Lexlegis.ai
YOUR TRUSTED LEGAL AID

Reference Material

DIGITAL PERSONAL DATA PROTECTION CORPORATE COMPLIANCE HANDBOOK (2025 EDITION)

- Security is not optional nor “best practice” - it is legally mandatory

Authored By: SAAKAR S. YADAV
With support from: Krish Jain, Kunal Ishwad, Trisha Gupta, Nandini Rao Budhagavi, Rohini Krishna Nair and Lexlegis Team

Lexlegis.ai
YOUR TRUSTED LEGAL AID

Digital Publication – No Physical Print Copies

Website: https://lexlegis.ai

Version: 1.0
Document Title: DIGITAL PERSONAL DATA PROTECTION CORPORATE COMPLIANCE HANDBOOK (2025 EDITION)
Document Type: Statutory Reference + Corporate Compliance Manual
Authored By: Saakar S. Yadav
Reviewed By: Krish Jain, Kunal Ishwad, Trisha Gupta, Nandini Rao Budhagavi, Rohini Krishna Nair and Lexlegis Team
Date of Issue: 19th November 2025
Supersedes: All earlier internal DPDPA guidance documents, summaries, notes, and templates
Intended Audience: Corporate leadership, Data Protection Officers, Compliance Teams, Technology & Security Functions, Legal Departments, Auditors, and All Personnel handling personal data
Confidentiality Classification: Public Use – General Distribution Permitted
Distribution Permission: This document may be freely shared, distributed, quoted, and referenced for professional, academic, training, and compliance purposes.

DISCLAIMER: This handbook has been prepared by LexLegis for reference, training, and corporate compliance guidance with respect to the Digital Personal Data Protection Act, 2023 (“DPDPA”) and the Digital Personal Data Protection Rules, 2025 (“Rules”). It incorporates statutory extracts, rule interpretations, operational checklists, and best-practice implementation notes intended to help organisations understand and apply the Act and Rules in their respective environments.

While every reasonable effort has been made to ensure that the material is **accurate, complete, and up to date**, inadvertent errors, omissions, or interpretive variances may occur. LexLegis does not assume responsibility or liability for such errors or for any consequences arising from the use, reliance, or application of this document.

All references to “Sections” or “Rules” within this handbook, where not expressly attributed to

another statute, are to be interpreted as references to the Digital Personal Data Protection Act, 2023 and the Digital Personal Data Protection Rules, 2025. This document **does not constitute legal advice**, regulatory opinion, statutory interpretation, or assurance of compliance. It is not a substitute for:

- Specific legal consultation
- Professional data protection advice
- Statutory guidance issued by competent authorities
- Internal governance reviews

Readers are advised to evaluate the contents of this handbook in the context of their **operational, legal, sectoral, contractual, and regulatory requirements**. Each organisation remains solely responsible for ensuring its own compliance with applicable laws, internal policies, and industry standards. LexLegis shall not be liable for any loss, damage, penalty, sanction, or adverse outcome resulting from the **direct or indirect use** of this handbook, including reliance on examples, checklists, templates, or explanatory notes. Use of this material is entirely at the discretion of the reader, who accepts full responsibility for verifying accuracy, ensuring compliance, and making appropriate decisions.

About the Author: Saakar S. Yadav is a seasoned technologist and platform architect with over two decades of hands-on experience designing and scaling large, high-impact digital systems. He has played a pivotal role in national technology initiatives—including building the Central Data Processing Centre for the National Judicial Reference System (NJRS), one of India's largest judicial-appeal repositories—demonstrating mastery in complex data handling, high-volume processing, and mission-critical system design.

As the founder of LexLegis.ai, Saakar brings deep expertise in robust architecture development, compliance-driven platform engineering, and real-world digital governance. His experience spans tax-tech, legal-tech, enterprise systems, and government-grade technology—making him uniquely positioned to define AI usage standards that are scalable, secure, compliant, and technically sound. His contributions ensure the handbook is grounded not only in theoretical governance principles but also in practical, technologically executable guidelines that reflect the realities of modern platform ecosystems.

TABLE OF CONTENTS

1. INTRODUCTION TO THE DPDPA AND COMPLIANCE FRAMEWORK

1.1 Purpose of the DPDPA

The Digital Personal Data Protection Act, 2023, establishes a comprehensive regulatory framework for processing personal data in digital form, ensuring that individuals' rights are protected while enabling lawful and responsible business operations.
Section 1 & Preamble of the DPDPA 2023

1.2 What Businesses Must Understand

Every organisation that processes digital personal data, regardless of sector, size, or business model, must align operations, technologies, and procedures with the legal obligations under the Act and Rules. This includes implementing governance measures, establishing operational controls, and ensuring transparent data handling.
Section 3; Rules 3–16 of DPDPA Rules 2025

1.3 Corporate Liability & Accountability

The law imposes **strict accountability** on Data Fiduciaries, including senior management and board-level oversight. Businesses must show evidence of compliance and maintain robust documentation to defend against regulatory actions, penalties, or inquiries.
Section 8(1); Section 33; Rule 6(f)

1.4 Compliance as a Business Risk & Reputation Priority

Non-compliance exposes organisations to:

- Severe financial penalties (up to ₹250 crore per violation)
- Suspension of services
- Blocking orders for digital platforms

- Reputation and trust damage
- Contractual liability with customers or partners

Therefore, compliance must be integrated into enterprise risk management and internal audit cycles.
Schedule; Section 37, 8(5), Rule 6

1.5 Key Compliance Components Covered in This Handbook

This manual provides detailed guidance on:

- Governance frameworks
- Notice and consent standards
- Technical and organisational security controls
- Breach reporting and incident response
- Rights management workflows
- Vendor data processing governance
- Data retention and deletion rules
- Children's data requirements
- Significant Data Fiduciary obligations
- Government data processing standards
  Sections 4–17; Rules 3–16

CHECKLIST

A. Leadership & Governance

- ☐ Appoint a Data Protection Contact Person or DPO based on SDF status.
- ☐ Define and document the internal data protection governance structure.
- ☐ Allocate budgets for compliance technology, training, and audits.
- ☐ Integrate data protection metrics into board oversight and risk reports.
- ☐ Establish a Data Protection Steering Committee.
  Sections 10(2), 8(1); Rule 9

B. Documentation & Policies

- ☐ Create or update privacy policies, data retention schedules, DPIA templates, and breach-management SOPs.
- ☐ Maintain evidence logs for every compliance step.
- ☐ Document the lawful basis for all data processing activities.
- ☐ Maintain processing records for audit trails.
  Section 8(3)-(4); Rule 6(c-d); Rule 14

C. Operational Foundations

- ☐ Establish internal workflows for notices, consent, withdrawal, and rights requests.
- ☐ Deploy secure systems for logging, access control, and monitoring.
- ☐ Train employees especially HR, Marketing, IT, and Customer Support.
  Rule 3; Rule 6(a–e)

2. APPLICABILITY, SCOPE & KEY DEFINITIONS

This chapter explains which organisations, activities, and operations fall under the purview of the Digital Personal Data Protection Act (DPDPA) 2023 and the DPDPA Rules 2025. Understanding scope is critical because compliance obligations depend entirely on whether an entity qualifies as a **Data Fiduciary**, **Data Processor**, or both, and whether the Act applies to its activities.

