

**Digital Personal Data Protection Act, 2023**  
**Important Provisions and Actionable**

**Basic**

- **Status as on 19.8.2023:**
  - Act yet to be in force.
  - Rules yet to be made.
  - Data Protection Board of India (DPBI) (Authority under the Act) yet to be established.
- **Preamble:** To provide for processing of digital personal data recognising:
  - (i) Right of individuals to protect their personal data; and
  - (ii) Need to process such personal data for lawful purposes.

**Principles for the use of Personal Data (As stated in the Explanation to the underlying Bill)**

1. To be lawful, fair and transparent to the related individual.
2. Only for the purposes for which it is collected.
3. To collect only minimum required for the specific purpose.
4. Reasonable effort to ensure it is accurate and kept up to date.
5. Not to store perpetually, but only for necessary duration.
6. Reasonable safeguards for no unauthorised collection or processing to prevent breach.
7. Person deciding the purpose and means of processing to be accountable.

**Important Definitions**

- **Data:** Representation of information, facts, concepts, opinions or instructions in a manner suitable for communication, interpretation or processing by human beings or by automated means.
- **Personal Data:** Data about an individual who is identifiable by or in relation to such data.
- **Digital Personal Data:** Personal Data collected in digital form or in non-digital form digitised subsequently.
- **Data Fiduciary:** Person who determines the purpose and means of processing of Personal Data.
- **Data Principal:** Individual to whom the Personal Data relates and includes guardian if any of the Individual
- **Data Processor:** Person who processes Personal Data on behalf of a Data Fiduciary.
- **Data Protection Officer:** An individual appointed as such by the Significant Data Fiduciary.
- **Significant Data Fiduciary:** Data Fiduciary notified by the Central Government as such.
- **Board:** Data Protection Board of India.
- **Processing:** Operation performed on Digital Personal Data including collection, recording, organisation, structuring, storage, adaptation, retrieval, use, alignment or combination, indexing, sharing, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction.
- **Consent Manager:** A person registered with the Board, who acts as a single point of contact to enable a Data Principal to give, manage, review and withdraw her consent through an accessible, transparent and interoperable platform.

**Digital Personal Data Protection Act, 2023**  
**Important Provisions and Actionable**

**Applicability of Data Fiduciary's Obligations**

- **Applicable in case of Digital Personal Data:**
  - Processed in India.
  - Processed outside India if it is for offering of goods or services in India to Data Principal.
- **Not applicable in case of Personal Data:**
  - Processed by an individual for any personal or domestic purpose
  - Made publicly available by
    - Data Principal to whom it relates; or
    - Any other person required to do so under law.
- **Not applicable** in certain situations under Section 17.

**Processing and Consent of Personal Data**

- To be processed only with the consent of the Data Principal.
- Data Fiduciary to give notice to the Data Principal stating the particulars of Personal Data and purpose for processing, methods of consent, withdrawal of consent and complaint to the Board, and contact details of the Data Protection Officer/ other authorised person.
- Notice to be in plain words (in English or in any Indian language).
- Consent to be free, specific, informed, unconditional, unambiguous by affirmative action and withdrawable.

**Data Fiduciary's responsibility regarding Personal Data**

- To protect Personal Data in its possession or under its control, during any processing undertaken by it or on its behalf by a Data Processor - taking reasonable safeguards to prevent breach.
- Unless required under law, to erase Personal Data (and also cause its Data Processor also to erase the same) on the date earlier of-
  - (i) Data Principal withdraws consent; and
  - (ii) The purpose is no longer served.
- To publish the contact information of a Data Protection Officer/ other person in lieu to answer the questions of Data Principal.
- To establish an effective mechanism to redress the grievances.
- On being asked by the Data Principal, to:
  - Provide details of the Personal Data processed/ with whom shared/ what is shared.
  - Provide to correct/ to complete/ to update/ to erase the Personal Data.

**Nomination**

- Data Principal can nominate another individual to act in case of death or incapacity of the Data Principal.

**Data Principal's Duties**

- Not to suppress any material information while providing own Personal Data.
- To provide only verifiable information while requesting for correction/ erasure of Personal Data.

**Digital Personal Data Protection Act, 2023**  
**Important Provisions and Actionable**

**Grievance Redressal for Data Principal**

- To first approach the Data Fiduciary/ Consent Manager.
- Thereafter may approach the Board.
- Board may refer the matter to mediation.
- Tribunal will have powers of Civil Court for summons to and examination on oath of any person, and for receiving evidence of affidavit, inspection of books and documents etc.
- Thereafter may appeal before the Telecom Disputes Appellate Tribunal.
- Order of Appellate Tribunal executable as decree of civil court for which Appellate Tribunal will have full powers of civil court.
- Thereafter may approach the Supreme Court.

**Penalty to Data Fiduciary**

<b>Breach</b>	<b>Penalty (Maximum)</b>
Breach in observing the obligation of Data Fiduciary to take reasonable security safeguards to prevent personal data breach	Rs. 250 crores
Breach in observing the obligation to give the Board or affected Data Principal notice of a personal data breach	Rs. 200 crores
Breach in observance of additional obligations in relation to children	Rs. 200 crores
Breach in observance of additional obligations of Significant Data Fiduciary	Rs. 150 crores
Breach of any term of voluntary undertaking	Various
Breach of any other provision of the Act or Rules made thereunder	Rs. 50 crores

**Penalty to Data Principal**

- For Breach in observance of the duties- Maximum Rs.10,000.-

**Actionable for Data Fiduciaries**

**(Banks/ NBFCs/ HFCs/ Fis/ Fintechs and their vendors/ partners etc receive Personal Data and would be liable as Data Fiduciary and also may even as Significant Data Fiduciary)**

- Establish Personal Data Management Policy & Procedure.
- Create Consent Mechanism.
- Consider appointing Consent Manager.
- Significant Data Fiduciary to:
  - Appoint Data Protection Officer and Independent Data Auditor.
  - Periodically do Data Protection Impact Assessment, Data Audit by independent Data Auditor etc.
- Other Data Fiduciaries may designate a person in lieu of Data Protection Officer.

**End**

See full text of the act here:

<https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf>