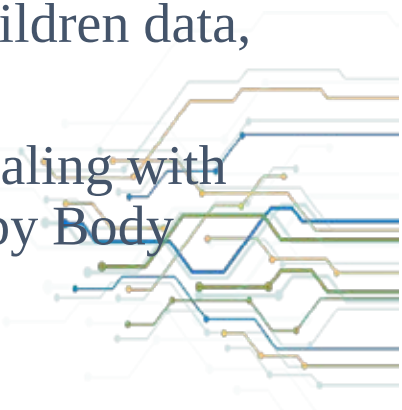
Understanding The Digital Personal Data Protection Act, 2023, Rules in the Judicial context

Rakesh Maheshwari
Advisor, Tech Policy and Regulatory Compliance
Former Sr. Director and GC, Cyber Law & Data governance
Ministry of Electronics and Information Technology (MeitY)
rakeshmaheshwari@gmail.com

The Digital Personal Data Protection (DPDP) Act, 2023

- Enacted on 11th August, 2023, the Rules have been notified w.e.f. 13th Nov., 2025 and hence the law has kicked into operation.
  - Empowers Individuals.
  - Defines Business responsibilities.
  - Establishes governing framework.
- Applicable to almost all organizations processing digital/ digitised personal data while they provide goods or services for users in India.
- The Act applies to the previously collected personal data also.
- The organizations (data Fiduciaries) need to be compliant by 13th May, 2027.
- Differentiated Obligations of organisations depending upon the the personal data handled by them. Government, R&D, organisations dealing with children data, SDFs, Smaller SDFs etc.
- The Act replaces the existing privacy provisions of section 43A (Dealing with processing and Security of Sensitive personal data and information by Body Corporate) of the Information Technology Act, 2000.



Applicability of the DPDP Act

Applies to

- **Processing** of digital personal data **within India** when the data is collected in digital form or non-digital form but digitised subsequently.
- **Processing** of digital personal data **outside India** if such processing is in connection with any activity related to offering of goods or services to Data Principals within India.
- Applicable to both the private and public entities, unless specifically exempted.
- applies uniformly to **all digital personal data irrespective of sensitivity/ classification;**

Does not apply to

- Digital personal data processed for **personal/ domestic** purpose.
- Digital personal data that is made **publicly available** by Data Principal or any other person under an obligation/ law.
- Data **not digital**, **not identifiable**, or **non-personal** (aggregate, anonymized)
- Notified Exempted State Instrumentality(ies).

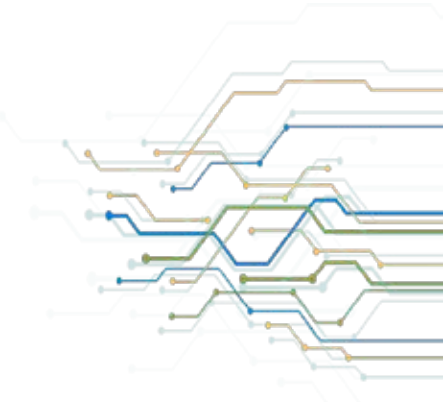
Key Definitions and their interpretation

Personal data

- **Personal data**: Any data about an individual who is identifiable by or **in relation** to it.
- It is broad definition.
- It is like Personally “Personally identifiable information (PII)”.
- Personal data can be:
  - Your physiological data, Health data, Financial data
  - Your location including the past locations.
  - Your preferences external/ internal
  - Your computer device
- Personal data can be:
  - Basic Personal details/ Basic Subscriber Information.
  - Transactional data/ Meta Data about the individual.
  - Actual Content data of the individual.
- The Act does not provide for any classification like Sensitive Personal Data or Information, as has been defined in the present IT Act.

Processing

- As per DPDP Act:
  - "***Processing***" means wholly/ partly automated operation/set of operations performed on digital personal data, and includes collection, recording, organisation, structuring, storage, adaptation, retrieval, use, indexing, sharing, disclosure, restriction, erasure, etc.



Key Stakeholders

Data Principal

- The individual whose personal data is being processed
- Include Child + parent, or disabled person + her legal guardian.

