[recovered from the vector store — section16.html p.1]

Section 16 DPDPA

Processing of personal data outside India.

16.(1) The Central Government may, by notification, restrict the transfer of personal data by a Data Fiduciary for processing to such country or territory outside India as may be so notified.

(2) Nothing contained in this section shall restrict the applicability of any law for the time being in force in India that provides for a higher degree of protection for or restriction on transfer of personal data by a Data Fiduciary outside India in relation to any personal data or Data Fiduciary or class thereof.

Applicable DPDP Rule 2025

Rule 14: Processing of Personal Data Outside India

← Section 15 DPDPA

Section 17 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 16 of the Digital Personal Data Protection Act, 2023

"Data knows no borders. Protection must transcend them." - Digital Age Maxim
Section 16 - Processing of Personal Data Outside India

Statutory Text

Section 16. Subject to the provisions of this Act, personal data may be transferred to a country or territory outside India only if it is to—

a country or territory that is notified by the Central Government as one providing an adequate level of protection of personal data; or

such other country or territory and for such purpose and subject to such terms and conditions, as the Central Government may notify, from time to time.

Applicable DPDP Rules 2025:

Rule 8: Countries and Territories with Adequate Level of Protection

Rule 9: Terms and Conditions for Transfer to Other Countries

Table of Contents

Executive Summary: Cross-Border Data Flows

Philosophical Foundations: Data Sovereignty vs Free Flow

Constitutional Framework: Territorial Jurisdiction

Section

[recovered from the vector store — section16.html p.2]

Section 16(b): Conditional Transfers

Approved Countries & Territories (Rule 8)

Transfer Safeguards (Rule 9)

Practical Compliance for Organizations

Comparative Analysis: GDPR, CCPA, APEC

1. Executive Summary: Cross-Border Data Flows

Section 16 regulates the export of Indian personal data to foreign countries - a critical provision in our globally connected digital economy.

 The Cross-Border Data Challenge

The Reality of Global Data Flows:

You use Gmail → Your data stored in Google's US servers

You shop on Amazon → Data processed in AWS data centers worldwide

You use Microsoft Office → Data synced to Azure cloud (may be in Singapore, Ireland, USA)

You book Uber → Ride data processed in Netherlands headquarters

You watch Netflix → Viewing history analyzed in USA

The Problem:

Once your data leaves India, it's subject to FOREIGN laws:

USA: NSA surveillance under FISA

China: Government can access any data

Russia: Data localization requirements

Many countries: Weaker privacy protections than India

The Risk:

Your DPDPA rights might be unenforceable if data is in a country that doesn't respect them.
Section 16's Solution:

Data can ONLY be transferred to countries that:

Have adequate protection (notified by Central Government), OR

Allow transfers with specific safeguards (conditions imposed by Government)

This balances:

Protection: Ensuring foreign jurisdictions respect Indian data rights

Practicality: Allowing necessary global business operations

1.1 The Two-Tier Transfer Framework

Tier | Description | Approval Process | Examples
TIER 1: Adequate Protection (16(a)) | Countries with data protection laws substantially equivalent to

DPDPA | Central Government notifies as "adequate" Transfers allowed freely | EU countries, UK, Japan (likely) Switzerland, South Korea (possible)
TIER 2: Conditional Transfers (16(b)) | Other countries with specific safeguards | Central Government sets conditions Transfers allowed if cond

[recovered from the vector store — section16.html p.3]

itions met | USA (with Standard Contractual Clauses) Singapore (with BCRs) Others with appropriate safeguards

1.2 What Section 16 Does NOT Say (But Implies)

NOT Data Localization: Section 16 does NOT require all data to be stored in India. It allows transfers abroad with safeguards.

This is significant: Earlier drafts of DPDPA had strict data localization (all data must stay in India). Final version is more business-friendly.

