1. **Digital Personal Data Protection Act**

The DPDP Act of 2023 is India's first data protection act, and it establishes a framework for the processing of personal data in India. It applies to the processing of digital personal data within the territory of India collected online or collected offline and later digitized. It is also applicable to processing digital personal data outside the territory of India, if it involves providing goods or services to the data principals within the territory of India.

The bill was introduced and passed in the upper house of the Indian Parliament Rajya Sabha on 9 August 2023. On 11 August 2023, President of India has given assent to the Digital Personal Data Protection Bill, 2023 which made it the Digital Personal Data Protection Act, 2023.

The Government of India has notified the Digital Personal Data Protection (DPDP) Rules, 2025 on 14 November 2025, marking the full operationalization of the DPDP Act, 2023. Together, the Act and Rules create a simple, citizen-focused and innovation-friendly framework for the responsible use of digital personal data.

Key principles:

1. **Data fiduciaries**: These are entities that determine how and why personal data is processed. The government can classify some data fiduciaries as "significant data fiduciaries" (SDFs). SDFs have heightened compliance obligations.
2. **Data principles**: These are the individuals whose personal data is being processed.
3. **Data Processor**: Individual who processes personal data on behalf of data fiduciary.
4. **Data protection officers (DPOs)**: Companies must appoint a DPO to ensure compliance with the law. The DPO acts as a point of contact between the organization, data principals, and regulatory authorities.
5. **Verifiable consent**: The act recognizes verifiable consent for children & people with disabilities.
6. **Enforcement**: The Data Protection Board is the enforcement authority under the DPDP Act and has power to issue penalties for non-compliance.
7. **Replacing existing laws**: The DPDP Act will replace key provisions of the Information Technology Act, 2000 (IT Act) and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data of Information) Rules, 2011 (SPDI rules).

Key considerations:

1. Digital personal data means personal data in digital form.
2. The Act introduces duties for data principles and imposes a penalty up to INR 10,000 for any breach of duty.
3. There are financial penalties up to INR 250 crore for data fiduciary and the Act does not impose criminal penalty for non-compliance.
4. Significant Data Fiduciary (SDF) notified by the government will be accountable for additional obligations.

Material and Territorial Scope

The act proposes to apply to, Within the Indian territory w.r.t processing of digital personal data within the territory of India, where the personal data is collected in

1. Digital form
2. Personal data collected in non-digital form and digitized subsequently

Outside the Indian territory- to processing of digital personal data outside the territory of India, if such processing is in connection with

1. Any activity related to offering of goods or services to data principals within the territory of India.

Exclusions

The Act doesn't apply to-

1. Personal data processed by an individual for any personal or domestic purpose; and Personal data that is made or caused to be made publicly available by the data principal to whom such personal data relates
2. Person who is under an obligation under any law for the time being in force in India to make such personal data publicly available

2. Data Privacy

To ensure that the bank collects, processes, and manages personal data responsibly, respecting the rights of data owners (customers) and complying with legal and regulatory requirements, including the Digital Personal Data Protection Act, 2023 (DPDP Act).

Key Principles and Responsibilities

Data Owner (Customer) Obligations

- Provide **accurate and complete personal data** while availing banking products and services.
- Understand the **purpose of data collection** and provide informed consent.
- Exercise rights under the DPDP Act, such as requesting corrections or exercising the **right to be forgotten**.

Data Fiduciary (Bank) Obligations

The bank, as a **data fiduciary**, must:

- **Process personal data lawfully and fairly**, only for specified purposes.
- Maintain **accuracy, integrity, and confidentiality** of personal data.
- Implement **technical and organizational measures** to prevent unauthorized access, misuse, or breaches.
- Maintain **records of data processing activities** for accountability and audit purposes.
- Ensure **third-party vendors** handling customer data comply with privacy requirements.

Consent Management

- Obtain **explicit consent** from customers before collecting or processing personal data.
- Clearly explain the **purpose, duration, and scope** of data processing.
- Allow customers to **withdraw or modify consent** at any time.
- Maintain a **centralized consent register** to track and manage consent status.

Privacy Impact Assessment (PIA)

- Conduct **Privacy Impact Assessments** before initiating new data processing projects or using new technologies.
- Identify **potential privacy risks** and implement mitigation measures.
- Ensure PIA findings are **documented and reviewed** by the Data Governance team.

Right to Forget / Data Erasure

- Facilitate customers' **right to request deletion of personal data** where:
    - Data is no longer necessary for the purpose it was collected.
    - Consent has been withdrawn.
    - Data processing is unlawful.
- Ensure secure **deletion or anonymization** of data from all systems, including backups, in a verifiable manner.

Additional Privacy Controls

- Implement **data minimization**: Collect only data necessary for the intended purpose.
- **Anonymize or pseudonymize** data for analytics or reporting to reduce exposure of personal information.
- Maintain **audit trails** for all processing activities.
- Provide **training to employees** on data privacy requirements and obligations.
- Access to PII must follow least-privilege and need-to-know principles.
- Role-based access controls (RBAC) must be enforced for all systems containing PII.
- Privileged access to PII (admins, DBAs, support staff) must be strongly controlled, monitored, and audited.
- Multi-factor authentication (MFA) must be enabled for all users accessing systems holding PII.

3. Aadhaar/Privacy Grievance Redressal

Any grievances related to Aadhar data processing shall be addressed promptly.
Bandhan Bank will nominate a suitable Aadhaar/Privacy grievance officer for handling matters related to Data privacy.

4. Regulatory References

1. Aadhaar (Targeted Delivery of Financial and other Subsidies, benefits and services) Act, 2016 i.e., Aadhaar Act, 2016 and its associated regulations and standards prescribed by UIDAI
2. Aadhar (Authentication and Offline Verification) Regulations, 2021

3. UIDAI Information Security Policy for AUA/KUA
4. Various circulars issued by UIDAI
5. Information Technology Act, 2000
6. Information Technology (Amendment) Act 2008
7. Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011
8. Digital Personal Data Protection Act, 2023 (DPDP Act) and Rules 2025