COMPLIANCE WORKBOOK FOR DATA FIDUCIARIES UNDER DIGITAL PERSONAL DATA PROTECTION ACT, 2023 & DIGITAL PERSONAL DATA PROTECTION RULES, 2025.

COMPLIANCE WORKBOOK AND OPERATIONAL MANUAL FOR DATA FIDUCIARIES

This workbook functions as a comprehensive regulatory map and practical guide for data fiduciaries' compliance officers, legal counsels, and management bodies acting under the statutory framework of the Digital Personal Data Protection Act, 2023 ("**DPDP Act**"), and the companion Digital Personal Data Protection Rules, 2025 ("**DPDP Rules**"). It translates statutory text into operational actions, detailing liabilities, structural exceptions, and audit parameters.

The DPDP Act applies to the personal data which is stored or processed electronically in India. This includes information that was first collected offline and later digitized. The DPDP Act shall also apply to businesses outside India if they process the digital personal data of people in India while offering products or services to them.

I. Statutory Scope: Who Qualifies as a "Data Fiduciary"?

Under Section 2(i) of the DPDP Act, a "**Data Fiduciary**" is defined as any person who alone or in conjunction with other persons determines the purpose and means of processing personal data. This designation is strictly operational: if your entity determines the purpose and means of processing of personal data, your entity bears primary regulatory responsibility.

The definition of a "person" under Section 2(s) of the DPDP Act encompasses a wide legal scope, meaning your organization falls within this framework if it operates as any of the following:

- An individual or sole proprietorship;
- A Hindu Undivided Family (HUF);
- A company registered under the Companies Act;
- A partnership firm or Limited Liability Partnership (LLP);
- An association of persons or a body of individuals, whether incorporated or not;
- The State and all its instrumentalities, municipal bodies, and public sector undertakings; and
- Every artificial juristic person not falling within the preceding sub-clauses.

Critical Structural Distinctions:

- **Data Fiduciary vs. Data Processor:** A Data Processor (Section 2(k) of the DPDP Act) merely handles digital personal data on behalf of a Data Fiduciary under a commercial contract. The legal liability for tracking consent, fulfilling individual requests, and reporting breaches remains with the Data Fiduciary.
- **Significant Data Fiduciary (SDF):** Under Section 10(1) of the DPDP Act, the Central Government can classify specific entities or classes of Data Fiduciaries as "Significant" based on parameters such as volume, data sensitivity, systematic risk to data privacy rights, potential impact on the sovereignty and integrity of

India, security of the State, or public order. SDFs must adhere to enhanced audit and administrative obligations.

II. Core Compliance Master Matrix

The following matrix translates the provisions of the DPDP Act and the DPDP Rules into actionable parameters. Use this to audit and track your organizational workflows:

Compliance Area	Statutory Provision	Required Action & Operational Workflow	Penalty for Non-Compliance	Explicit Exceptions / Carve-outs
Notice Architecture	Section 5(1), Section 5(2), Rule 3	Formulate an itemized notice to accompany or precede every consent request. It must be in clear language and outline: (i) the exact personal data collected, (ii) specific processing purposes, (iii) pathways to exercise access/erasure rights, and (iv) methods for filing complaints with the Board. Give users the choice to read notices in English or any of the 22 constitutional languages. For personal data collected prior to November 13 2025, the retrospective notice must be issued as soon as reasonably practicable and must specify: (i) the categories of personal data held, (ii) the purposes for which it is currently being processed, and (iii) how the Data Principal may exercise their rights including withdrawal of consent. For children's data collected prior to the Act, the retrospective notice must be issued to the parent or guardian. Following issue of the retrospective notice, any Data Principal who withdraws consent must have their data erased promptly and all downstream processors must be instructed to do the same. Data Fiduciaries with large user bases should note that the mass communication exercise required for legacy data re-solicitation – including data mapping, notice distribution, consent tracking, and erasure workflows – requires significant lead time and should be scoped and	**Standard breach penalty up to Rs. 50 Crore under Section 33(1).**	Not required if processing falls under "Certain Legitimate Uses" (Section 7) or if the data is voluntarily self-disclosed by the user in the public domain. Startups may also be exempted via notifications.

