under Section 9(3)(b))

11. Comparative Analysis: DPDPA vs GDPR vs CCPA

Aspect | India (DPDPA Sec 11) | EU (GDPR Art 15) | USA (CCPA Sec 1798.110)
Right Name | Right to Access Information | Right of Access | Right to Know

Scope | Only consent-based processing + Sec 7(a) | All processing | All processing
Data Summary | ✅ Required | ✅ Required | ✅ Required
Processing Activities | ✅ Required | ✅ Required ("purposes") | ✅ Required ("business purposes")
Third Party Disc

[recovered from the vector store — section11.html p.15]

losure | ✓ Required (11(1)(b)) | ✓ Required (Art 15(1)(c)) | ✓ Required (categories)
Response Timeline | 30 days (extendable to 60) | 1 month (extendable to 3 months) | 45 days (extendable to 90)
Format | Commonly used, structured | Electronic if possible | Portable format
Frequency | First annual request free | Generally free (fee if excessive) | Twice per 12 months
Law Enforcement Exception | ✓ Yes (11(2)) | ✓ Yes (Art 23) | ✓ Yes (various exemptions)
Copy of Data | ⚠ Summary required, full copy not explicit | ✓ Explicit right to copy (Art 15(3)) | ✓ Right to specific pieces

Key Difference: DPDPA's Section 11 applies ONLY to consent-based processing (narrower than GDPR/CCPA). However, for consent-based processing, protection is comprehensive.
12. Practical Compliance Guidance

12.1 Section 11 Compliance Checklist for Data Fiduciaries

✓ Pre-Launch Setup

INFRASTRUCTURE:

✓ Access request submission mechanism (web form, email, etc.)

✓ Identity verification system

✓ Data inventory system (know what data you have)

✓ Processing activity register (know what you do with data)

✓ Third-party sharing log (know who you share with)

✓ Automated report generation system (to respond quickly)

✓ Tracking system for requests (timeline monitoring)

POLICIES & TEMPLATES:

✓ Access request policy documented

✓ Response templates prepared

✓ Identity verification procedures

✓ Fee schedule (for subsequent requests)

✓ Staff training materials

TIMELINE MANAGEMENT:

✓ Auto-acknowledgment system (within 7 days)

✓ Response deadline tracking

✓ Escalation process for complex requests

✓ Extension justification procedures

12.2 Common Section 11 Violations

✓ Top 10 Access Right Violations

1. Ignoring Requests

✓ No response to access request

Penalty: ₹200 crores

2. Excessive Delays

 Responding after 90+ days

Penalty: ₹200 crores

3. Incomplete Disclosure

 Hiding some processing activities

Penalty: ₹200 crores

[recovered from the vector store — section11.html p.16]

xYz123..." (incomprehensible)

Penalty: ₹200 crores

5. Refusing Valid Request

 "We don't process your data" (when clearly they do)

Penalty: ₹200 crores

6. Charging for First Request

 ₹500 fee for first annual request

Penalty: ₹200 crores

7. No Third-Party Disclosure

 Not mentioning data processors/shared entities

Penalty: ₹200 crores

8. Inadequate Identity Verification

 Disclosing data to wrong person (identity theft risk)

Penalty: Security breach (₹250 crores)

9. Retaliation

 Downgrading service after access request

Penalty: ₹200 crores
10. Obstructive Process

 Making access request deliberately difficult (hidden contact, complex forms)

Penalty: ₹200 crores

12.3 Sample Access Request Template (For Data Principals)

 Sample Request Email

Subject: Section 11 DPDPA Access Request - [Your Name]

To: [Data Fiduciary's Data Protection Contact]

Dear Sir/Madam,

I am writing to exercise my right to access information about my personal data under Section 11 of the Digital Personal Data Protection Act, 2023. My Details:

Name: [Your Full Name]

Email: [Your Email]

Phone: [Your Phone Number]

Account ID (if applicable): [Your Account Number/Username]

I request the following information:

Summary of Personal Data (Section 11(1)(a)): Please provide a summary of all personal data you hold about me and the processing activities you undertake with this data. Data Sharing Information (Section 11(1)(b)): Please identify all Data Fiduciaries and Data Processors with whom my personal data has been shared, along with a description of the data shared with each.
Additional Information (Section 11(1)(c)): Please provide any other information prescribed under the DPDP Rules 2025, including retention periods, cross-border transfers, automated decision-making, and breach history affecting my data. Preferred Format: PDF document sent to my email address above. As this is my first access request in the past 12 months, I expect no fee to be charged as per Rule

[recovered from the vector store — section11.html p.17]

13.

I look forward to your acknowledgment within 7 days and full response within 30 days as required by law.

Thank you for your attention to this matter.

Sincerely,

[Your Name]

Date: [Today's Date]

Section 11 is more than a legal right - it's a power shift.

For decades, organizations held all the cards: they knew everything about us, we knew nothing about what they knew. This information asymmetry created a power imbalance that enabled exploitation.

Section 11 rebalances the scales.

"The only thing more powerful than knowing is knowing that you have the right to know."
Section 11 gives Data Principals not just access to information, but the legal power to demand it.

Key Principles to Remember:

Consent = Access Right: If you consented, you can access

Three Components: (a) Data summary & processing, (b) Sharing disclosure, (c) Other prescribed info

Plain Language Requirement: Summaries must be understandable, not technical dumps

30-Day Response: Data Fiduciaries must respond within 30 days (extendable to 60)

First Request Free: No charge for first annual access request

Law Enforcement Exception: Sharing with police/investigators need not be disclosed (11(2))

Enables Other Rights: Access information enables correction (Sec 12), erasure (Sec 13)
Section 11 is the foundation of informational self-determination - you cannot control what you do not know about.

Comprehensive Legal Interpretation Complete

This interpretation covers Section 11 DPDPA 2023 comprehensively - Right to Access Information About Personal Data

 Complete analysis of all three subsections

 Philosophical foundations (Mill, Brandeis, Sen)

 Constitutional framework (Puttaswamy, Article 21, RTI parallel)

 Detailed breakdown of 11(1)(a), (b), (c)

 Law enforcement exception analysis (11(2))

 Rule 13 implementation guide

 Access request process step-by-step

 Compliant response templates

 GDPR & CCPA comparative analysis

 Sample requ