Digital Personal Data Protection Rules, 2025

Detailed Summary & Compliance Note

(Based solely on MeitY Notification G.S.R. 846(E), dated 13 November 2025)

---

1. Background & Commencement

1.1 Legal Basis

The **Digital Personal Data Protection Rules, 2025** are issued under **section 40(1) & (2)** of the **Digital Personal Data Protection Act, 2023 (DPDPA)**.

Draft rules were published on **3 January 2025** inviting objections/suggestions within 45 days. After considering public comments, the final rules have now been notified.

1.2 Short Title & Commencement (Rule 1)

- These rules are called the **Digital Personal Data Protection Rules, 2025**.
- Commencement is staggered:

1. **Effective immediately on publication in Official Gazette**:
    - **Rules 1 & 2** (short title & definitions)
    - **Rules 17 to 21** (Data Protection Board constitution & functioning)
2. **Effective 1 year after publication**:
    - **Rule 4** (Registration & obligations of Consent Managers)
3. **Effective 18 months after publication**:
    - **Rules 3, 5 to 16, 22 and 23**
      These include core operational obligations: notice, security safeguards, breach notification, retention, verifiable consent, Significant Data Fiduciary duties, cross-border transfers, research exemptions, appeals, and information requests.

Compliance takeaway:

- Governance & Board-related rules bite **immediately**.
- Core operational / compliance obligations kick in **after 18 months**, giving an implementation window (which everyone will still waste until the last 2 weeks because humans).

© Aayush Desai | LinkedIn: linkedin.com/in/desaiaayush

2. Definitions & Key Terms (Rule 2 + context from Act)

The Rules rely heavily on terms defined in the **Act**. Rule 2 adds some specific definitions:

2.1 Defined in the Rules

1. **"Act"**
   - Means the **Digital Personal Data Protection Act, 2023 (22 of 2023)**.
2. **"Techno-legal measures"**
   - Refers to measures mentioned under **Rules 20 and 22**.
   - Practically: use of digital processes, systems and tools to enable **fully digital functioning** of the Board and Appellate Tribunal (e.g., e-filings, online hearings, remote participation, electronic authentication, etc.).
3. **"User account"**
   - The **online account** registered by the **Data Principal** with the **Data Fiduciary**, including:
     - Profiles, pages, handles
     - Email address, mobile number
     - Any other presence used to access the Fiduciary's services.
4. **"Verifiable consent"**
   - Consent as specified in **Rule 10 or Rule 11**, i.e.:
     - For **children**: verifiable consent of the parent.
     - For **persons with disability with lawful guardian**: verifiable consent of the lawful guardian.

2.2 Key Terms (from the Act, relied upon in the Rules)

Without reprinting the whole Act, the following terms are central for applying these Rules:

- **Data Principal**: Individual to whom the personal data relates.
- **Data Fiduciary**: Entity that determines the purpose and means of processing.
- **Significant Data Fiduciary (SDF)**: Data Fiduciary notified as such by the Central Government based on volume/sensitivity/risk.
- **Data Processor**: Processes personal data on behalf of a Data Fiduciary.
- **Board**: Data Protection Board of India.
- **Consent Manager**: Entity that enables Data Principals to give, manage, review, and withdraw consent through an interoperable platform.

Compliance takeaway:
You need to treat **"verifiable consent"**, **"user account"**, and **"techno-legal**

© Aayush Desai | LinkedIn: linkedin.com/in/desaiaayush

measures" as technical compliance hooks directly referenced in later operational rules.

---

3. Notice & Transparency Obligations (Rule 3, Rule 9 & Rule 14)

3.1 Notice by Data Fiduciary (Rule 3)

The **notice** to Data Principals must:

1. **Be standalone & understandable**
   - Notice must be **presented and be understandable independently** of other information (no burying in 20-page T&Cs).
2. **Be clear, plain & specific**
   Must provide a **fair account** enabling **specific and informed consent**, including at minimum:
   - **Itemised description** of personal data being processed.
   - **Specified purpose(s)** of processing.
   - **Specific description of goods/services** to be provided or uses to be enabled by such processing.
3. **Include access & rights links**
   Notice must give:
   - The **specific communication link** (URL/app path) for accessing the Data Fiduciary's **website/app**; and
   - A description of other means, if any, through which the Data Principal may:
     - **Withdraw consent**, with **ease comparable** to that of giving consent.
     - **Exercise rights** under the Act.
     - **Make a complaint to the Board**.