2.1 Applicability of the Act

2.1.1 Processing of Digital Personal Data Within India

The Act applies to all processing of digital personal data carried out within India, regardless of whether the processing relates to Indian citizens, residents, foreigners, or legal entities operating within India. This includes personal data that originates offline but is later digitised for processing.
Section 3(a)

2.1.2 Extraterritorial Applicability - Activities Targeting Individuals in India

The Act also applies to processing outside India if the purpose is to offer goods or services to individuals located inside India. Foreign companies that run websites, apps, SaaS platforms, OTT services, gaming platforms, or e-commerce storefronts targeting Indian users must be fully compliant with the Act.
Section 3(b)

2.1.3 Non-Applicability: Personal or Domestic Use

The Act does **not** apply when individuals process personal data for purely personal or household purposes (e.g., maintaining personal contacts, diaries, photos, messages). However, once such data is processed for business or professional use, the exemption ceases.
Section 3(c)(i)

2.1.4 Non-Applicability: Publicly Available Personal Data

If personal data has been made publicly available by:

- the Data Principal themselves, or
- any person who is legally required to publish it,

then such data is exempt from DPDPA obligations. Examples: Public company filings, court orders, government registries, self-disclosed social media posts.
Section 3(c)(ii)

2.2 Key Definitions Relevant to Corporates

2.2.1 Personal Data

Personal data means any information about an identifiable individual, whether directly or indirectly identifiable. This includes names, IDs, numbers, addresses, IPs, cookies, behavioural data, biometrics, and more.
Section 2(t)

2.2.2 Digital Personal Data

Personal data in digital format, whether originally collected digitally or later digitised from a physical source.
Section 2(n)

2.2.3 Processing

Any fully or partly automated operation on personal data, including collecting, storing, combining, aligning, sharing, indexing, or deleting.
Section 2(x)

2.2.4 Data Principal

The individual to whom the personal data relates. For children, the parent or lawful guardian is the Data Principal. For persons with disability, lawful guardians act on their behalf.
Section 2(j)

2.2.5 Data Fiduciary

Any entity that determines the purpose and means of processing personal data. ALL companies, LLPs, firms, NGOs, startups, platforms, and government bodies may be Data Fiduciaries depending on activities.
Section 2(i)

2.2.6 Data Processor

A person/entity that processes personal data on behalf of a Data Fiduciary under a valid contract.
Section 2(k)

2.3 Key Corporate Implications of Scope & Definitions

2.3.1 Nearly All Modern Organisations Are Covered

Any business that collects employee, customer, vendor, visitor, partner, or contractor data must assume it is a Data Fiduciary unless proven otherwise.
Section 3(a)

2.3.2 Dual Role Entities

Many companies are simultaneously:

- **Data Fiduciaries** (for employees, customers, website/app users)
- **Data Processors** (for outsourced services, cloud hosting, analytics, call centres)
  Section 8(1)

2.3.3 Public vs Private Processing Does Not Change Obligations

Corporate obligations remain unchanged irrespective of whether the entity is private or public, except for specific exemptions granted to government entities.
Section 17(2)

CHECKLIST

A. Identify Applicability

- Identify all business functions that process digital personal data (HR, Sales, Marketing, IT, Finance).
- Map all systems (CRM, ERP, HRMS, POS, mobile apps, cloud storage) where personal data is stored or processed.
- Document cross-border data flows involving global vendors or cloud platforms.
- Confirm whether any processing targets individuals in India from abroad.
  Section 3(a)-(b)

B. Role Identification

- Identify which functions act as Data Fiduciary.
- Identify vendor relationships that constitute Data Processor roles.
- Create a central register of all Data Processors with purpose, contract validity, and compliance status.
  Section 2(i)-(k), Section 8(1)

C. Publicly Available Data

- Confirm whether any business workflow uses publicly available personal data.
- Document sources and confirm that the data was lawfully published under statutory obligations or voluntarily by the individual.
  Section 3(c)(ii), Section 8(1)

3. LAWFUL PROCESSING, NOTICES & CONSENT

Lawful processing forms the core compliance requirement under the DPDPA. Every corporate data-handling activity must satisfy both transparency requirements (notices) and lawful basis requirements (consent or deemed consent).

3.1 Lawful Basis for Processing

3.1.1 Consent-Based Processing

A Data Fiduciary may process personal data only when the Data Principal has provided **free, specific, informed, unambiguous, affirmative consent** for a stated purpose. Consent cannot be bundled, forced, or conditional unless necessary for service.
Section 4(1)(a), Section 6(1); Rule 3

3.1.2 Deemed Consent for Certain Legitimate Uses

Processing is permitted without explicit consent only if it falls under the specific categories of "certain legitimate uses" detailed in Section 7. *Section 4(1)(b), Section 7*

3.2 Notice Requirements (Rule 3)

3.2.1 Mandatory Notice Before or At Consent Collection

Before collecting personal data for a specified purpose, the Data Fiduciary must provide a notice that is clear, distinct, independent from terms and conditions, and available in English or any Eighth Schedule language.
Section 5(1)-(3); Rule 3(a)

3.2.2 Mandatory Contents of the Notice (Rule 3(b))

The notice must include:

- Itemised description of personal data to be collected
- Description of goods or services provided
- Purpose of processing
- Consequences of refusing consent
  Rule 3(b)(i)-(ii)

3.2.3 Mandatory Links in Notice (Rule 3(c))

The notice must contain links for:

- Consent withdrawal
- Rights request submission
- Complaint to the Board
  Rule 3(c)(i)-(iii)

3.2.4 Multilingual Availability

Notice must be accessible in English and optionally Indian languages.
Section 6(3)

3.3 Consent Requirements

3.3.1 Consent Must Be Affirmative & Unambiguous

No pre-ticked boxes, no inactivity, and no implied consent.
Section 6(1)

3.3.2 Consent Must Be Granular

Separate purposes require separate consent options.
Section 6(1)

3.3.3 Consent Withdrawal Must Be As Easy As Giving Consent

Opt-out workflows must not introduce new friction.
Section 6(4)

3.3.4 Data Fiduciary Must Keep Proof of Notice + Consent

If a dispute arises, the burden of proof is on the Data Fiduciary.
Section 6(10)

CHECKLIST

A. Notice Compliance

- ☐ Prepare a unified Privacy Notice compliant with Rule 3(b)-(c).
- ☐ Notify the subject at every collection point (app, website, forms, chatbot, IVR).
- ☐ Capture version numbers of notice and consent.
- ☐ Ensure notices are accessible in English and optionally Indian languages.
  Section 5, Section 6(3) ; Rule 3

B. Consent Management

- ☐ Implement a consent management system (CMS) that logs:
  - ☐ Timestamp
  - ☐ Purpose
  - ☐ Notice version
  - ☐ Method of capture
- ☐ Implement a single-click withdrawal option.
- ☐ Ensure consent withdrawal automatically triggers downstream deletion where applicable.
  Section 6(1)-(7)

C. UI/UX Compliance

- ☐ Remove dark patterns (forced consent, manipulative design).
- ☐ Make refusal to consent non-punitive unless necessary for service.

4. DEEMED CONSENT & LEGITIMATE USES

Deemed consent allows organisations to process data without explicit consent but **only under specific, limited, well-defined situations**.

4.1 Voluntarily Provided Data for a Specific Purpose (Section 7(a))

If an individual voluntarily provides personal data for a particular purpose without objecting to its usage, it is considered deemed consent. Example: A customer gives their phone number at a pharmacy to receive a digital bill.
Section 7(a)

4.2 State Functions (Section 7(b)-(c))

4.2.1 Government Benefits, Subsidies & Services

If a Data Principal has already provided data to access any government benefit, service, certificate, license, or permit, the data may be processed again for similar government functions.
Section 7(b)

4.2.2 Sovereignty, Security & Public Order

Processing is permitted for functions related to:

- Sovereignty & integrity of India
- Security of the State
- Public order maintenance
  Section 7(c)

4.3 Legal Compliance Obligations (Section 7(d))

Businesses must process and share certain personal data to comply with statutory requirements (e.g., KYC, tax reporting, law enforcement requests).
Section 7(d)

4.4 Judicial, Regulatory or Enforcement Requests (Section 7(e))

Processing is lawful for compliance with:

- Court orders
- Regulatory directions
- Foreign civil judgments
  Section 7(e)

4.5 Medical Emergencies & Public Health Threats (Section 7(f)-(g))

Permits processing for:

- Emergency health treatment
- Epidemic response
- Public health threats
  Section 7(f), Section 7(g)

4.6 Disasters & Public Order Breakdowns (Section 7(h))

Allows processing during natural disasters or breakdown of public order for rescue, assistance, or safety measures.
Section 7(h)

4.7 Employment-Related Processing (Section 7(i))

Data may be processed without consent to:

- Provide corporate benefits
- Ensure safety
- Prevent espionage
- Protect trade secrets
- Handle HR operations
  Section 7(i)

CHECKLIST

A. Identify All Deemed Consent Scenarios

- ☐ HR operations (attendance, payroll, ID badges, surveillance).
- ☐ Compliance (tax, labour laws, SEBI filings).
- ☐ Emergency workflows.
- ☐ Service-based voluntary submissions.
- ☐ Government-mandated reporting.
  Section 7

B. Implement Purpose Limitation

- ☐ Validate that data used under deemed consent is used only for that purpose.
- ☐ No expansion of purpose without explicit consent.
  Section 4(1); Section 7

C. Documentation

- ☐ Maintain logs showing the basis for deemed consent.
- ☐ Maintain SOPs for responding to lawful requests.

- ☐ Conduct reviews to ensure no misuse.
  Section 8

5. RIGHTS OF DATA PRINCIPALS

The DPDPA establishes a structured set of rights for individuals (“Data Principals”) to help them maintain control over their personal data. These rights must be supported by transparent, easily accessible, and verifiable corporate mechanisms.

This chapter explains each right, what organisations must do, and how compliance workflows should be implemented.

5.1 Right to Access Information (Section 11; Rule 14)

5.1.1 Scope of the Access Right

A Data Principal has the right to request a detailed summary of the personal data being processed, including categories, processing activities, and the purpose. Companies must provide this information promptly through transparent and easily accessible channels. *Section 11(1)(a)*

5.1.2 Understanding Data Sharing

The Data Principal is entitled to know the identities of all Data Fiduciaries and Data Processors with whom the personal data has been shared, along with a description of what data was shared, except for cases involving law enforcement or statutory authorities.
Section 11(1)(b) and Section 11(2)

5.1.3 Other Information to Be Provided

Any additional information relevant to the Data Principal’s personal data, such as retention periods, grievance channels, or rights mechanisms, must be disclosed upon request.
Section 11(1)(c)

5.1.4 Method for Submitting Access Requests

Organisations must publish a clear and accessible method for submitting rights requests, such as a rights portal, email address, or in-app form. The method must be published prominently.
Rule 14(1)

5.2 Right to Correction and Updating (Section 12(2))

5.2.1 Correction Obligations

A Data Principal may request correction of inaccurate or misleading personal data. Businesses must correct such data within a reasonable time, and ensure the updates propagate to all relevant internal systems.
Section 12(2)(a)

5.2.2 Completion of Incomplete Data

If the information held is incomplete, the Data Principal may request its completion. The Data Fiduciary must verify the authenticity of the new information where appropriate.
Section 12(2)(b)

5.2.3 Updating of Outdated Data

Organisations must update personal data upon request and maintain processes to ensure continued accuracy, especially for time-sensitive or regulatory data.
Section 12(2)(c)

5.3 Right to Erasure (Section 12(3))

5.3.1 General Deletion Obligation

A Data Principal may request erasure of personal data that is no longer necessary for the specified purpose, or where the Data Principal has withdrawn consent.
Section 12(3)

5.3.2 Exceptions to Deletion

If retention is required by law (e.g., financial record retention, KYC retention), the Data Fiduciary must deny erasure with justification.
Section 8(7)(a); Section 12(3)

5.3.3 Downstream Deletion

Data Processors must be instructed to erase the data when the Data Fiduciary erases it, unless they have independent legal obligations to retain it.
Section 8(7)(b)

5.4 Right to Grievance Redressal (Section 13; Rule 14(3))

5.4.1 Mandatory Grievance System

Data Fiduciaries must establish a system for receiving and resolving grievances related to personal data processing. This may include ticketing systems, email channels, or dashboards.
Section 13(1)

5.4.2 Resolution Timelines

Organisations must respond to grievances within the time period prescribed by the Rules, which must not exceed 90 days. *Rule 14(3)*

5.4.3 Exhaustion Before Board Complaint

The Data Principal must exhaust grievance mechanisms before approaching the Data Protection Board.
Section 13(3)

5.5 Right to Nominate (Section 14)

5.5.1 Nominee Identification

Data Principals may nominate another individual to exercise their rights upon death or incapacity.
Section 14(1)

5.5.2 Process to Facilitate Nomination

Organisations must create a secure method for nomination submission, verification, and storage.
Rule 14(4)

CHECKLIST

A. Rights System Setup

- ☐ Establish a Data Principal Rights Portal or dedicated communication channel.
- ☐ Publish the rights process on the website/app in clear and plain language.
- ☐ Train customer support and grievance teams on rights handling.
- ☐ Maintain logs of all rights requests and responses.
  Rule 14(1)-(4)

B. Access, Correction & Erasure

- ☐ Implement identity verification steps for rights requests.

- ☐ Develop SOPs for correction, updating, and erasure workflows.
- ☐ Ensure deletion triggers processor notifications.
- ☐ Configure systems to handle data mapping & downstream consistency.
  Section 11; Section 12; Section 8(7)

C. Grievances

- ☐ Ensure grievance mechanisms meet the 90-day requirement.
- ☐ Publish DPO/contact person details.
- ☐ Maintain grievance dashboards for management review.
  Section 13; Rule 14(3)

D. Nomination

- ☐ Implement nomination options in account settings.
- ☐ Secure verification of nominee identity.
  Section 14; Rule 14(4)

6. DATA FIDUCIARY OBLIGATIONS

The DPDPA places primary responsibility for compliance on the **Data Fiduciary**. This chapter details the organisational, technical, security, and procedural obligations businesses must implement.

6.1 Accountability for Personal Data Processing

6.1.1 Full Responsibility for Processing

Data Fiduciaries are responsible for compliance with the Act for all processing conducted by themselves or by Data Processors acting on their behalf.
Section 8(1)

6.1.2 Contracts with Data Processors

Organisations may engage Data Processors only under a valid contract. The contract must detail processing activities, retention, security requirements, and breach obligations.
Section 8(2)

6.2 Data Quality and Accuracy (Section 8(3))

6.2.1 When Accuracy Is Required

Where personal data is used to make decisions affecting Data Principals or shared with another Data Fiduciary, reasonable effort must be taken to ensure accuracy.
Section 8(3)

6.2.2 Operational Requirements

- Validation of commonly used fields (address, mobile number).
- Automated checks to detect outdated or conflicting records.
  Section 8(3)

6.3 Organisational and Technical Measures (Section 8(4))

6.3.1 Policy Requirements

Organisations must adopt policies covering data protection, access control, breach response, vendor management, and encryption.
Section 8(4)

6.3.2 Training & Awareness

Employees handling personal data must be trained regularly on legal obligations and organisational policies.
Section 8(4)

6.4 Security Safeguards (Section 8(5); Rule 6)

6.4.1 Reasonable Security Safeguards

Data Fiduciaries must take reasonable safeguards to prevent personal data breaches. The minimum safeguards are defined in Rule 6.
Section 8(5); Rule 6

6.4.2 Technical Safeguards (Rule 6(a)-(e))

Organisations must implement:

- Encryption, pseudonymisation, masking
- Access control and IAM
- Logging and security monitoring
- Backup and disaster recovery
- Incident detection and response
  Rule 6(a)-(e)

6.4.3 Log Retention Requirement

Fiduciaries must retain personal data logs for a minimum of one year.
Rule 6(e)

6.5 Personal Data Breach Notification (Section 8(6); Rule 7)

Breach requirements are detailed in Chapter 9, but as a fiduciary obligation:

- Notify affected Data Principals
- Notify the Board
  Section 8(6); Rule 7

6.6 Data Retention & Erasure (Section 8(7); Rule 8)

6.6.1 Erasure Upon Purpose Completion or Withdrawal

Data must be erased when it is no longer required for the purpose, or upon withdrawal of consent (unless retention is legally required).
Section 8(7)(a)

6.6.2 Processor Erasure Obligations

Data Fiduciaries must direct all their Data Processors to erase data accordingly.
Section 8(7)(b)

6.7 Publication Requirement (Section 8(9); Rule 9)

6.7.1 Publish Contact Details

Data Fiduciaries must publish contact information of a DPO (for SDFs) or authorised contact person.
Section 8(9); Rule 9

6.8 Grievance Redressal Mechanism (Section 8(10))

Data Fiduciaries must establish and maintain an effective grievance redressal system accessible to all Data Principals.
Section 8(10)

CHECKLIST

A. Governance Controls

- ☐ Establish enterprise-wide data protection governance.
- ☐ Implement policies: access control, security, breach response, retention.
- ☐ Ensure DPO/contact person details published.
  Section 8(9)

B. Processor Oversight

- ☐ Maintain contracts with all Data Processors.
- ☐ Ensure contracts include Rule 6(f) safeguarding obligations.
- ☐ Perform annual vendor audits.
  Section 8(2); Rule 6(f)

C. Data Accuracy

- ☐ Implement validation checks.
- ☐ Maintain mechanisms to update outdated data.
  Section 8(3)

D. Security Controls

- ☐ Implement encryption, access control, monitoring, backups.

- ☐ Retain logs for minimum 1 year.
  Rule 6(a)-(e)

E. Retention & Deletion

- ☐ Map all data retention periods by purpose.
- ☐ Schedule periodic deletion cycles.
- ☐ Trigger deletion upon consent withdrawal.
  Section 8(7)

7. DATA PROCESSOR OBLIGATIONS & VENDOR MANAGEMENT

Although primary responsibility lies with Data Fiduciaries, Data Processors play a critical role in operational compliance.

7.1 Contractual Engagement Requirement

7.1.1 Valid Contract Requirement

A Data Fiduciary may engage a Data Processor only under a valid and enforceable contract specifying:

- Purpose of processing
- Security measures
- Retention rules
- Breach response obligations
  Section 8

7.2 Processor Compliance with Security Safeguards (Rule 6(f))

Data Fiduciaries must ensure processors implement appropriate security safeguards in accordance with Rule 6. *Rule 6(f)*

7.3 Prohibition on Unauthorised Sub-processing

Data Processors cannot onboard sub-processors without prior written approval from the Data Fiduciary.
Section 8(5)

7.4 Log Retention & Monitoring

Processors must retain logs for at least one year and ensure availability for Audit, DPIA, or Board enquiries.
Rule 6(e)

7.5 Breach Reporting

Processors must promptly notify Data Fiduciaries of any suspected or confirmed personal data breach.
Section 8(6); Rule 7

7.6 Data Deletion Obligations

Processors must erase personal data upon direction from the Data Fiduciary, unless retention is legally mandated.
Section 8(7)(b)

CHECKLIST

A. Vendor Identification

- ☐ Map all vendors handling personal data.
- ☐ Classify vendors by data sensitivity.
- ☐ Maintain updated processor inventory.
  Section 10, 8(2)

B. Contracts & Legal Requirements

- ☐ Ensure all processors have valid DPA agreements.

- ☐ Incorporate confidentiality, breach notification, and deletion clauses.
- ☐ Include Rule 6(f) security requirements.

C. Operational Oversight

- ☐ Conduct periodic vendor audits.
- ☐ Monitor vendor incident reports.
- ☐ Maintain performance KPIs for processors.
  Section 8(1), Section 8(6) & Section 10(2)

D. Offboarding Process

- ☐ Ensure data is deleted upon contract termination.
- ☐ Obtain deletion certificates.
- ☐ Validate downstream deletion from sub-processors.
  Section 8(7)(b)

8. SECURITY SAFEGUARDS & TECHNICAL CONTROLS

The Digital Personal Data Protection Act and Rules impose mandatory, minimum security requirements on all Data Fiduciaries and Data Processors. These requirements form the backbone of operational compliance and are essential for preventing breaches, ensuring data integrity, and avoiding penalties.

Security controls must be implemented holistically across technology, processes, human resources, and third-party ecosystems.

8.1 Principle of “Reasonable Security Safeguards”

8.1.1 Mandatory Security Measures

Every Data Fiduciary must implement reasonable security safeguards to protect personal data from breaches, unauthorised access, accidental disclosure, alteration, or loss. These safeguards must be proportionate to the volume, sensitivity, and risk associated with the data.
Section 8(5)

8.1.2 Practical Corporate Implication

Security is not optional nor “best practice” - it is **legally mandatory**. Any compromise, even by a vendor or processor, results in liability for the Data Fiduciary.
Section 8(1), Section 8(5)

8.2 Mandatory Minimum Technical Controls (Rule 6)

Rule 6 lays down mandatory minimum controls. All companies must implement these irrespective of size, industry, or technology stack.

8.2.1 Encryption & De-identification Controls (Rule 6(a))

Businesses must use up-to-date encryption, pseudonymisation, anonymisation (where appropriate), tokenisation, or masking methods when storing or transmitting personal data. *Rule 6(a)*

8.2.2 Access Control Measures (Rule 6(b))

Organisations must enforce role-based access control (RBAC), enforce least privilege principles, and ensure authentication systems prevent unauthorised access. Multi-factor authentication (MFA) is strongly recommended.
Rule 6(b)

8.2.3 Logging & Monitoring (Rule 6(c))

Systems that store or process personal data must maintain logs for access, modification, transfers, configuration changes, and automated actions. Logs must be protected, monitored, and regularly reviewed.
Rule 6(c)

8.2.4 Backup, Resilience & Continuity (Rule 6(d))

Organisations must maintain secure backups, disaster-recovery plans, and continuity procedures to ensure personal data remains available and intact despite failures or attacks. *Rule 6(d)*

8.2.5 Log Retention (Rule 6(e))

Logs relating to personal data processing must be retained for a **minimum of one year** from the date of each processing activity. *Rule 6(e)*

8.2.6 Processor Security Obligations (Rule 6(f))

If processing is outsourced, the Data Fiduciary must ensure the Data Processor implements the same safeguards and complies with all security instructions.
Rule 6(f)

8.3 Human & Organisational Measures

8.3.1 Workforce Training

All employees handling personal data must receive recurring training to detect breaches, avoid social engineering threats, and follow correct data-handling procedures.
Section 8(4)

8.3.2 Access Review & Privilege Management

Periodic access reviews must be conducted to ensure only authorised personnel retain access.
Rule 6(b)

8.4 Physical Security Measures

8.4.1 Device & Facility Controls

Businesses must secure data centres, servers, office equipment, storage devices, and access points to prevent theft, loss, or unauthorised access.
Section 8(5); Rule 6(a)-(d)

8.5 Incident Detection Systems

8.5.1 Proactive Monitoring

Security Information & Event Management (SIEM) systems, IDS/IPS, and automated anomaly detection tools should be deployed wherever feasible to detect breaches early. *Rule 6(c)*