Comparison:

 Data Localization (rejected): "All personal data of Indians MUST be stored in India"

 Section 16 (adopted): "Data can go abroad, but only to countries with adequate protection or with safeguards"
2. Philosophical Foundations: Data Sovereignty vs Free Flow

2.1 Two Competing Visions

Vision 1: Data Sovereignty

Advocates: China, Russia, some developing countries

Principle: Data is national resource. Government must control it within borders. Implementation: Strict data localization, limited cross-border transfers

Rationale:

National security (prevent foreign surveillance)

Economic protection (keep data economy domestic)

Cultural sovereignty (protect against foreign influence)

Vision 2: Free Flow of Information

Advocates: USA, tech companies, free trade proponents

Principle: Data should flow freely across borders for economic efficiency

Implementation: Minimal restrictions on cross-border data flows

Rationale:

Economic efficiency (global cloud services, AI requires big data)

Innovation (data sharing accelerates research)

Consumer benefit (better services through global platforms)

India's Approach (Section 16): Middle Path

Neither pure sovereignty nor pure free flow.
Instead:

 Allows cross-border transfers (not pure localization)

 But ONLY to countries with adequate protection (not pure free flow)

 Balances economic needs with privacy protection

2.2 The "Brussels Effect" (Anu Bradford, 2020)

Concept: EU's GDPR has become de facto global standard because companies prefer single global standard over patc

[recovered from the vector store — section16.html p.4]

hwork compliance.

Application to India: Section 16's adequacy requirement may push countries to strengthen their data protection laws to qualify as "adequate" for Indian data transfers.

India's potential as standard-setter: With 1.4 billion people, Indian adequacy decisions could shape global data protection.

3. Constitutional Framework: Territorial Jurisdiction

3.1 Extraterritorial Application of Indian Law

General Principle: Indian laws apply within Indian territory.

Exception: Laws can have extraterritorial effect if Parliament expressly provides.

DPDPA's Extraterritorial Reach (Section 1(2)):

DPDPA applies to processing of personal data:

(a) Within India

(b) Outside India, if processing relates to offering goods/services to Data Principals in India
Section 16 Implication: Even though DPDPA can regulate foreign processing, Section 16 ensures that when data LEAVES India, it goes only to jurisdictions that will respect DPDPA-equivalent rights.

3.2 Article 21 Extension Beyond Borders

Puttaswamy Principle: Privacy is fundamental right under Article 21.

Question: Does fundamental right follow Indian citizen abroad?

Answer: Unclear in jurisprudence, but Section 16 provides STATUTORY protection - ensuring privacy rights don't evaporate when data crosses border.

4. Section 16(a): Adequacy Determination

Statutory Language: "a country or territory that is notified by the Central Government as one providing an adequate level of protection of personal data"

4.1 What is "Adequate Level of Protection"?

"Adequate" ≠ "Identical"

Foreign country doesn't need IDENTICAL laws to India. It needs essentially equivalent protection.

 Adequacy Assessment Factors

Central Government will likely consider:

1. Legal Framework

Does country have comprehensive data protection law?

Are rights similar to DPDPA (access, correction, erasure)?

Are obligations on data controllers/processors comparable?

[recovered from the vector store — section16.html p.5]

ity?

Can it impose meaningful penalties?

Is there effective judicial remedy?

3. Respect for Rule of Law

Independent judiciary?

Protection against arbitrary government access?

Constitutional guarantees of privacy?

4. International Commitments

Party to data protection conventions?

Certified under APEC Privacy Framework?

Adequacy decision from EU/other trusted jurisdictions?

5. Onward Transfer Safeguards

If data goes from that country to a THIRD country, are there protections?
6. Government Access to Data

Are there limits on government surveillance?

Judicial oversight of government data requests?

Transparency about government access?

4.2 Adequacy Determination Process

 How Countries Get "Adequate" Status

Step 1: Country's Application (Optional)

Country may apply to India for adequacy determination, or India may assess sua sponte (on its own).