Practical impact:

- No dark patterns. Withdrawal must be as easy as consent.
- Need **standardised DP notice templates** with itemised data categories, purposes, and direct links.

3.2 Contact for Questions on Processing (Rule 9)

Each Data Fiduciary must:

- **Prominently publish** on its website/app:

© Aayush Desai | LinkedIn: linkedin.com/in/desaiaayush

    - The **business contact information** of the **Data Protection Officer** (if applicable) or
    - A person **able to answer** questions of Data Principals regarding processing of their personal data.
- Also **mention this contact** in **every response** to a Data Principal exercising rights.

Compliance task:

- Create a **single, consistent contact line** (email, phone, etc.) and bake it into templates for rights responses.

3.3 Rights of Data Principals & Grievance Redressal (Rule 14)

1. **Publication of process (Rule 14(1))**
   Data Fiduciary & Consent Manager must **prominently publish** on website/app:
    - **How** a Data Principal can make a rights request.
    - **What identifiers/particulars** (e.g., username, account no., email, etc.) are required.
2. **Making rights requests (Rule 14(2))**
    - Data Principal may make a request to the Data Fiduciary **to whom she has previously given consent**, using the published means.
3. **Grievance redressal timelines (Rule 14(3))**
    - Each Data Fiduciary / Consent Manager must:
        - Have a **grievance redressal system** to respond to grievances of Data Principals **within a "reasonable period" not exceeding 90 days**; and
        - Implement **technical & organisational measures** to ensure effectiveness.
4. **Nomination (Rule 14(4))**
    - Data Principal may **nominate** one or more individuals (in line with the Act) to exercise her rights, using means & particulars required by the Data Fiduciary.
5. **Identifier (Rule 14(5))**
    - "Identifier" includes:
      Customer ID, CAF number, application reference number, enrolment ID, email, mobile number, licence number, etc.

Compliance takeaway:

- Need **documented rights-handling SOPs**, with clear identification criteria.
- 90-day upper limit for grievance resolution is baked into law; internal SLA should be **shorter**.

© Aayush Desai | LinkedIn: linkedin.com/in/desaiaayush

4. Security Safeguards & Data Breach Management (Rules 6, 7 & 8)

4.1 Reasonable Security Safeguards (Rule 6)

Data Fiduciary must protect personal data **in its possession or under its control**, including what is processed by Data Processors, by taking **reasonable security safeguards** to prevent personal data breach. Minimum measures include:

1. **Data security techniques**
    - Encryption
    - Obfuscation
    - Masking
    - Virtual tokens mapped to personal data.
2. **Access control**
    - Measures to control access to **computer resources** used by the Data Fiduciary / Data Processor.
3. **Logging & monitoring**
    - Visibility on access to personal data through **logs, monitoring, and review**
    - Designed to enable **detection**, **investigation**, **remediation**, and **prevention of recurrence**.
4. **Continuity & backups**
    - Reasonable measures to ensure **continued processing** in case of loss/destruction/unavailability of personal data (e.g., backups).
5. **Minimum 1-year retention of logs & personal data**
    - To support detection, investigation, remediation, and continuity, the Data Fiduciary must:
        - Retain logs and personal data for **at least 1 year**, unless another law requires otherwise.
6. **Contracting with Data Processors**
    - Contracts must contain **appropriate provisions** requiring the Data Processor to take reasonable security safeguards.
7. **Technical & organisational measures**
    - Must ensure effective observance of security safeguards overall.

Compliance tasks:

- Formal **security controls framework** aligned with these minimums.
- Mandatory **logging & log retention** (minimum 1 year).
- DP-Processor contracts to be **updated** to mirror these obligations.

© Aayush Desai | LinkedIn: linkedin.com/in/desaiaayush

4.2 Intimation of Personal Data Breach (Rule 7)

On becoming aware of a **personal data breach**, the Data Fiduciary must notify both:

(A) Affected Data Principals

Intimation must be:

- **Without delay**
- In a **concise, clear, and plain** manner
- Through user account or another **registered communication mode**

Must include:

1. **Description of breach**: nature, extent, timing.
2. **Consequences** relevant to the Data Principal.
3. **Measures implemented / being implemented** by the Fiduciary to mitigate risk.
4. **Recommended safety measures** for the Data Principal.
5. **Business contact information** of a person who can respond to queries.

(B) The Board

Two-stage obligation:

1. **Immediately ("without delay")**:
    - Basic description: **nature, extent, timing, location**, and likely impact.
2. **Within 72 hours of awareness** (or extended period allowed by Board on written request):
    - Updated and detailed information including:
        1. Detailed description of breach.
        2. Broad facts of events, circumstances, reasons.
        3. Measures implemented/proposed to mitigate risk.
        4. Findings on person who caused the breach.
        5. Remedial steps to prevent recurrence.
        6. Report regarding intimations given to affected Data Principals.

Compliance takeaway:

- Need a **formal incident response playbook** mapped to the **72-hour outer limit**.
- Evidence trail (logs, root cause report, remediation, DP notifications) is legally mandatory, not optional PR.

© Aayush Desai | LinkedIn: linkedin.com/in/desaiaayush

4.3 Purpose Limitation & Data Retention (Rule 8 + Third & Seventh Schedules)

4.3.1 Deemed end of specified purpose for certain large platforms (Rule 8(1) & Third Schedule)

For specific **classes of large digital Data Fiduciaries**, personal data must be erased after a defined period of **inactivity** by the Data Principal, unless retention is required by law.

Classes covered (Third Schedule):

1. **E-commerce entity** with **≥ 2 crore registered users in India**
2. **Online gaming intermediary** with **≥ 50 lakh registered users in India**
3. **Social media intermediary** with **≥ 2 crore registered users in India**

For these:

- For **all purposes**, *except*:
  - Enabling the Data Principal to **access her user account**; and
  - Enabling access to **virtual tokens** stored on the platform that can be used to obtain money, goods, or services.
- Personal data must be erased:
  - After **3 years** from the date the Data Principal **last approached** the Data Fiduciary for:
    - performance of specified purpose, or
    - exercise of rights

    OR
  - From the commencement of these Rules, **whichever is later**,

unless retention is required by any law.

4.3.2 Advance intimation before erasure (Rule 8(2))

At least **48 hours before** the erasure date, the Data Fiduciary must **inform the Data Principal** that:

- Personal data will be erased upon completion of the period;
- Unless she logs into the user account or otherwise initiates contact to perform the specified purpose or exercise rights.

4.3.3 Mandatory 1-year retention for logs & traffic data for all processing (Rule 8(3))

Separately from the above:

- For **any processing** by the Data Fiduciary or its Processor, it must retain:
  - Personal data

© Aayush Desai | LinkedIn: linkedin.com/in/desaiaayush

    - **Associated traffic data**
    - Logs of processing
- For **minimum 1 year** from the date of such processing, for purposes in the **Seventh Schedule**, after which data/logs must be erased unless further required by law.

Compliance takeaways:

- Large platforms must implement **inactivity-based deletion** logic (3 years) + **48-hour pre-erasure notification**.
- Everyone must build **1-year minimum data & log retention** into their data lifecycle, especially for investigation/tracing/state use purposes.

---

5. State Processing, Research & Exemptions (Rules 5 & 16 + Second Schedule)

5.1 Processing by State & its Instrumentalities for Subsidy/Benefit/Service (Rule 5)

Rule 5 applies to processing of personal data by the **State or its instrumentalities** for:

- Provision/issue of **subsidy, benefit, service, certificate, licence, permit**, etc.:
    - **Under law**
    - **Under policy** (executive power)
    - **Using public funds** (CFI, State Consolidated Fund, public accounts, or funds of local authorities).

Processing must follow the **standards in the Second Schedule**, which include:

- Lawful processing
- Limited to necessary data
- Accuracy and consistency
- Appropriate retention (only as long as required or mandated by law)
- Security safeguards
- Intimation to Data Principals where processing is under section 7(b) (including DP contact info & link to rights)
- Accountability of the person determining purposes & means of processing.