Data Fiduciary (DF)

- The entity who alone or in conjunction with other persons determines the purpose and means of processing
- The entity can be any person including private or Govt. entity

Data Processor (DP)

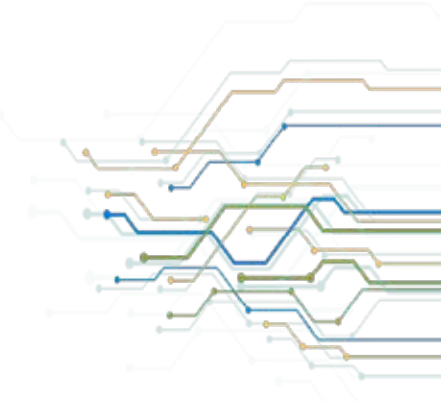
- The Person who processes personal data on behalf of a Data Fiduciary

Child: An individual below 18 years.

Personal data Breach

- Personal Data Breach means
  - any **unauthorised processing (e.g unauthorized sharing, stealing, hacking, attack)** of personal data or
  - **accidental disclosure, acquisition, sharing, use, alteration, destruction** or
  - **loss of access to personal data**,

  that compromises the confidentiality, integrity or availability of personal data.
- Can be by a person within or outside.



Principles underlying the DPDP Act (Not explicitly stated in the Act)

1. **Principle of lawful, fair & transparent usage of personal data**

2. **Principle of purpose limitation**
   Use data only for the specified purpose

3. **Principle of data minimisation**
   Collect only data necessary for the specified purpose

4. **Principle of data accuracy**
   Make reasonable efforts to update & ensure accuracy

5. **Principle of storage limitation**
   Store data only for the duration in which it is needed for the specified purpose

6. **Principle of reasonable safeguards**
   Reasonable security safeguards to ensure no unauthorised collection or processing

7. **Principle of accountability**
   Person deciding purpose & means of processing to be accountable

Broad Structure of the DPDP Act

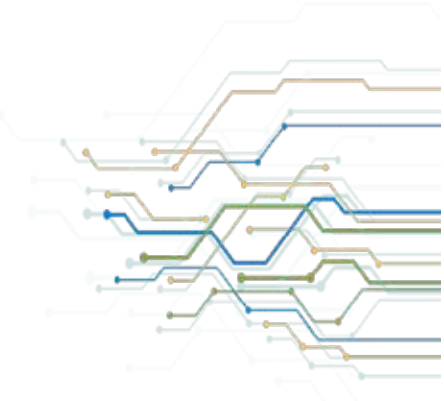
Chapter-I **PRELIMINARY**	Chapter-II **OBLIGATIONS OF DATA FIDUCIARY**	Chapter-III **RIGHTS AND DUTIES OF DATA PRINCIPAL**	Chapter-IV **SPECIAL PROVISIONS**	Chapter-V and VI **DATA PROTECTION BOARD OF INDIA**
• Title and Commencement	• Grounds for processing personal data. • Notice • Consent (and also **Consent manager)**	• Right to access information about personal data (PD)	Processing of personal data outside India.	Composition, Appointments, salary, powers etc Officers and Employees
• Definitions	• General Obligations of the Data Fiduciary	• Right to correction and erasure of PD	• Exemptions • For Business and Lawful requests. • Exemptions from the Act (Agencies to be notified) • Exemptions to startups and specified DF	Proceedings Members and Officers to be Public servants
• Application/ of the Act	• Certain legitimate uses	• Right of grievance redressal.		
	• Processing of personal data of children.	• Right to nominate.		**Powers and functions of Board**
	• Addl obligations of Significant Data Fiduciary. (SDF)	• Duties of Data Principal.		Procedure to be followed by Board. **(Digital...)**

Broad structure of the DPDP Act

Chapter-VII **APPEAL AND ALTERNATE DISPUTE RESOLUTION**	Chapter-VIII **PENALTIES AND ADJUDICATION**	Chapter-IX **Miscellaneous**
Appeal to Appellate *(Telecom Disputes Settlement and Appellate Tribunal. (TDSAT)*	**Penalties (Schedule-I)** ₹ 250 crores for failure to prevent breach ₹ 200 crores for failure to report Breach ₹ 150-200 crores for failure to fulfil obligations ₹ 50 crores for failure to comply with any provision of this Act.	Protection of action taken in good faith.
		Power (of the central Govt) to call for information.
Orders passed by Tribunal to be executable as decree of a Civil Court		**Power of Central Government to issue directions.**
		Consistency with other laws.
Alternate dispute resolution.		Bar of jurisdiction.
Voluntary undertaking		Power to make rules/ laying of Rules/Amend Schedule
	₹ 10 K for Breach in observance of the duties by Data Principal	**Amendments to certain Acts**

Applicability of DPDP Act for Judicial / Quasi Judicial functions

- Such bodies are likely to be the the data Fiduciary in the context of the law.
- The general petitioner and respondents (as individuals) are the data principals.
- Formal notice and consent need not be obtained, as the functions covered under the legitimate use cases and also exempt under section



Commencement of the Act has already begun!