CHECKLIST

A. Technical Controls

- ☐ Implement encryption at rest and in transit.
- ☐ Deploy tokenisation/masking for sensitive fields.
- ☐ Enforce MFA across sensitive systems.
- ☐ Configure RBAC and least-privilege access.
  Rule 6(a)-(b)

B. Logs & Monitoring

- ☐ Enable logs for all processing activities.
- ☐ Protect logs from tampering.
- ☐ Retain logs for minimum 12 months.
- ☐ Review logs regularly using SIEM tools.
  Rule 6(c)-(e)

C. Backups & DR

- ☐ Maintain periodic backups.
- ☐ Test restoration procedures periodically.
- ☐ Document disaster-recovery plans.
  Rule 6(d)

D. Human Controls

- ☐ Conduct mandatory DP training for all staff.
- ☐ Conduct phishing simulations.
- ☐ Run periodic access reviews.
  Section 8(4); Rule 6(b)

9. PERSONAL DATA BREACH MANAGEMENT & REPORTING

A breach is one of the most serious compliance issues for any organisation. The Act imposes **strict mandatory reporting obligations**. Failure to report a breach promptly can attract penalties up to ₹200 crore.

9.1 Definition of Personal Data Breach

A personal data breach includes unauthorised processing, accidental disclosure, alteration, loss, or loss of access. This includes cyber incidents, accidental emails, misdelivery, theft of devices, or exposure due to misconfiguration.
Section 2(u)

9.2 Data Fiduciary Obligations Upon a Breach (Section 8(6))

9.2.1 Mandatory Notification to the Board

The Data Fiduciary must notify the Data Protection Board of India about any breach “in such form and manner as may be prescribed”which is detailed in Rule 7.
Section 8(6)

9.2.2 Mandatory Notification to Affected Data Principals

Data Principals must be informed about the breach, its consequences, and recommended safety measures.
Section 8(6)

9.3 Mandatory Contents of Notification (Rule 7)

When notifying a breach, companies must include:

- Nature, categories, and volume of personal data involved
- Number of Data Principals affected

- Likely consequences
- Mitigation actions taken
- Contact details of the authorised person
  Rule 7(1)(a)-(e)

9.4 Timelines for Breach Reporting

9.4.1 Immediate Notice

Data Fiduciaries must notify the Board **"without delay"** upon becoming aware of the breach.
Rule 7(1)

9.4.2 Detailed 72-Hour Report

A comprehensive written report must be filed within **three days** of initial notification.
Rule 7(2)

9.5 Internal Corporate Requirements for Breach Response

9.5.1 Incident Response Team (IRT)

Businesses must designate a cross-functional team comprising Legal, IT Security, HR, Operations, and Communications staff.
Section 8(4); Rule 6(d)

9.6 Processor's Obligations in Breach Situations

A Data Processor that becomes aware of a breach must notify the Data Fiduciary immediately, enabling the latter to fulfil statutory reporting obligations.
Section 8(6); Rule 7

CHECKLIST

A. Detection & Monitoring

- ☐ Deploy breach-detection tools (SIEM, IDS/IPS).
- ☐ Establish breach reporting hotline/email internally.
- ☐ Perform breach audits periodically.
  Rule 6(c)

B. Notification Workflow

- ☐ Trigger Board notification immediately.
- ☐ Prepare 72-hour detailed breach report.
- ☐ Identify affected Data Principals and notify them.
  Rule 7(1)-(2)

C. Mitigation Procedures

- ☐ Secure compromised systems.
- ☐ Reset access controls.
- ☐ Conduct root-cause analysis.
- ☐ Document and preserve all evidence.
  Section 8(5), Section 8(6); Rule 7

D. Vendor Breach Management

- ☐ Require processors to notify breaches instantly.
- ☐ Verify vendor logs and timelines.
- ☐ Demand remediation updates.
  Section 8(2), Section 8(6)

10. CHILDREN'S DATA & PROCESSING FOR DISABLED PERSONS

Children and persons with disabilities receive enhanced legal protection under the DPDPA. This chapter explains the special rules and operational safeguards every organisation must implement.

10.1 Verifiable Parental Consent for Children (Section 9(1); Rule 10)

10.1.1 Consent Requirement

A Data Fiduciary must obtain **verifiable parental consent** before processing the personal data of a child (under 18).
Section 9(1)

10.1.2 Verification of Parental Identity (Rule 10)

Companies must verify that the consenting parent is:

- An adult; and
- The lawful parent/guardian.

Verification must occur using reliable mechanisms such as:

- DigiLocker-based identity token
- Equivalent authorised validation
- Internal verification workflows
  Rule 10(1), Rule 10(2)

10.2 Data of Persons with Disabilities (Section 2(j)(ii); Rule 11)

10.2.1 Lawful Guardian Verification

A lawful guardian must be verified using:

- Court orders
- Designated authority certificates
- Local level committee documentation
  Rule 11(a)-(c)

10.3 Prohibited Processing Activities for Children

10.3.1 No Detrimental Processing

A Data Fiduciary must not process personal data in a manner that could harm a child's well-being.
Section 9(2)

10.3.2 No Tracking or Behavioural Monitoring

Tracking or behavioural analysis of children is prohibited.
Section 9(3)

10.3.3 No Targeted Advertising

Children must not be targeted for advertising.
Section 9(3)

10.4 Exemptions for Child-Facing Services (Rule 12)

Child-serving sectors such as schools, hospitals, day-care facilities, and transportation providers are exempt from some restrictions when necessary for safety, education, and care.
Rule 12; Fourth Schedule

10.5 Children's Data Retention & Minimum Use

Data collected for children must be used strictly for the intended purpose and deleted promptly when no longer needed.
Section 8(7)

CHECKLIST

A. Parental Consent

- ☐ Deploy age verification for all users.
- ☐ Deploy parental verification (DigiLocker or equivalent).
- ☐ Maintain logs of parental consent.
  Section 9(1); Rule 10

B. Processing Restrictions

- ☐ Disable behavioural tracking for child accounts.
- ☐ Disable targeted advertising.
- ☐ Conduct DPIAs for child data workflows.
  Section 9(2)-(3), Section 10(2)

C. Disability Data Handling

- ☐ Verify lawful guardian using Rule 11 documents.

- ☐ Maintain secure storage of guardian documents.
  Rule 11

D. Deletion & Retention

- ☐ Delete children's data upon purpose completion.
- ☐ Ensure processors delete it as well.
  Section 8(7)

11. DATA RETENTION, ARCHIVAL & DELETION RULES

Data retention is one of the most misunderstood but strictly regulated areas of the DPDPA. Unlike many global regimes, DPDPA creates a **dual-layer retention framework** consisting of:

1. **Purpose-based automatic deletion (Section 8(7))**
2. **Mandatory minimum retention of logs and records (Rule 8)**

This chapter explains how organisations must implement both simultaneously using structured corporate processes.

