DIGITAL PERSONAL DATA PROTECTION ACT, 2023

updated as per the DRAFT DPDP RULES, 2025

tsaaro consulting

KEY DEFINITIONS (SECTION 2)

DATA FIDUCIARY

Determines purpose and means of processing personal data.

DATA PRINCIPAL

Individual to whom personal data belongs

PERSONAL DATA

Any data about a person that can be used to identify them.

SIGNIFICANT DATA FIDUCIARY

Data fiduciary notified by the Central Government based on factors like volume and sensitivity of personal data processed, etc.

BOARD

Data Protection Board of India established for implementation and enforcement of the Act.

CONSENT MANAGER

Person registered with the Board acting as single point of contact to enable a Data Principal to manage her consent.

OBLIGATIONS OF SIGNIFICANT DATA FIDUCIARIES (SDF) (SECTION 10)

- Appointment of **Data Protection Officer.**
- Appointment of **independent data auditor.**
- Undertake **Data Protection Impact Assessments** and **Audits** once every period of **12 months** from the date notified as SDF. (Rule 12(1))
- DPIA and Audit reports to be shared with the Board. (Rule 12(2))
- Must ensure algorithmic software does not risk Data Principals' rights. (Rule 12(3))
- Must ensure specified personal data is processed **without transfer outside India**, as restricted by the Government. (Rule 12(4))

PROCESSING OF PERSONAL DATA OUTSIDE INDIA (Section 16)

The transfer of personal data outside India by a Data Fiduciary, whether processed within India or outside in relation to offering goods or services to Data Principals in India, is subject to compliance with requirements specified by the Central Government through *general or special orders* regarding such transfers to foreign states or entities under their control. (Rule 14)

APPLICABILITY (SECTION 3)

This Act applies to digital **personal data processed in India**, collected in digital form and non-digital form that are digitized subsequently.

It also covers **data processing outside India** related to offering goods or services to Data Principals within the territory of India.

RIGHTS OF DATA PRINCIPALS

Right to Access Information (Section 11)

Request for summary of processed personal data and identities of shared entities.

Right to Correction and Erasure (Section 12)

Right to correct, complete, update, and erase personal data.

Right to Grievance Redressal (Section 13)

Right to access grievance redressal mechanisms to raise complaints. Data Fiduciary to publish grievance response timelines. (Rule 13(3))

Right to Nominate (Section 14)

Right to nominate an individual in the event of death or incapacity. (Section 14)

PROCESSING OF CHILDREN'S PERSONAL DATA (SECTION 9)

- Data Fiduciaries must obtain **verifiable consent** from a parent or lawful guardian before processing a child's or disabled person's data.
- **Due diligence** is required to confirm the parent or guardian's identity and legal authority, using reliable records or government-verified tokens like Digital Lockers. (Rule 10)
- **Healthcare providers**, **educational institutions**, **daycare centres**, and **transport providers** are exempted from processing limited to health, safety, education, age verification, and welfare-related purposes. (Rule 11 r/w Schedule 4)

Additional Provisions

Registration and obligations of Consent Manager (Rule 4 r/w Schedule I)

Eligible individuals can apply for Consent Manager registration. The Board verifies compliance, registers or rejects applications with reasons, and enforces obligations. Non-compliance may lead to suspension or cancellation after a hearing.

Exemption for research, archiving and statistical purposes (Rule 15 r/w Schedule II)

Exemptions from certain DPDPA provisions apply for research, archiving, and statistical purposes with appropriate safeguards. These safeguards must ensure lawful processing, data minimization, accuracy, limited retention, security, and accountability.

Retention Timelines (Rule 8 r/w Schedule III)

SDFs like **E-commerce entities** (≥2 crore users), **online gaming intermediaries** (≥50 lakh users), and **social media intermediaries** (≥2 crore users) must retain data for ***three years*** from the last interaction, rights exercise, or commencement of DPDP Rules, whichever is latest, except for account maintenance or token-based services.

OBLIGATIONS OF DATA FIDUCIARIES (SECTION 8)

VALID CONTRACT

Process personal data on its behalf for any activity related to offering of goods or services to Data Principals only under a valid contract.

DATA PROTECTION MEASURES

Implement reasonable security safeguards to protect personal data like **encryption**, **obfuscation** or **masking** or the use of **virtual tokens**. Additional measures also include implementing **access controls**, maintaining **logs** and data **backups mechanisms** (Rule 6).

DATA ACCURACY AND CONSISTENCY

Ensure the accuracy, completeness, and consistency of personal data.

BREACH NOTIFICATIONS

Notify affected Data Principals and the Board immediately after a data breach, including details, risks, and mitigation steps. Provide a detailed report to the Board within **72 hours**. (Rule 7)

BUSINESS CONTACT INFORMATION

Publish contact details of representative or a DPO on *website* or *app* to handle data principals' queries about personal data processing (Rule 9).

DATA ERASURE

Notify the Data Principals **48 hours** before erasing personal data, allowing them to log in, contact the Fiduciary, or exercise their rights if needed (Rule 8).

DUTIES OF DATA PRINCIPAL: (SECTION 15)

- Comply with all applicable laws while exercising rights under this Act.
- Ensure not to impersonate another person when providing personal data.
- Ensure not to suppress material information when providing personal data for official documents or identifiers.
- Ensure not to register false or frivolous grievances or complaints with a Data Fiduciary or the Board.
- Provide only verifiably authentic information when exercising the right to correction or erasure.

PENALTIES FOR NON-COMPLIANCE: (SECTION 33)

- Data fiduciaries risk up to **INR 850 crore** for breach of any provision of the act.
- Data principals can be penalized up to **INR 10,000** for breach in observance of their duties.