5.2 Research, Archiving, Statistical Purposes (Rule 16 + Second Schedule)

- Processing of personal data **necessary** for:
    - **Research**,
    - **Archiving**, or

© Aayush Desai | LinkedIn: linkedin.com/in/desaiaayush

- **Statistical purposes**

is **exempt from the Act** if carried out in accordance with the **Second Schedule standards**.

Compliance takeaway:

- For State / research projects, you need documented adherence to **Second Schedule standards**, not a free-for-all "research" excuse.

---

6. Verifiable Consent: Children & Persons with Disability (Rules 10, 11 & 12 + Fourth Schedule)

6.1 Verifiable Consent for Children (Rule 10)

For processing **personal data of a child**, the Data Fiduciary must:

1. **Obtain verifiable consent of the parent**, using appropriate technical & organisational measures.
2. **Verify that the parent is an identifiable adult** (≥ 18 years), by reference to:
    - Reliable identity & age details already available with the Fiduciary; or
    - Identity & age details voluntarily provided by:
        - The individual; or
        - A **virtual token** mapped to such details issued by an **authorised entity**, including via a **Digital Locker service provider**.

Key definitions:

- **Adult**: Individual who has completed 18 years.
- **Authorised entity**:
    - Entity entrusted by law or Government to issue identity & age details or virtual token,
    - Or a person appointed by such entity,
    - Includes details/tokens made available and verified by a **Digital Locker service provider**.
- **Digital Locker service provider**: Intermediary/body corporate/Government agency notified by Central Government under IT Act rules.

The rule provides illustrations covering:

- Child declaring parent; parent already registered on platform.

© Aayush Desai | LinkedIn: linkedin.com/in/desaiaayush

- Child declaring parent; parent not registered; verification via ID/token/DigiLocker.
- Parent initiating account for child (registered & unregistered cases).

Compliance task:

- Build **age/parent verification flow** that can integrate with ID data or virtual tokens / DigiLocker.
- Document what your system treats as "reliable" age & identity proof.

6.2 Verifiable Consent for Person with Disability with Lawful Guardian (Rule 11)

When obtaining **verifiable consent from a lawful guardian** of a person with disability, the Data Fiduciary must:

- Exercise **due diligence** to verify that:
    - The guardian is appointed under applicable guardianship law by:
        - A court of law, or
        - A **designated authority**, or
        - A **local level committee**.

Definitions tie into:

- **Rights of Persons with Disabilities Act, 2016**
- **National Trust Act, 1999**
- "Person with disability" covers:
    - A person with long term physical/mental/intellectual/sensory impairment unable to take legally binding decisions despite support; and
    - A person with autism, cerebral palsy, mental retardation, multiple disabilities, etc., unable to take legally binding decisions despite support.

Compliance takeaway:

- Need a **document-checking protocol** for guardianship orders/certificates; simple self-declaration is not enough.

6.3 Exemptions for Child Data Processing (Rule 12 & Fourth Schedule)

Section 9(1) & (3) of the Act usually impose additional obligations for processing children's data. Under Rule 12:

© Aayush Desai | LinkedIn: linkedin.com/in/desaiaayush

1. **Part A – Exempt classes of Data Fiduciaries**

Certain categories are **exempt from section 9(1) and (3)**, subject to conditions, including:

- **Clinical establishments / mental health establishments / healthcare professionals**
  - Processing restricted to provision of health services & necessary for protection of child's health.
- **Allied healthcare professionals**
  - Processing restricted to supporting implementation of treatment/referral plans for child.
- **Educational institutions**
  - Processing restricted to tracking/behavioural monitoring:
    - For educational activities; or
    - In the interest of safety of enrolled children.
- **Individuals running crèches/child day care centres**
  - Processing for tracking & behavioural monitoring in interest of safety.
- **Transport providers engaged by educational institutions/crèches**
  - Processing restricted to tracking location of children for safety during travel.

2. **Part B – Exempt purposes**

Section 9(1) & (3) do not apply where processing children's data is for purposes such as:

- Exercise of powers/performance of functions in children's interest under law.
- Provision of subsidy/benefit/service under law/policy using public funds in child's interest.
- Creating a **user account for communication by email** (restricted to that purpose).
- Determining **real-time location of a child** for their safety and protection.
- Ensuring harmful/detrimental content/ads/services are **not accessible to the child**.
- Confirming that a Data Principal is **not a child**, and performing due diligence under Rule 10.

