**1️⃣ Overview**

* **Full name:** Digital Personal Data Protection Act, 2023
* **Enforced by:** Government of India (future: Data Protection Board of India – DPBI)
* **Scope:** Covers processing of **digital personal data** within India, and outside India if for offering goods/services to individuals in India.
* **Focus:** Balances **individual rights** and **lawful processing** of personal data, while enabling innovation and government functions.

**2️⃣ Key Definitions**

| **Term** | **Meaning** |
| --- | --- |
| **Data Principal** | The individual whose personal data is processed. |
| **Data Fiduciary** | Entity determining purpose & means of processing. |
| **Data Processor** | Processes data on behalf of the Data Fiduciary. |
| **Consent Manager** | Registered entity to manage consents on behalf of Data Principals. |
| **Significant Data Fiduciary (SDF)** | DF with large volume/sensitivity of data, risk to rights, or impact on state security — extra obligations. |
| **Personal Data** | Any data about an individual who can be identified. |
| **Digital Personal Data** | Personal data in digital form, or digitized from physical form. |

**3️⃣ Core Principles (Similar to GDPR Art. 5)**

* **Lawfulness** – Only process data for lawful purposes.
* **Purpose Limitation** – Use data only for stated purposes.
* **Data Minimization** – Collect only what’s necessary.
* **Accuracy** – Keep data accurate and updated.
* **Storage Limitation** – Delete data when no longer needed.
* **Security Safeguards** – Protect against breaches.
* **Accountability** – Fiduciary is accountable for compliance.

**4️⃣ Lawful Bases for Processing**

* **Consent** – Must be free, specific, informed, unconditional, clear affirmative action.
* **Legitimate Uses** (similar to GDPR Art. 6 exceptions):
  + State functions (licenses, subsidies, legal obligations)
  + Compliance with law/judicial orders
  + Emergencies (health, disaster)
  + Employment purposes (within reasonable scope)

**5️⃣ Data Principal Rights**

* **Right to Access** – Info on processing, summary of data.
* **Right to Correction & Erasure** – Correct inaccurate data, delete when not needed.
* **Right to Grievance Redressal** – Appeal to DPBI if unsatisfied with DF’s response.
* **Right to Nominate** – Nominee can exercise rights in case of death/incapacity.

**6️⃣ Data Fiduciary Obligations**

* Publish **privacy notice** in English + local languages.
* Obtain valid consent (via own platform or Consent Manager).
* Implement security measures to protect data.
* Notify DPBI and affected Data Principals in case of breach.
* Erase personal data once purpose is served & no legal retention applies.
* Maintain accuracy of data used.
* For **SDFs**: Appoint **Data Protection Officer (DPO)**, conduct **DPIA**, maintain records, periodic audits.

**7️⃣ Data Breach Process**

* **Trigger:** Any personal data compromise affecting confidentiality, integrity, or availability.
* **Obligation:** Notify **DPBI** and **affected individuals** “as soon as possible” (no fixed hours yet in law).
* **Content:** Nature of breach, data affected, mitigation steps.

**8️⃣ Penalties**

* Up to **₹250 crore per instance** for significant breaches (esp. children’s data, breach notifications).
* Penalties graded depending on type & severity of violation.

**9️⃣ Comparison – DPDP vs GDPR**

| **Area** | **GDPR** | **DPDP** |
| --- | --- | --- |
| Scope | Personal data (digital + physical) | Digital personal data only |
| Rights | 8 main rights (access, erasure, portability, objection, etc.) | Fewer rights (access, correction/erasure, grievance, nominate) |
| Supervisory Authority | Independent DPAs in each EU state | Data Protection Board of India (central) |
| Basis for Processing | 6 lawful bases | Consent + Legitimate Uses |
| Cross-Border Transfer | Adequacy decisions, SCCs, BCRs | To countries notified by Central Govt (positive whitelist) |
| Breach Notification | 72h to authority | “As soon as possible” (no exact hours defined yet) |
| Penalties | Up to €20M or 4% global turnover | Up to ₹250 crore per instance |
| Children’s Data | Consent from guardian under 16 (can be lowered to 13) | Parental consent mandatory under 18 |

**🔟 Implementer vs Auditor View**

**Implementer Perspective**

* Build **consent management process** (recording, withdrawal).
* Classify if you are a **Significant Data Fiduciary** → appoint DPO, run DPIA.
* Create **privacy notices** & ensure they’re updated and multilingual.
* Set up **data retention schedule**.
* Train employees handling personal data.
* Build **breach detection & reporting process**.

**Auditor Perspective**

* Check existence & clarity of privacy notices.
* Verify consent records & withdrawal process.
* Review breach logs, evidence of timely reporting.
* Inspect DPIA reports (if SDF).
* Check records of erasure requests & retention compliance.
* Sample test accuracy maintenance process.