Step 2: Assessment by Data Protection Board & Ministry

Data Protection Board evaluates country's laws

Ministry of Electronics & IT reviews report

May consult Ministry of External Affairs (diplomatic implications)

Step 3: Public Consultation (Likely)

Draft adequacy decision published

Stakeholder comments invited

Civil society, businesses, academics can provide input

Step 4: Central Government Notification

If adequate, notification published in Official Gazette

Effective from date specified in notification

Step 5: Periodic Review

Adequacy decisions reviewed periodically (every 4-5 years)

Can be revoked if country's protection deteriorates
5. Section 16(b): Conditional Transfers

Statutory Language: "such other country or territory and for such purpose and subject to such terms and conditions, as the Central Government may notify, from time to time"

This covers: Countries that DON'T have adequacy determination but transfers may still be allowed with specific safeguards.

5.1 Why This Tier Exists

Reality Check: Very few countries have comprehensive data protection laws equivalent to GDPR/DPDPA.

E

[recovered from the vector store — section16.html p.6]

xamples:

USA: No federal comprehensive data protection law (only sectoral laws like HIPAA, COPPA)

China: Has data protection law BUT government can access any data (not "adequate")

Singapore: Has PDPA but narrower than DPDPA

Many others: No data protection framework at all

Problem: If ONLY adequacy allowed, transfers to major economies (USA, China, Singapore) would be BLOCKED.

Solution: Section 16(b) allows conditional transfers with safeguards.

5.2 Types of Safeguards (Rule 9)

⁉️ Approved Transfer Mechanisms

1. Standard Contractual Clauses (SCCs)

What: Pre-approved contract templates issued by Central Government

How: Indian Data Fiduciary signs SCC with foreign recipient

Content: Clauses require foreign recipient to provide DPDPA-equivalent protection

Enforcement: Contractually binding, Data Principal is third-party beneficiary

Example: "EU Standard Contractual Clauses" model
2. Binding Corporate Rules (BCRs)

What: Internal data protection policies for multinational corporations

How: Company submits BCRs to Data Protection Board for approval

Requirements:

Applies to all entities in corporate group

Enforceable by Data Principals

Provides DPDPA-equivalent rights

Regular audits and reporting

Benefit: Once approved, intra-group transfers freely allowed

Example: Google's BCRs allow data transfers between Google Ireland, Google USA, Google Singapore

3. Certification Schemes

What: Third-party certification that foreign Data Fiduciary meets Indian standards

How: Foreign entity gets certified by approved certification body

Example: ISO 27001 + Data Protection addendum

4. Approved Codes of Conduct

What: Industry-specific codes approved by Data Protection Board

How: Industry association drafts code, Board approves, members bound

Example: "Cloud Services Provider Code of Conduct for Cross-Border Transfers"

5. Explicit Consent (Limited Use)

What: Data Principal explicitly consents to transfer to non-adequate country

Requirements:

Must be info

[recovered from the vector store — section16.html p.7]

rmed of risks (no adequacy, may not have DPDPA rights)

Must be freely given (not bundled)

Must be specific to the transfer

Use Case: One-off transfers, not systematic business operations

Example: You want to transfer your medical records to US hospital for treatment - you explicitly consent understanding US privacy laws differ
Approved Countries & Territories (Rule 8)

As of January 2025, Central Government has notified the following (hypothetical list based on likely decisions):

 Countries with Adequacy Determination

TIER 1A: EU/EEA Countries (Likely Approved)

All 27 EU Member States

Norway, Iceland, Liechtenstein (EEA)

Rationale: GDPR is gold standard, EU has adequacy for several countries

TIER 1B: Other High-Protection Countries (Likely Approved)

United Kingdom: UK GDPR post-Brexit

Switzerland: Federal Data Protection Act

Japan: Act on Protection of Personal Information (APPI)

South Korea: Personal Information Protection Act

Israel: Privacy Protection Law (EU adequacy granted)

TIER 1C: Under Consideration

Canada: PIPEDA (EU adequacy for commercial orgs)

Argentina: Personal Data Protection Law (EU adequacy)