Compliance takeaway:

- Child-related services in healthcare/education/transport have broader room to process data for safety/health, but within **strict necessity-based limits**.

© Aayush Desai | LinkedIn: linkedin.com/in/desaiaayush

7. Significant Data Fiduciaries (SDFs): Extra Duties (Rule 13)

Once notified as a **Significant Data Fiduciary**, an entity must:

1. **Annual DP Impact Assessment & Audit (Rule 13(1))**
    - At least **once in every 12-month period** from notification, the SDF must:
        - Undertake a **Data Protection Impact Assessment (DPIA)**; and
        - Undertake an **audit** to ensure effective observance of the Act & Rules.
2. **Report to Board (Rule 13(2))**
    - The DPIA/audit executor must submit a **report containing significant observations** to the Board.
3. **Due diligence on technical measures & algorithms (Rule 13(3))**
    - SDF must verify that **technical measures including algorithmic software** used for hosting/display/upload/modification/publishing/transmission/storage/updating/sharing of personal data are **not likely to pose a risk to Data Principals' rights**.
4. **Localized processing of specified personal data (Rule 13(4))**
    - SDF must ensure that **certain personal data specified by Central Government** (on recommendation of a committee) is processed with the restriction that:
        - The personal data and **traffic data** relating to its flow **are not transferred outside India**.
5. **Committee (Rule 13(5))**
    - Central Government will constitute a committee with:
        - Officials from MeitY
        - May include officials from other Ministries/Departments
    - This committee will recommend which personal data is to be restricted from cross-border transfer.

Compliance takeaway:

- SDFs must build **continuous DPIA + audit cycles**, algorithmic risk assessments, and possibly implement **data localisation** for specified categories and corresponding traffic data.

© Aayush Desai | LinkedIn: linkedin.com/in/desaiaayush

8. Consent Managers: Registration & Obligations (Rule 4 & First Schedule)

8.1 Registration (Rule 4 + First Schedule Part A)

To register as a **Consent Manager**, an applicant must:

- Apply to the **Board** with particulars the Board specifies.
- Meet conditions such as:
    - Being a **company incorporated in India**.
    - Having sufficient technical, operational & financial capacity.
    - Sound financial condition & management character.
    - **Net worth ≥ INR 2 crore**.
    - Adequate business prospects & capital structure.
    - Directors/KMP/senior management with reputation for fairness & integrity.
    - MOA/AOA to include adherence obligations & amendment only with prior Board approval.
    - Operations must be in **interests of Data Principals**.
    - Independent certification of:
        - Interoperable platform consistency with **data protection standards & assurance framework** published by the Board;
        - Adequacy of technical/organisational measures.

Board may:

- **Register & publish particulars**; or
- **Reject application** with reasons.

Board may:

- Monitor adherence,
- Issue directions for corrective measures, and
- **Suspend/cancel registration** if necessary in Data Principals' interests (after hearing).

8.2 Obligations of Consent Manager (First Schedule Part B)

Key obligations:

1. **Enable giving, managing, reviewing & withdrawing consent**
    - Through its platform, directly to a Data Fiduciary or via another onboarded Fiduciary.
2. **Non-readability of content**

© Aayush Desai | LinkedIn: linkedin.com/in/desaiaayush

- Manner of making available or sharing personal data should ensure **contents are not readable** by the Consent Manager.

3. **Recordkeeping**
   - Maintain records of:
     - Consents given/denied/withdrawn
     - Notices preceding/accompanying consent requests
     - Sharing of personal data with transferee Fiduciaries
   - Give Data Principal:
     - Access to records
     - Ability to obtain records in **machine-readable form**
   - Maintain records **at least 7 years** (or longer by agreement/law).
4. **Platform presence**
   - Must maintain **website or app (or both)** as primary access mechanism.
5. **No subcontracting of obligations**
   - Cannot sub-contract or assign performance of its obligations under Act/Rules.
6. **Security safeguards**
   - Must take reasonable security safeguards to prevent personal data breach.
7. **Fiduciary capacity**
   - Must act in a **fiduciary capacity** vis-à-vis the Data Principal.
8. **Conflict of interest management**
   - Avoid conflict with Data Fiduciaries (promoters/KMP etc.).
   - Measures to ensure no conflict arising from directors/KMP/senior management holding significant shareholding/employment/pecuniary relationships with Data Fiduciaries.
9. **Transparency obligations**
   - Publish on website/app:
     - Promoters, directors, KMP & senior management
     - Persons holding >2% shareholding
     - Body corporates in which they hold >2%
     - Any other information directed by Board.
10. **Audit mechanisms**
    - Maintain effective audit mechanisms and report:
      - Controls, systems, procedures, safeguards
      - Continued fulfilment of registration conditions
      - Adherence to obligations under Act & Rules.
11. **Change of control**
    - Control cannot be transferred (sale, merger, etc.) without **prior Board approval** and subject to conditions.