11.1 Purpose-Based Retention (Section 8(7))

11.1.1 Deletion When Purpose Is Fulfilled

A Data Fiduciary must erase personal data as soon as it is reasonable to assume that the purpose for which the data was processed is no longer being served.
Section 8(7)(a)

11.1.2 Withdrawal of Consent

If processing is based on consent and the Data Principal withdraws consent, personal data must be erased unless retention is required by law.
Section 8(7)(a)

11.1.3 Processor Obligation to Delete

Data Processors must also erase personal data when instructed by the Data Fiduciary.
Section 8(7)(b)

11.2 Mandatory Minimum Retention (Rule 8)

11.2.1 One-Year Mandatory Log Retention (Rule 8(3))

Data Fiduciaries and Processors must retain **personal data, traffic data, and logs** for a minimum of one year from processing. This requirement applies **even if** the purpose is completed.
Rule 8(3)

11.2.2 Automatic Deletion for Certain Data Fiduciaries (Rule 8(1))

Large-scale platforms such as e-commerce players, social media platforms, OTT apps, and online games must delete personal data if the user has not interacted for **3 years**.
Rule 8(1)

11.2.3 Mandatory 48-Hour Notice Before Deletion (Rule 8(2))

Before deleting data under Rule 8(1), the Data Fiduciary must give the user at least **48 hours** notice. *Rule 8(2)*

11.3 Corporate Retention Schedule Requirements

11.3.1 Master Retention Register

Every organisation must maintain a documented retention schedule mapping each data class to its:

- Purpose
- Legal retention period
- Corporate retention commitments
- Deletion triggers
  Section 8(7), Rule 8

11.3.2 Deletion Workflows Must Be Automated

Manual deletion is not scalable or auditable; systems should implement automated retention and auto-purge jobs.
Section 8(4), Section 8(7)

11.4 Retention Exceptions

11.4.1 Legal Obligations Override Deletion Requests

Certain data must be retained even if the Data Principal withdraws consent (e.g., banking, tax, AML, PF, ESIC).
Section 8(7)(a)

11.4.2 Litigation Hold

If the data is needed for legal defence, investigation, or dispute resolution, retention continues.
Section 7(e)

CHECKLIST

A. Retention Mapping

- ☐ Identify all categories of personal data processed.
- ☐ Map each category to purpose and minimised retention period.
- ☐ Identify legal retention obligations.
  Section 8(7), Section 10)(1)

B. Automated Deletion Controls

- ☐ Configure auto-deletion for purpose completion.
- ☐ Configure auto-deletion for 3-year inactivity (if applicable).

- ☐ Maintain deletion logs.
  Rule 8(1)-(3)

C. Notices & User Communication

- ☐ Automate 48-hour deletion notices.
- ☐ Make deletion workflow transparent to users.
  Rule 8(2)

D. Vendor Retention Oversight

- ☐ Ensure processors retain logs for 1 year.
- ☐ Validate deletion downstream with certificates.
  Section 8(7)(b); Rule 8(3)

12. GRIEVANCE REDRESSAL MECHANISMS

The DPDPA mandates a formalised, structured grievance redressal system for Data Principals. This includes publishing clear procedures, ensuring timely responses, and maintaining complete audit trails.

12.1 Requirement to Provide Grievance Mechanism

12.1.1 Mandatory Public-Facing Grievance System

Every Data Fiduciary must provide Data Principals with clearly defined grievance channels and instructions to submit complaints.
Section 13(1)

12.1.2 Publication of Mechanism

The grievance process must be displayed prominently on the website, mobile app, or digital interface.
Rule 14(1)

12.2 Timelines for Response

12.2.1 Mandatory Resolution Time (Rule 14(3))

Grievances must be resolved within the timelines specified by the Rules - **not exceeding 90 days**. *Rule 14(3)*

12.2.2 Acknowledgment Mechanism

After a grievance is submitted, the Data Fiduciary must acknowledge receipt and provide reference details.
Rule 14(1)-(3)

12.3 Exhaustion Requirement Before Board Complaint

12.3.1 Mandatory Pre-Condition Before Approaching the Board

A Data Principal must first raise a grievance with the Data Fiduciary. The Board will only accept a complaint after this remedy is exhausted.
Section 13(3)

12.4 Corporate Grievance Officer or DPO

12.4.1 Required Contact Details

Data Fiduciaries must publish the contact details of:

- The Data Protection Officer (if SDF), or
- The authorised data protection contact person.
  Section 8(9); Rule 9

12.5 Maintaining Audit Trails

12.5.1 Mandatory Logging of Grievances

Businesses must maintain complete logs of grievance submissions, responses, resolution dates, and escalations.
Section 8(4); Rule 14(3)

CHECKLIST

A. System Requirements

- ☐ Create a user-friendly grievance interface (web, app, email, portal).
- ☐ Publish process, identifiers, and contact person details.

- ☐ Maintain ticketing or CRM-based grievance systems.
  Rule 14(1)-(3)

B. Response Management

- ☐ Acknowledge grievances within 24–48 hours.
- ☐ Resolve within 90 days.
- ☐ Document all actions taken.
  Rule 14(3)

C. Employee Training

- ☐ Train support teams on legal requirements.
- ☐ Standardise response templates.
- ☐ Maintain escalation matrix.
  Section 8(4)

D. Reporting & Audit

- ☐ Conduct periodic reviews of grievance trends.
- ☐ Submit reports to senior management.
  Section 8(1)

13. SIGNIFICANT DATA FIDUCIARIES (SDFs)

The DPDPA introduces a special category of high-risk Data Fiduciaries known as **Significant Data Fiduciaries (SDFs)**. These entities must implement additional, advanced measures such as annual audits, DPIAs, and algorithmic risk assessments.

13.1 Criteria for SDF Classification

13.1.1 Government Notification Requirement

The Central Government designates SDFs based on a risk assessment covering:

- Volume & sensitivity of personal data
- Risk to Data Principals' rights
- Impact on sovereignty, integrity, or public order
- Risk to electoral democracy
- Use of emerging technologies
  Section 10(1)

13.2 Additional Obligations for SDFs

13.2.1 Appointment of Data Protection Officer (DPO)

SDFs must appoint a DPO based in India who reports directly to the Board of Directors.
Section 10(2)(a)

13.2.2 Appointment of Independent Data Auditor

An independent auditor must conduct yearly data audits to assess compliance.
Section 10(2)(b)

13.2.3 Mandatory Data Protection Impact Assessment (DPIA)

SDFs must conduct periodic DPIAs detailing:

- Rights of Data Principals
- Processing purpose
- Risk assessment
- Risk mitigation measures
  Section 10(2)(c)(i)

13.2.4 Periodic Audits

In addition to annual audit, SDFs must conduct periodic internal audits and monitoring assessments.
Section 10(2)(c)(ii)

13.2.5 Algorithmic Transparency & Risk Controls (Rule 13(3))

If algorithms are used, SDFs must verify they:

- Do not result in discriminatory outcomes
- Do not violate rights of Data Principals
- Do not produce harmful or misleading outputs
  Rule 13(3)

13.2.6 Potential Data Localisation Restrictions (Rule 13(4))

Government may notify certain categories of personal data that SDFs cannot transfer outside India.
Rule 13(4)

13.3 Governance Expectations from SDFs

13.3.1 Enterprise Risk Management Integration

SDFs must integrate data protection risks into their ERM frameworks, board risk reports, and compliance dashboards.
Section 10(2)

13.3.2 Enhanced Vendor Oversight

SDFs must conduct deeper due diligence on processors and sub-processors.
Section 10(2)(c)

CHECKLIST

A. SDF Determination

- ☐ Verify if Government has notified your organisation as SDF.
- ☐ Document internal reassessment annually.
  Section 10(1)

B. Governance & Appointments

- ☐ Appoint a DPO reporting to the Board.
- ☐ Appoint an independent data auditor.
  Section 10(2)(a)-(b)

C. DPIA Requirements

- ☐ Conduct DPIAs for high-risk processing.
- ☐ Document risk mitigation measures.

- ☐ Maintain DPIA register.
  Section 10(2)(c)

D. Algorithmic Accountability

- ☐ Document how algorithms work.
- ☐ Evaluate bias, discrimination, and risk.
- ☐ Maintain technical logs of model decisions.
  Rule 13(3)

E. Vendor Oversight

- ☐ Conduct advanced processor audits.
- ☐ Request periodic compliance reports.
  Section 10(2)(c)

14. CROSS-BORDER DATA TRANSFERS

Cross-border data transfer requirements under the DPDPA 2023 and Rules 2025 follow a **"negative list" regime** meaning transfers are generally allowed except to countries that the Central Government specifically restricts through notification.