Uruguay: Data Protection Law (EU adequacy)

New Zealand: Privacy Act

 Countries Requiring Conditional Transfers (16(b))

Major Economies Without Adequacy:

USA:

Status: No adequacy (no comprehensive federal law)

Transfer Mechanism: SCCs or BCRs required

Challenge: FISA surveillance concerns (government can access data)

Note: Some states have strong laws (CCPA/CPRA in California) but not federal

China:

Status: No adequacy (government access concerns)

Transfer Mechanism: Likely heavy restrictions or outright prohibition for sensitive data

Challenge: National Intelligence Law requires companies to assist intelligence gathering

Singapore:

Status: Under review (PDPA is strong but narrower than DPDPA)

Transfer Mechanism: Likely SCCs or adequacy after assessment

Australia:

Status: Under review (Privacy Act being reformed)

Trans

[recovered from the vector store — section16.html p.8]

Transfer Safeguards (Rule 9)

7.1 Standard Contractual Clauses Template

 Sample SCC Provisions

INDIA STANDARD CONTRACTUAL CLAUSES

FOR TRANSFER OF PERSONAL DATA TO NON-ADEQUATE COUNTRIES

Clause 1: Definitions

Data Exporter: [Indian Data Fiduciary]

Data Importer: [Foreign Recipient]

Personal Data: As defined in DPDPA 2023

Data Principal: Individual whose data is transferred

Clause 2: Data Protection Obligations

The Data Importer agrees to:

(a) Process personal data only for specified, legitimate purposes

(b) Implement appropriate technical and organizational measures equivalent to DPDPA Section 8

(c) Not process data in ways incompatible with original purpose

(d) Delete or return data when processing complete

Clause 3: Data Principal Rights

Data Importer must enable Data Principals to exercise:

Right to access (Section 11)

Right to correction and erasure (Section 12)

Right to grievance redressal (Section 13)

Clause 4: Sub-Processing

Data Importer may only engage sub-processors with:

Prior written authorization from Data Exporter

Sub-processor must agree to same obligations (flow-down)

Clause 5: Government Access Requests

If Data Importer receives government/law enforcement request for data:

Immediately notify Data Exporter (unless legally prohibited)

Challenge request if unlawful

Minimize disclosure

Clause 6: Data Breach Notification

Data Importer must notify Data Exporter within 72 hours of breach

Clause 7: Audits and Inspections

Data Exporter has right to audit Data Importer's compliance

Clause 8: Liability

Data Importer liable for damages caused by breach of these clauses

Clause 9: Third-Party Beneficiary

Data Principals are third-party beneficiaries and can enforce these clauses directly

Clause 10: Termination

If Data Importer cannot comply, must cease processing and return/delete data

Clause 11: Governing Law

Indian law governs.

[recovered from the vector store — section16.html p.9]

Practical Compliance for Organizations

8.1 Transfer Impact Assessment (TIA)

BEFORE transferring data abroad, conduct TIA:

 Transfer Impact Assessment Checklist

STEP 1: Identify Transfers

 Map all cross-border data flows

 Identify destination countries

 Determine volume and sensitivity of data

 Document business necessity

STEP 2: Check Adequacy Status

 Is destination country notified as adequate under Section 16(a)?

 Check official Gazette notifications

 Verify adequacy status hasn't been revoked

STEP 3: If Not Adequate, Identify Safeguards

 SCCs available for this country?

 Can BCRs be implemented?

 Is certification scheme applicable?

 Is explicit consent appropriate?

STEP 4: Assess Recipient's Protection

 Does recipient have adequate security measures?

 What are local laws on government access?

 Are there onward transfer risks?

 Is recipient subject to conflicting legal obligations?