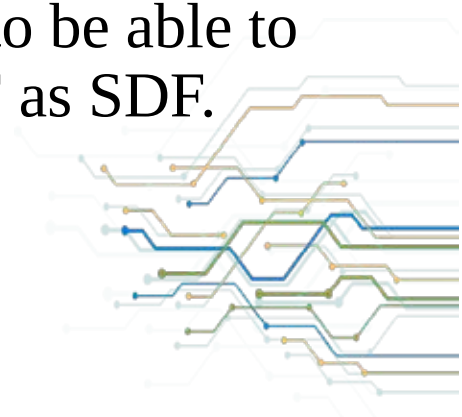
- The law is (generally) non-prescriptive and requires Rules and other related Notifications for making it operational..
- The DPDP Rules published on 13th Nov., 2025. In all 23 Rules have been published
  - Rules 1, 2 and 17 to 21 (Mainly **Regarding Constitution and functioning of the DPBI**): **Effective immediately** from the date of publication of the Gazette.
  - Rule 4 (**Consent Manager** registration): Effective 1 year after publication i.e 13 November 2026
  - Rules 3, 5 to 16, 22 and 23: Regarding DP rights and obligations of DFs. Effective 18 months after publication i.e. 13 May 2027
- The DPBI though digital by design, is being setup with office in NCR.
- The onus is the Organization to prove that have complied with Act. (Principle of Onus)
- The Section 43A of the IT Act and the SPDI Rules, which govern security of sensitive personal data as of today, shall stand withdrawn w.e.f. 13th May, 2027.

Other likely Notifications in near future

- Notification of SDF, Start-up data fiduciaries, Exempt Govt organizations and their Nodal Officers. There can be multiple notifications at different times.

- On Cross Border data flow restrictions:
  - In respect of SDF: The “Committee” comprising of Executives from MeitY and other Central Govt Ministries etc.
  - In respect of all DFs: The Central Government may also issue general or specific orders.

- Notification designating a suitable officer from MeitY to be able to seek information of the purposes of assessment of a DF as SDF. (Based on Rule 23)



Rights and Duties of the Data Principals

Right to access information about personal data.
Right to correction and erasure of personal data
Right of grievance redressal
Right to nominate

Duties of Data Principal

Obligations of data Fiduciary

Including

Additional Obligations of Significant data Fiduciaries

Exemptions for Small/ MSME Data Fiduciaries

Exemptions and Obligations of Government Organisations

Exemptions and Obligations of R&D Organs

OBLIGATIONS OF DATA FIDUCIARY UNDER THE ACT/ Rules

Notice & Consent

- Issue notice to obtain valid consent from data principal in the language of her choice
- Consent can be effectuated via Consent Managers
- Cease and cause Data Processor(s) to cease processing in case consent is withdrawn

Completeness & accuracy

- When processing data influences decisions affecting the Data Principal
- Fiduciary shall ensure completeness, accuracy and consistency
- Including any activity undertaken by Data Processor

Security Safeguards

- Protect data in its possession or under its control
- Take reasonable security safeguards to prevent data breach

Erasure of Data/ Grievance Redressal

- Publish Grievance redressal mechanism on every notice, communication and on its website/ app.
- Erase personal data upon withdrawal of consent/specified purpose is met.
- Unless retention is necessary for compliance with any law

OBLIGATIONS OF DATA FIDUCIARY UNDER THE ACT

Data Breach

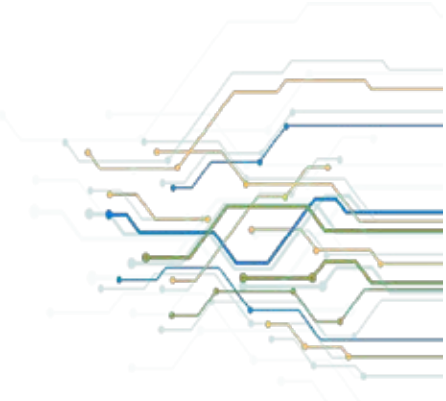
- Intimate the Board and Data Principal of such breach
- Establish an effective mechanism to redress grievances

Compliance

- Shall be responsible for complying with the Act
- Including any activity undertaken by Data Processor

Security Requirements in DPDP Act

- Have reasonable Security Safeguards to protect personal data in its possession or under its control, including in respect of any processing undertaken by it or on its behalf by a Data Processor and to prevent personal data breach.
- Implement appropriate **technical and organizational measures**
  - Maintaining the integrity of Records and Integrity.
  - Ensuring the Records to be stored and retained as required by the laws.
  - Reporting of Data Breach to the DPO for onward reporting to Board
- Have reasonable security measures like encryption, access control, obfuscation, masking or use of virtual tokens.
- Ensure appropriate terms and conditions in the contract with Data Processors.