Compliance takeaway (if you ever use/partner with a Consent Manager):

© Aayush Desai | LinkedIn: linkedin.com/in/desaiaayush

- Treat Consent Manager relationships like **regulated infrastructure**, not just another SaaS integration. Their governance & transparency obligations are high.

---

9. Cross-Border Transfer of Personal Data (Rule 15)

Rule 15 states:

- **Any personal data** processed by a Data Fiduciary under the Act **may be transferred outside India** subject to the restriction that:
    - The Data Fiduciary shall meet **requirements specified by the Central Government** (via general or special order) regarding making such personal data available to any:
        - **Foreign State**, or
        - **Person/entity under control of or an agency of such State**.

Compliance takeaway:

- General cross-border transfers are permitted but subject to **Government-imposed conditions**, especially where data is to be made available to foreign States or their controlled entities.
- SDFs also face specific localisation and traffic data restrictions under Rule 13(4).

---

10. Governance & Institutional Framework (Rules 17–21, Fifth & Sixth Schedules)

10.1 Appointment of Chairperson & Members of the Board (Rule 17)

- Central Government constitutes **Search-cum-Selection Committees**:
    - For **Chairperson**:
        - Chaired by Cabinet Secretary
        - Members: Secretaries (Legal Affairs & MeitY) + 2 experts
    - For **Members (other than Chairperson)**:
        - Chaired by Secretary, MeitY
        - Members: Secretary, Legal Affairs + 2 experts
- Government appoints Chairperson/Members based on recommendations.
- Committee proceedings not invalid due to vacancy, absence, or defect in constitution.

© Aayush Desai | LinkedIn: linkedin.com/in/desaiaayush

10.2 Terms of Service of Chairperson & Members (Rule 18 & Fifth Schedule)

Key points:

- **Consolidated salary**:
  - Chairperson: **INR 4,50,000 per month**
  - Member: **INR 4,00,000 per month**
  - No house or car facility.
- **Provident Fund**, no pension/gratuity from Board service.
- **TA/DA**, **LTC**, **leave**, **medical assistance**, **conduct**, **disciplinary** provisions largely mirror those of senior Central Government officers at:
  - **Level 17 of pay matrix** (Chairperson)
  - **Level 15 of pay matrix** (Members)
- No sitting fee, no sumptuary allowance; conflict of interest rules applies.

10.3 Procedure of Board (Rule 19)

- Chairperson fixes date/time/place & agenda of meetings.
- **Quorum**: one-third of membership.
- Decisions by **majority**; tie-breaking vote with Chairperson/chairing Member.
- Members with interest in an item must **recuse**.
- Chairperson can:
  - Take **emergent decisions** (recording reasons) and place for ratification later.
  - Use **circulation** for decision-making.
- Board must **complete inquiries within 6 months** of receipt under section 27 of the Act, extendable by max **3 months at a time** with recorded reasons.

10.4 Digital Functioning of Board (Rule 20)

- Board shall function as a **digital office** and may adopt **techno-legal measures** to conduct proceedings without requiring **physical presence** of individuals, subject to its powers to summon & examine persons on oath.

10.5 Officers & Employees of Board (Rule 21 & Sixth Schedule)

- Board may appoint officers/employees with **prior Central Government approval**, including on **deputation** (from Government, PSUs, statutory bodies, NISG, etc.).
- Terms of service for officers/employees mirror Central Civil Services rules (leave, LTC, conduct, discipline, gratuity, etc.).