Compliance Area	Statutory Provision	Required Action & Operational Workflow	Penalty for Non-Compliance	Explicit Exceptions / Carve-outs
		planned well in advance of the May 2027 deadline.		
Consent Verification	Section 6, Section 6(10)	Ensure that any consent relied upon is free, specific, informed, unconditional, and unambiguous, supported by a clear affirmative action. Any part of a consent format that waives user rights or violates the law is legally invalid. The consent obtained herein shall be limited to a specified purpose and the processing of such personal data as necessary for such purpose. Establish a consent management mechanism through which the Data Principal may withdraw her consent at any time. Under Section 6(10), the Data Fiduciary carries the burden of proof to demonstrate that proper notice was delivered and valid consent was actively provided during any subsequent legal proceeding.	**Standard breach penalty up to Rs. 50 Crore under Section 33(1).**	No consent needed for Section 7 legitimate uses: medical emergency response, sovereign functions of the State, court order compliance, public order enforcement, or employment safeguards.
Data Security Safeguards	Section 8(4), Section 8(5), Rule 6	Implement technical and organizational infrastructure to prevent data exposure. Minimum standards require: (i) encryption, masking, or tokenization of data, (ii) strict computer access controls, (iii) monitoring and visibility through system logs, and (iv) periodic backups for disaster recovery. Under Rule 6(1)(e), security access logs must be retained for a minimum period of one year.	**Critical penalty up to Rs. 250 Crore for failing to implement controls to prevent a breach.**	Exemptions apply to data processed strictly for personal or domestic functions, or individual research/archiving adhering to the Second Schedule.
Incident Reporting	Section 8(6), Rule 7	Upon discovering a data breach, notify the Data Protection Board and every affected individual immediately and without delay — this initial notification must describe the nature of the breach, its timing, likely consequences, and the Data Fiduciary's contact details. This	**Severe penalty up to Rs. 200 Crore for failure to report a breach to the Board or users.**	None. If a personal data breach occurs, reporting is mandatory irrespective of the corporate structure or entity class.

This note has been prepared as of July 01, 2026, and is based on our understanding and interpretation of the applicable law as of that date.

Compliance Area	Statutory Provision	Required Action & Operational Workflow	Penalty for Non-Compliance	Explicit Exceptions / Carve-outs
		immediate notification is separate from and precedes a comprehensive report to the Board, which must be submitted within 72 hours of discovery and must contain exhaustive facts, updated impact scope, mitigation steps taken, and internal compliance summaries.		
Data Minimization & Erasure	Section 8(7), Rule 8	Erase personal data when consent is withdrawn or when the specified purpose is no longer being served, unless retention is required by applicable law. Ensure downstream Data Processors also erase such data. Data Fiduciaries covered by Rule 8(1) read with the Third Schedule – e-commerce entities with not less than 2 crore registered users in India, social media intermediaries with not less than 2 crore registered users in India, and online gaming intermediaries with not less than 50 lakh registered users in India – must erase personal data after three years if the Data Principal has not approached the Data Fiduciary for performance of the specified purpose or exercised any rights in relation to the processing. Notify the Data Principal at least 48 hours before such auto-erasure. Retain personal data, associated traffic data and processing logs for a minimum of one year before deletion, unless a longer retention period is required under applicable law.	**Standard breach penalty up to Rs. 50 Crore under Section 33(1).**	Retention is permitted if required for compliance with any active Indian law (e.g., banking or tax mandates requiring multi-year ledger storage). Not applicable to specific State databases.
Children's Data Governance	Section 9, Rule 10, Rule 12	Before processing data belonging to a minor under 18 years of age, obtain the verifiable consent of a parent or lawful guardian. Apply due diligence via age records or digital validation tools to verify the guardian is an adult. Fully cease tracking, targeted advertising, or behavioural monitoring directed at children. Do not conduct any	**Severe penalty up to Rs. 200 Crore for violating child safety or minor consent protocols.**	Rule 12/Fourth Schedule exempts clinical establishments, educational institutions, creches, and children's transport providers

Compliance Area	Statutory Provision	Required Action & Operational Workflow	Penalty for Non-Compliance	Explicit Exceptions / Carve-outs
		processing that could negatively affect a child's well-being.		from parental consent/tracking restrictions for specific educational, safety, or healthcare purposes.
Vendor & Processor Risk	Section 8(2), Rule 6(1)(f)	Ensure that any third-party Data Processor or sub-contractor is engaged exclusively under a valid written contract. The contract must contain strict clauses obligating the processor to implement identical security safeguards, restrict processing to the specified purpose, maintain log retention, and immediately report anomalies to the Data Fiduciary.	**The Data Fiduciary remains directly liable for the processor's defaults. Where a processor's default results in a data breach, the applicable penalty against the Data Fiduciary is not limited to the residual Rs. 50 Crore under Section 33(1) — security failures carry a penalty of up to Rs. 250 Crore and breach notification failures carry a penalty of up to Rs. 200 Crore. The Rs. 50 Crore residual penalty applies only to defaults that do not trigger the higher specific penalty provisions.**	Processing data of non-residents inside India pursuant to contracts executed with entities outside India is exempt from most Chapter II restrictions.

Compliance Area	Statutory Provision	Required Action & Operational Workflow	Penalty for Non-Compliance	Explicit Exceptions / Carve-outs
Data Accuracy	Section 8(3), Rule 5	If your entity processes personal data that is likely to be used to make an impactful decision affecting the individual, or is disclosed to another Data Fiduciary, you must implement verification protocols to maintain data completeness, accuracy, and consistency.	**Standard breach penalty up to Rs. 50 Crore under Section 33(1).**	State processing for non-decision-making registries or archival statistical datasets under Rule 16 is exempt from accuracy clauses.
Rights & Grievance Redressal	Section 8(10), Section 11, Section 12, Section 13, Rule 14	Provide visible endpoints on applications and websites for users to exercise access, correction, erasure, or nomination requests. Establish an internal grievance redressal mechanism. Resolve all user grievances or requests within an explicit compliance timeframe not exceeding a maximum of 90 days. Publish contact details of the grievance resolution officer prominently. Additionally, under Section 14, Data Principals have the right to nominate another individual to exercise their data rights on their behalf in the event of death or incapacity. Data Fiduciaries must provide a mechanism for users to register and update such nominations.	**Standard breach penalty up to Rs. 50 Crore under Section 33(1).**	Data sharing driven by legal demands from enforcement agencies for offence prevention or cyber incident management is exempt from user access disclosures (Section 11(2)).
Legitimate Uses of Data	Section 7	Section 7 permits processing without a notice-and-consent cycle in the following categories of legitimate use: (a) processing by the State or its instrumentalities for providing subsidies, benefits, services, or the issuance of licences or permits; (b) performance of any function under any law or for the exercise of any power vested in the State; (c) compliance with a judgment or decree of any court or tribunal; (d) response to a medical emergency or epidemic; (e) en-	**Not applicable as a standalone ground – however, if processing purportedly under Section 7 is found to fall outside its scope, standard penalties under Section 33(1) apply.**	The boundary of what qualifies as a legitimate use under Section 7 is unsettled and is likely to be contentious – processing models relying heavily on this provision carry interpretive risk.

This note has been prepared as of July 01, 2026, and is based on our understanding and interpretation of the applicable law as of that date.