This chapter provides the complete operational guidance for export of personal data outside India by Data Fiduciaries and Data Processors.

14.1 General Rule: Cross-Border Transfers Are Permitted

14.1.1 Permissive Regime

Unlike earlier drafts of the Indian data protection law, the final Act adopts a transfer-friendly model: personal data **may be transferred to any country**, unless the Central Government declares that transfers to that country are restricted.
Section 16(1)

14.1.2 Business Impact

This gives organisations flexibility to use global hosting, cloud platforms, SaaS providers, or distributed vendor ecosystems unless restrictions apply.
Section 16(1)

14.2 Government Power to Restrict Transfers (Rule 15)

14.2.1 Country-based Restrictions

The Central Government can notify specific **countries or territories** where personal data cannot be transferred for processing.
Section 16; Rule 15(1)(a)

14.2.2 Category-based Restrictions

It may also restrict transfer of **specific categories** of personal data, such as:

- Children's data
- Sensitive health data
- Government-related data
  Section 16

14.2.3 Condition-based Restrictions

The Government may impose compliance conditions such as:

- Contractual clauses
- Adequacy requirements
- Audit certifications
- Data localisation for specific sectors
  Section 16, Rule 15(1)(c)

14.3 Additional SDF-specific Restrictions (Rule 13(4))

If an organisation is designated a Significant Data Fiduciary, the Government may impose **additional restrictions** on cross-border transfers. This includes potential mandatory localisation for certain categories of data.
Rule 13(4)

14.4 Corporate Compliance Actions

14.4.1 Internal Cross-Border Mapping

Companies must maintain detailed records of all cross-border data flows including:

- The country receiving the data
- Purpose of transfer
- Systems involved
- Data categories
  Section 16

14.4.2 Transfer Impact Assessment (TIA)

Before transferring data abroad, organisations should perform a structured assessment evaluating:

- Local privacy laws in the receiving country
- Ability to enforce contracts
- Vendor security capabilities
- Risk of unlawful access by foreign authorities
  Section 16; Rule 13(4)

CHECKLIST

A. Transfer Mapping

- ☐ Identify all cross-border data flows.
- ☐ Create a transfer register detailing purposes, destinations, and vendors.
- ☐ Update the register quarterly.
  Section 16

B. Compliance Controls

- ☐ Verify that no transfers occur to restricted countries.
- ☐ Implement contracts with processors including restrictions and safeguards.
- ☐ Confirm processors abroad comply with Rule 6 controls.
  Rule 15; Rule 6

C. SDF Considerations

- ☐ Check if your SDF designation prohibits certain transfers.
- ☐ Implement localisation if mandated.
  Rule 13(4)

D. Best Practices

- ☐ Conduct Transfer Impact Assessments.
- ☐ Encrypt all exported data.
- ☐ Maintain off-shore vendor audit reports.
  Section 8(5); Rule 6(a)-(d)

15. GOVERNMENT DATA PROCESSING

This chapter governs how organisations interact with the Government or its instrumentalities when personal data is processed for subsidies, benefits, licenses, certificates, permits, regulatory functions, or public authority obligations.

15.1 State-Related Processing (Section 7(b))

15.1.1 Processing for Government Services

Personal data may be processed by the State or its instrumentalities to provide benefits, subsidies, certificates, licenses, permits, or public services without requiring fresh consent if the data was previously provided for similar government-linked purposes.
Section 7(b)(i)

15.1.2 Use of Government Databases

If personal data exists in government records, the State may process it for providing benefits as prescribed.
Section 7(b)(ii)

15.2 Public Order, Security & Sovereignty (Section 7(c))

15.2.1 Mandatory Disclosure in Certain Scenarios

Organisations must disclose data to government authorities when required for:

- Security of the State
- Sovereignty & integrity of India
- Maintenance of public order
  Section 7(c)

15.3 Legal Obligations to Disclose (Section 7(d)-(e))

15.3.1 Statutory Disclosures

If any law requires disclosure e.g., tax, financial regulations, KYC etc, then organisations must comply.
Section 7(d)

15.3.2 Compliance with Court or Tribunal Orders

Processing to comply with judicial orders is always lawful.
Section 7(e)

15.4 Second Schedule Standards (Rule 5)

15.4.1 Mandatory Standards for Government Processing

When processing is done for government purposes under Section 7(b), the following standards apply:

- Minimal personal data processing
- Data quality checks
- Purpose limitation
- Security safeguards
- Transparency obligations
- Publication of contact information
  Rule 5; Second Schedule

15.5 Corporate Responsibilities When Disclosing Data to Government

15.5.1 Validation of Identity and Authority

Corporates must verify that officers making requests are authorised under applicable laws. *Section 7(d)*

15.5.2 Documentation of Disclosures

Maintain logs of:

- What was disclosed
- When
- Under which legal provision
- To which authority
  Section 8(4)

CHECKLIST

A. Lawful Requests

- ☐ Verify legal basis for government requests.
- ☐ Maintain register of government disclosures.
- ☐ Securely share data only through approved channels.
  Section 7(d)-(e)

B. Government Processing Standards

- ☐ Apply Second Schedule standards for government-related processing.
  Rule 5

C. Data Minimisation

- ☐ Share only the minimum personal data required.
- ☐ Document justification for each disclosure.
  Section 7(b); Second Schedule

16. RESEARCH, ARCHIVAL & STATISTICAL EXEMPTIONS

The Act provides specific exemptions for personal data processed for research, archival, and statistical purposes provided that such processing does not affect individual rights.

16.1 Conditions for Research Exemption (Section 17(2)(b))

16.1.1 No Decision-Making Impact

Personal data may be processed without applying certain rights and obligations if the purpose is research, archiving, or statistics, **and** the processing does not lead to decisions affecting individuals.
Section 17(2)(b)

16.1.2 Standards May Be Prescribed

The Central Government may issue standards for such processing.
Section 17(2)(b)

16.2 Requirements for Archival & Statistical Use

16.2.1 Purpose Limitation

Data collected for research or statistics must not be reused for unrelated purposes.
Section 4(1); Section 17(2)(b)

16.2.2 De-identification & Minimisation

Wherever feasible, organisations should de-identify personal data used for research or analytics.
Rule 6(a)

16.3 Safeguards for Research Exemption

16.3.1 Security Requirements Still Apply

Even with exemptions, all Rule 6 security measures remain mandatory.
Section 17(2)(b); Rule 6

16.3.2 Documentation of Research Purposes

Organizations must maintain written records of:

- The research purpose
- Data categories used
- Safeguards applied
  Section 8(4)

CHECKLIST

A. Purpose Validation

- ☐ Confirm the processing is strictly for research or statistics.
- ☐ Verify no decisions are made about individuals.
  Section 17(2)(b)

B. Technical Safeguards

- ☐ Apply anonymisation/pseudonymisation.
- ☐ Restrict access to research teams only.
  Rule 6(a)-(b)

C. Documentation

- ☐ Maintain clear documentation of research purpose.

- ☐ Track data sets used and retention periods.
  Section 8(4)

17. CONSENT MANAGERS & INTEROPERABLE CONSENT SYSTEMS

The DPDPA introduces a new category of regulated entities called **Consent Managers**, designed to make consent more standardised, transparent, interoperable, and portable across platforms.

Consent Managers act as independent intermediaries who enable Data Principals to give, manage, review, or withdraw consent from multiple Data Fiduciaries via a single interface.