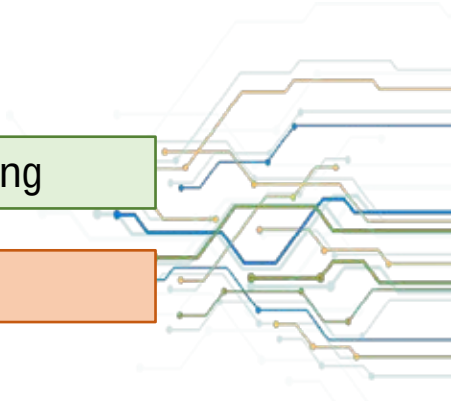


Penalties

- Max. ₹ 250 crores for each instance of Breach of Act.
  - Max. ₹ 250 crores for failure to prevent breach of personal data.
  - Max. ₹ 200 crores for failure to report to Data Protection Board or the DPs.
  - Max. ₹ 150 crores for failure to fulfil obligations as mandated for SDF.
  - Max. ₹ 50 crores for failure to comply with any provision of this Act.
- Provision for doubling the penalties, subject to notification

The Act also provides a opportunity to the DF to provide a Voluntary Undertaking

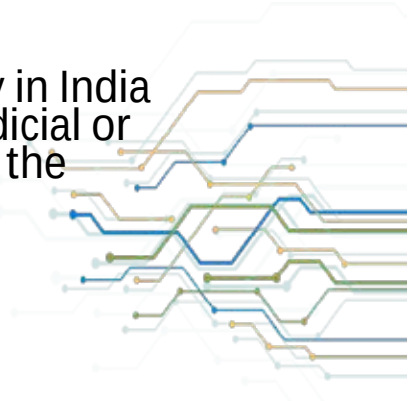
The Act also provides a penalty of upto ₹ 10, 000 to the data Principal.



Legitimate Use cases and Exemptions

- Legitimate use cases:
- Section 7(c):
  - for the performance by the State or any of its instrumentalities of any function under any law for the time being in force in India or in the interest of sovereignty and integrity of India or security of the State;
- Section 7((e):
  - for compliance with any judgment or decree or order issued under any law for the time being in force in India, or any judgment or order relating to claims of a contractual or civil nature under any law for the time being in force outside India;

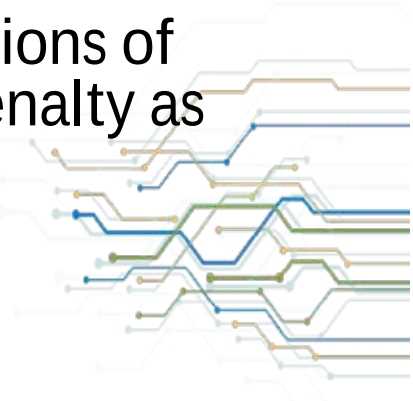
- Exemptions
- Section 17(1)(a):
  - the processing of personal data is necessary for enforcing any legal right or claim.
- Section 17(1)(b) :
  - the processing of personal data by any court or tribunal or any other body in India which is entrusted by law with the performance of any judicial or quasi-judicial or regulatory or supervisory function, where such processing is necessary for the performance of such function;



Bar on Jurisdiction

- **Section 39 of the DPDP Act reads as:**
  - **39.** No civil court shall have the jurisdiction to entertain any suit or proceeding in respect of any matter for which the Board is empowered under the provisions of this Act and no injunction shall be granted by any court or other authority in respect of any action aken or to be taken in pursuance of any power under the provisions of this Act.

- However, Whether courts can direct the DPBI for conducting an inquiry.
  - Yes.
  - The DPBI will have to act in compliance of the directions of any court, to inquire into such breach and impose penalty as provided in this Act;



Thank you

Rakesh Maheshwari
Formerly Sr. Director and GC, Cyber Law & Data governance
Ministry of Electronics and Information Technology (MeitY)
rakeshmaheshwari@gmail.com