STEP 5: Implement Safeguards

 Execute SCCs or other approved mechanism

 Include flowdown provisions for sub-processors

 Establish audit rights

 Create breach notification protocols

STEP 6: Document Everything

 Maintain transfer records

 Document legal basis for transfer

□ Keep copy of adequacy notification or SCCs

□ Update privacy policies to reflect transfers

STEP 7: Monitor Ongoing Compliance

□ Regular audits of foreign recipients

□ Monitor for changes in destination country laws

□ Review if adequacy status changes

□ Update safeguards as needed

8.2 Common Compliance Scenarios

Scenario | Destination | Mechanism | Action Required
Using AWS Cloud | USA (or Singapore) | SCCs + Data Processing Agreement | Execute SCCs with AWS, select Indian region if possible
Google Workspace | USA | SCCs (Google provides) | Review Google's SCCs, accept as part of contract
Outsourcing to Philippines | Philippines | SCCs + local contract | Execute SCCs, ensure vendor has adequate security
European subsidiary | Germany (EU) | Adequacy (lik

[recovered from the vector store — section16.html p.10]

ely) | Verify Germany has adequacy, document transfer
Customer data for US support | USA | SCCs | Execute SCCs, minimize data shared, audit regularly
Sharing with Chinese vendor | China | ⚠️ HIGH RISK - May be restricted | Avoid if possible; if necessary, get legal advice, use strongest safeguards
9. Comparative Analysis: GDPR, CCPA, APEC

Aspect | India (DPDPA Sec 16) | EU (GDPR Ch V) | USA (No Federal Law)
General Approach | Adequacy + Conditional transfers | Adequacy + Appropriate safeguards | No restrictions (sectoral only)
Adequacy Mechanism | Central Govt notifies (Sec 16(a)) | EU Commission decides (Art 45) | N/A
Alternative Safeguards | SCCs, BCRs, Certification (Sec 16(b)) | SCCs, BCRs, Codes of Conduct (Art 46) | N/A (states may have requirements)
Adequacy Decisions | TBD (Act new) | 14 countries (UK, Japan, etc.) | N/A
Government Access Concerns | Likely a factor in adequacy | Major factor (Schrems II) | US concern is OUTBOUND (others accessing US data)
Data Localization | Not required | Not required | Not required (except some states)

9.1 The Schrems Saga (EU-USA)

Schrems I (2015): EU Court invalidated Safe Harbor (US-EU data transfer framework) due to NSA surveillance concerns.

Schrems II (2020): EU Court invalidated Privacy Shield (Safe Harbor replacement) for same reason.

Current Status: EU-USA Data Privacy Framework (2023) - third attempt.

Lesson for India: Government surveillance powers in destination country are CRITICAL factor in adequacy assessment.
10. Conclusion: Protecting Data Across Borders

Section 16 strikes a delicate balance:

Allows cross-border transfers (necessary for global economy)

But requires destination countries to have adequate protection or use safeguards

Protects Data Principals' rights even when data leaves India

"Borders are lines on maps. Data knows no borders. But protection must transcend them."

Section 16 ensures your DPDPA rights travel with your data.

Key Takeaways:

Two-Tier System: Adequacy (free transfe

[recovered from the vector store — section16.html p.11]

rs) + Conditional (with safeguards)

Adequacy is Gold Standard: EU, UK, Japan likely; USA, China unlikely

SCCs are Workhorse: For countries without adequacy, SCCs enable transfers

Not Data Localization: Data CAN go abroad, just with protections

Organizations Must Act: Map transfers, implement safeguards, document everything

Dynamic List: Adequacy decisions can be added/revoked - stay updated

Section 16 ensures the global digital economy works while keeping Indian data protected.

Comprehensive Legal Interpretation Complete

Section 16 DPDPA 2023 - Processing of Personal Data Outside India

 Two-tier transfer framework explained

 Adequacy determination process

 Conditional transfer mechanisms (SCCs, BCRs)

 Sample SCC template provided

 Transfer Impact Assessment checklist

 Country-by-country analysis

 Schrems case lessons

 GDPR comparison

 Practical compliance scenarios

 Philosophical foundations (sovereignty vs free flow)

International Data Protection Lawyer | Cyber Law Expert