Compliance Area	Statutory Provision	Required Action & Operational Workflow	Penalty for Non-Compliance	Explicit Exceptions / Carve-outs
		suring safety during a disaster or breakdown of public order; (f) processing by an employer of personal data of employees for employment-related purposes; and (g) processing for purposes related to the Data Principal's voluntary self-disclosure in a specific context. Note that Section 7 deemed consent does not override the security safeguard and breach notification obligations under Section 8(4) and 8(5), which apply regardless.		
Cross-Border Data Transfers	Section 16	Personal data may be transferred outside India subject to such terms and conditions as the Central Government may prescribe. The framework operates on a blacklist model — transfers are permitted to all jurisdictions unless the Central Government specifically restricts transfer to a particular country or entity by notification. Data Fiduciaries with offshore data infrastructure, foreign parent companies, or international operations should monitor Central Government notifications under Section 16 and maintain a record of the jurisdictions to which personal data is transferred. SDFs are additionally subject to potential data localisation requirements under Rule 13(4) – specified categories of personal data and related traffic metadata may be required to be stored within India.	**Violations of Central Government restrictions on cross-border transfers would attract penalty under Section 33(1) up to Rs. 50 Crore.**	Processing of personal data of individuals located outside India by an Indian entity pursuant to a contract with an entity outside India is exempt from Chapter II obligations under Section 17(1)(d).
Consent Manager Integration	Section 6, Rule 4	A new class of regulated intermediary – the Consent Manager – will provide Data Principals a single interface to grant, review, and withdraw consent across multiple platforms. Registration of Consent Managers opens November 13, 2026. While use of a Consent Manager is not mandatory, every Data Fiduciary relying on consent must	**Failure to honour consent withdrawal signals would constitute a breach of Section 6 consent obligations — penalty up to Rs. 50 Crore**	-

This note has been prepared as of July 01, 2026, and is based on our understanding and interpretation of the applicable law as of that date.

Compliance Area	Statutory Provision	Required Action & Operational Workflow	Penalty for Non-Compliance	Explicit Exceptions / Carve-outs
		build API infrastructure capable of receiving consent signals from registered Consent Managers and acting on withdrawals in real time without delay. All consent records – whether managed through a Consent Manager or directly – must be retained for a minimum of seven years. Data Fiduciaries should commence infrastructure development immediately to enable integration testing once the first Consent Managers are registered.	**under Section 33(1).**	

III. Operational Protocols for Significant Data Fiduciaries (SDF)

If your enterprise is notified as a Significant Data Fiduciary under Section 10(1) of the DPDP Act, you must implement the following advanced operational structures within the timeline specified in Rule 13 of the DPDP Rules:

1. **Appoint an India-Based Data Protection Officer (DPO):** Under Section 10(2)(a), you must appoint an individual who is based physically in India and who reports directly to your Board of Directors or an equivalent governing body. This DPO must serve as the structural point of contact for the grievance mechanism and represent the entity before the Board.
2. **Engage an Independent External Data Auditor:** Under Section 10(2)(b), you must appoint an independent auditor to carry out periodic data audits. The auditor will evaluate the company's structural compliance metrics and operational gaps.
3. **Mandatory 12-Month Audits and DPIA:** Under Rule 13(1) and 13(2), you must conduct a Data Protection Impact Assessment (DPIA) and an independent compliance audit at least once every 12 months. A detailed report containing significant observations from the assessment and audit must be formally submitted to the Data Protection Board of India. The DPIA must include an exhaustive description of individual rights, processing risks, and systemic risk mitigation tactics.
4. **Algorithmic Due Diligence:** Under Rule 13(3), the SDF must undertake periodic due diligence of its algorithmic systems and processing logic to ensure they do not pose a risk to the rights of Data Principals.
5. **Territorial Data Localization:** Under Rule 13(4), you must monitor and comply with restrictions that prevent the cross-border flow or transfer of specified personal datasets and related traffic metadata outside the physical territory of India, based on central committee recommendations.
6. **Penalty for SDF Default:** Failure to execute any of these enhanced Section 10 obligations carries an independent monetary penalty that may extend to Rs.150 Crore under Sl. No. 4 of the Schedule.

This note has been prepared as of July 01, 2026, and is based on our understanding and interpretation of the applicable law as of that date.

IV. Comprehensive Analysis of Exemptions & Carve-outs

The DPDP Act and the DPDP Rules provide structured exemptions where specified compliance mandates do not apply to a Data Fiduciary. These are categorized into distinct operational frameworks:

1. **Absolute Out-of-Scope Exceptions (Section 3(c)):**
   - **Personal/Domestic Purpose:** The provisions of the Act do not apply to data processed by an individual completely for a personal or domestic function.
   - **Voluntary Self-Disclosure:** The Act does not apply to data made available in the public domain voluntarily by the Data Principal to whom it relates. For example, if a user blogs about their personal contact details on public social media fields, further corporate use of that specific public field does not violate notice rules.
   - **Legal Mandate Disclosures:** Data made available in the public domain under a statutory obligation in India (e.g., public shareholder registries or land transactions) is completely out of scope.