17.1 Role and Function of Consent Managers

17.1.1 Single-Window Consent Governance

Consent Managers provide a unified, interoperable system for Data Principals to manage all their consents across different Data Fiduciaries using a single platform (e.g., an app, portal, digital dashboard).
Section 6(7)

17.1.2 Acting on Behalf of the Data Principal

The Consent Manager is accountable to the Data Principal and must act strictly on their instructions.
Section 6(8)

17.1.3 No Commercial Misuse

Consent Managers are prohibited from processing personal data for their own benefit except as required to provide the consent management service.
Section 6(8); Rule 4 Part B Clause 10

17.2 Registration Requirements (Rule 4)

17.2.1 Mandatory Registration with the Board

A Consent Manager must register with the Data Protection Board of India and comply with the eligibility conditions prescribed.
Section 6(9); Rule 4

17.2.2 Technical & Operational Requirements (Rule 4 Part A)

To be registered, the Consent Manager must demonstrate:

- Technical capability
- Interoperability with all Data Fiduciaries
- Secure consent lifecycle management
- Ability to maintain auditability
  Rule 4 Part A Clauses 1–12

17.2.3 Financial Fitness

Consent Managers must maintain the required net worth and operational capacity as notified by the Board.
Rule 4 Part B Clause 4

17.3 Duties & Limitations of Consent Managers

17.3.1 Maintain Consent Lifecycle Records for 7 Years

Consent Managers must keep complete, immutable records of consent creation, review, and withdrawal for a minimum of **seven years**.
Rule 4 Part B Clause 4(c)

17.3.2 Prohibition on Sub-Processing

Consent Managers cannot subcontract or outsource any material consent-management responsibility.
Rule 4 Part B Clause 6

17.3.3 Interoperability Requirements

Consent Managers must provide API interfaces compatible with all Data Fiduciaries, ensuring no platform lock-in and seamless consent portability.
Rule 4 Part A Clause 9

17.4 Obligations of Data Fiduciaries when Working with Consent Managers

17.4.1 Automatic Acceptance of Consent Signals

If a Data Principal gives or withdraws consent through a Consent Manager, the Data Fiduciary must honour it as if directly received.
Section 6(7)-(8)

17.4.2 Synchronisation of Consent Logs

Data Fiduciaries must synchronise internal consent records with Consent Manager logs.
Rule 4 Part A Clause 7

17.4.3 Provide Consent Metadata

Fiduciaries must provide “consent receipt” metadata (e.g., timestamp, purpose, data categories) to the Consent Manager system.
Rule 4 Part A Clause 5

CHECKLIST

A. Integrating with Consent Managers

- ☐ Integrate APIs provided by registered Consent Managers.
- ☐ Synchronise consent logs in real time.
- ☐ Verify Consent Manager registration before integration.
  Section 6(7)-(9); Rule 4

B. Consent Management Controls

- ☐ Generate consent receipts containing required metadata.
- ☐ Honour all withdrawal or modification signals immediately.
- ☐ Log consent changes internally for 7+ years.
  Rule 4 Part B Clause 4(c)

C. Compliance Oversight

- ☐ Conduct annual audits on Consent Manager integrations.
- ☐ Document interoperability tests.
- ☐ Maintain security controls for consent APIs.
  Section 10(2)(c), Section 8(3) & Section 8(5); Rule 4 Part A,B

18. DATA PROTECTION BOARD OF INDIA

The Data Protection Board (the “Board”) is the central regulatory authority for enforcing the DPDPA. It operates digitally and holds wide powers to conduct inquiries, issue directions, and impose penalties.

18.1 Establishment & Structure of the Board

18.1.1 Digital-by-Design Regulatory Body

The Board operates as a fully digital office - complaints, hearings, submissions, and decisions are all conducted through digital mechanisms.
Section 28(1)

18.1.2 Composition

The Board consists of a Chairperson and Members appointed by the Central Government based on expertise in law, technology, governance, administration, or consumer protection.
Section 19(1)-(3)

18.2 Powers & Functions (Section 27)

18.2.1 Handling Personal Data Breaches

The Board may initiate inquiries into any breach reported by a Data Fiduciary and direct urgent mitigation measures.
Section 27(1)(a)

18.2.2 Handling Complaints

The Board investigates complaints submitted by Data Principals concerning:

- Breach of obligations

- Violation of rights
- Breach by Consent Managers
  Section 27(1)(b)-(d)

18.2.3 Issuing Directions

The Board may issue binding directions during or after an inquiry to ensure compliance. *Section 27(2)-(3)*

18.3 Procedure for Inquiries (Section 28)

18.3.1 Grounds for Inquiry

The Board determines whether sufficient grounds exist before launching an inquiry.
Section 28(3)

18.3.2 Principles of Natural Justice

The Board must provide an opportunity of being heard and record reasons in writing.
Section 28(6)-(11)

18.3.3 Civil Court Powers

The Board has powers similar to a civil court:

- Summons
- Discovery
- Inspection
- Receiving evidence
  Section 28(7)

18.4 Appeals (Section 29)

18.4.1 Filing Appeals

Appeals from the Board's orders lie with the Telecom Disputes Settlement and Appellate Tribunal (TDSAT).
Section 29(1)-(2)

CHECKLIST

A. Before a Board Inquiry

- ☐ Maintain updated compliance documentation.
- ☐ Maintain processing records and logs.
- ☐ Maintain breach reports and grievance logs.
  Section 27–29

B. During an Inquiry

- ☐ Respond promptly to Board directions.
- ☐ Submit all evidence digitally.
- ☐ Engage legal counsel.
  Section 28(6)-(11)

C. After an Inquiry

- Implement corrective measures.
- Update Board with compliance reports if asked.
  Section 27(3), Section 28(2), Section 33

19. PENALTIES, ENFORCEMENT & AUDIT READINESS

The DPDPA enforces strict monetary penalties for violations, with maximum penalties reaching ₹250 crore per instance.

19.1 Penalties Framework (Section 33)

19.1.1 Significant Breach Penalties

The Board may impose penalties up to the amounts specified in the Schedule depending on:

- Nature and gravity of breach
- Duration
- Repetitive behaviour
- Gain realised or loss avoided
- Impact on Data Principals
  Section 33(1)-(2)

19.2 Schedule of Penalties (Key Highlights)

- **Failure to prevent a data breach**: up to ₹250 crore *Schedule Item 1*
- **Failure to notify breaches to Data Principals or Board**: up to ₹200 crore *Schedule Item 2*
- **Failure to comply with children's data provisions**: up to ₹200 crore *Schedule Item 3*
- **Failure of Significant Data Fiduciary to meet obligations**: up to ₹150 crore *Schedule Item 4*
- **Negligence of Data Principal duties**: up to ₹10,000 *Schedule Item 5*

19.3 Corporate Audit Readiness

19.3.1 Internal Audits

Corporations must conduct periodic internal audits of:

- Consent management
- Data retention
- Breach readiness
- Vendor contracts
- Security controls
  Section 8(4), Section 8(7); Rule 6

19.4 Documentation Required for Defence

19.4.1 Evidence Repository

Maintain a repository containing:

- Policies & SOPs
- Consent logs
- Rights request logs
- DPIAs
- Vendor assessments
- Training logs
  Section 8(4), Section 10(2)(c); Rule 6(e)

CHECKLIST

A. Prevention Controls

- ☐ Implement robust security safeguards.
- ☐ Maintain retention schedules.

- ☐ Conduct periodic DPIAs.
  Section 8(5), Section 8(7), (8); Section 10(2)

B. Response Controls

- ☐ Maintain breach response teams.
- ☐ Notify the Board without delay.
- ☐ Notify Data Principals with required details.
  Rule 7

C. Audit Readiness

- ☐ Maintain compliance evidence.
- ☐ Conduct quarterly risk reviews.
- ☐ Prepare board-level dashboards.
  Section 10

--END OF DOCUMENT--