Governance takeaway:

© Aayush Desai | LinkedIn: linkedin.com/in/desaiaayush

- Board is designed as a **digitally-native regulator**, with strong continuity with Indian civil service frameworks.

---

11. Appeals & Government Information Requests (Rules 22 & 23 + Seventh Schedule)

11.1 Appeals to Appellate Tribunal (Rule 22)

- Any person **aggrieved by Board's order/direction** may appeal to the **Appellate Tribunal**.
- Appeal must be filed **in digital form** as decided by Tribunal.
- Appeal fee:
  - Same as applicable to appeals under **TRAI Act, 1997**,
  - Payable digitally via **UPI or other RBI-authorised payment system**,
  - Can be **reduced/waived at Chairperson's discretion**.
- Tribunal:
  - Not bound by **Civil Procedure Code, 1908**,
  - Guided by **principles of natural justice**, may regulate its own procedure.
  - Functions as a **digital office**, may use techno-legal measures to avoid physical presence.

11.2 Calling for Information from Data Fiduciary or Intermediary (Rule 23 & Seventh Schedule)

- **Central Government** may, for purposes specified in Seventh Schedule, acting through an **authorised person**, require any Data Fiduciary or **intermediary** to furnish information within a specified period.

Seventh Schedule purposes include:

1. **Use of personal data** by State or its instrumentalities in the interests of:
   - **Sovereignty & integrity of India**
   - **Security of the State**
2. Use of personal data by State/instrumentalities for:
   - Performing functions under law
   - Disclosing information for fulfilling legal obligations
3. **Assessment for notifying a Data Fiduciary or class as SDF**

- Where disclosure of such information would **prejudicially affect sovereignty/integrity/security of State**, Central Government may require the Data Fiduciary/intermediary **not to disclose** such furnishing to the affected Data Principal or others, except with prior written permission.

© Aayush Desai | LinkedIn: linkedin.com/in/desaiaayush

Compliance takeaway:

- You need a **Government request handling process**, including logging, escalation, and classification, especially for non-disclosure instructions.

---

12. Quick Compliance Checklist for Your Privacy Team

If you want the short operational punch-list from all this:

1. **Notices & consent**
   - Redraft notices to be **itemised, specific, and standalone**.
   - Build easy **withdrawal channels** (same ease as giving consent).
2. **Security & breach**
   - Implement **encryption/masking/tokenisation** where relevant.
   - Ensure **access control**, **logging**, and **minimum 1-year log retention**.
   - Draft **breach response SOP** with:
     - DP notification template
     - Board intimation (immediate + 72-hour report) templates.
3. **Retention & erasure**
   - Design **data retention schedule** incorporating:
     - 1-year minimum logs/traffic data
     - 3-year inactivity-based deletion for large e-comm/gaming/social media (if applicable).
     - 48-hour pre-erasure notice triggers.
4. **Children & disability**
   - Build **verifiable parent consent flows** & **age verification**.
   - Create **guardian documentation** checks under applicable disability laws.
5. **Rights & grievances**
   - Publish clear **rights request channels** and identifier requirements.
   - Implement a **≤90-day grievance closure** mechanism (internally target sooner).
6. **SDF readiness (if likely to be notified)**
   - Plan for **annual DPIA + audit**.
   - Design **algorithmic risk assessment framework**.
   - Prepare for **data localisation** for notified datasets & traffic data.
7. **Consent Manager interactions**
   - If using Consent Managers, ensure they are **properly registered** and aligned to First Schedule obligations.
8. **Government & law enforcement**
   - Establish **standard operating procedure** for handling information requests under Rule 23 & Seventh Schedule, including confidentiality constraints.

© Aayush Desai | LinkedIn: linkedin.com/in/desaiaayush

Disclaimer

This document is a **summary prepared for educational and informational purposes only**. It is **not legal advice**, does not constitute a legal opinion, and should not be relied upon for compliance or decision-making. Parts of the formatting and refinement were assisted using AI tools; readers should **independently verify the accuracy** of all content with the official notification, the Digital Personal Data Protection Act, 2023, and the Digital Personal Data Protection Rules, 2025.

Neither the author nor the publishing platform assumes responsibility for any errors, omissions, or interpretations contained herein.

© Aayush Desai | LinkedIn: linkedin.com/in/desaiaayush