2. **Strategic Operational Exemptions (Section 17(1)):**
   In the following scenarios, the provisions of Chapter II (except security safeguards under Section 8(4) and breach obligations under Section 8(5)), Chapter III (Data Principal Rights), and Section 16 (Cross-border transfer rules) shall not apply:
   - **Legal Rights Enforcement:** Processing data to enforce an active legal right or maintain an active judicial claim.
   - **Judicial & Quasi-Judicial Processing:** Processing handled by a court, tribunal, or regulatory body in India executing judicial or regulatory functions.
   - **Offence Prevention & Investigation:** Data processed by authorized agencies for the prevention, detection, investigation, or prosecution of any offence or contravention of law in India.
   - **Cross-Border Outsourcing Contracts:** Personal data of individuals located outside India processed by an Indian entity pursuant to an outsourcing contract executed with an organization outside India.
   - **Corporate Restructuring:** Processing necessary to implement a scheme of arrangement, compromise, merger, or amalgamation approved by a court or competent authority.
   - **Financial Default Recovery:** Processing required to ascertain financial info, assets, or liabilities of a credit defaulter who has breached a loan contract with a financial institution.

3. **Special Class Exemptions (Section 17(2) & 17(3)):**
   - **Research, Archiving, & Statistics:** Under Section 17(2)(b) and Rule 16, processing for historical research, archiving, or statistical analysis is exempt from standard constraints, provided data is not used to make a specific decision affecting a particular individual and complies with the Second Schedule.
   - **Startup Carve-outs:** Under Section 17(3), the Central Government can exempt notified startups and specific classes of small Data Fiduciaries from Section 5 (Notice obligations), Section 8(3) (Data accuracy parameters), Section 8(7) (Mandatory data erasure timelines), Section 10 (SDF structures),

and Section 11 (Access parameters). This helps reduce operational overhead for early-stage companies. **Note**: As of the date of this workbook, the Central Government has not yet operationalised this exemption or prescribed eligibility criteria. The startup carve-out is therefore not currently available to rely upon.

V. Enforcement Framework: Board Inquiries & Appellate Channels

Note: As of the date of this workbook, the Data Protection Board has been constituted but its Chairperson and Members have not yet been formally appointed. The Board is therefore not yet fully operational. This does not affect the May 13, 2027 compliance deadline, which is statutory and independent of the Board's operational status. Enforcement actions can only practically commence once the Board is fully constituted. To manage corporate risks effectively, compliance teams must understand the procedural timelines governing enforcement actions handled by the Data Protection Board of India (DPB) and judicial channels:

1. **Inquiry Completion Timelines:** Under Rule 19(9) of the DPDP Rules, any formal inquiry into a breach, complaint, or reference must be completed by the Board within an explicit period of six months from the date of receipt. Extensions can be granted for reasons recorded in writing, limited to a maximum of three months at a time.
2. **Civil Court Bar:** Under Section 39 of the DPDP Act, civil courts are barred from entertaining any suit or proceeding in respect of matters falling within the Board's statutory powers. No injunctions can be granted against actions taken in good faith under this law.
3. **TDSAT Appellate Channel:** Any Data Fiduciary aggrieved by an order or direction issued by the Board can file a formal appeal before the Telecom Disputes Settlement and Appellate Tribunal (TDSAT), designated as the Appellate Tribunal under Section 2(a) and Section 44(1) of the DPDP Act.
4. **Appellate Timelines:** Under Section 29(2) of the DPDP Act, the appeal must be filed within 60 days from the date of receiving the order. Under Rule 22 of the DPDP Rules, the appeal must be submitted digitally via the system and accompanied by the fee applicable under the TRAI Act, 1997, payable through UPI or RBI-authorized digital networks. The Tribunal is mandated under Section 29(6) to resolve the appeal within a target timeframe of six months.