

DIGITAL PERSONAL DATA PROTECTION ACT, 2023

BACKGROUND

- Central government enactment – August 2023.
- Puttaswamy case (2017) – right to privacy is a fundamental right.
- Previous versions:
 - Personal Data Protection Bill, 2018
 - Personal Data Protection Bill, 2019
 - Digital Personal Data Protection Bill, 2022
- Intent of the Act – To protect the personal data; to process data safely.
- Not yet been notified – so the Act is not applicable until the govt. notifies it.

LONG TITLE

- *An Act to provide for the processing of digital personal data in a manner that recognises both the right of individuals to protect their personal data and the need to process personal data for lawful purposes and for matters connected therewith or incidental thereto.*

IMPORTANT TERMS

- **Personal data** – data about an individual who is identifiable by or in relation to the data.
- **Digital personal data** – personal data in digital form.
- **Persons** – not just individuals but also companies, firms, governments, etc.
- **Data principal** – individual to who the personal data relates (guardian/parents – minors; guardian - PWDs).
- **Data fiduciary** – person(s) determining the purpose and means of processing the data.
- **Data processor** – person processing the data on behalf of data fiduciary.
- **Significant data fiduciary** – declared so by the central govt.

IMPORTANT TERMS

- **Processing** – 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.
- **Personal data breach** – any unauthorised processing 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.
- **Digital data** – (i) data collected digitally; (ii) data collected non-digitally and digitised subsequently.
- **Lawful purpose** – not forbidden by law.

APPLICATION OF THE ACT

- Processing of personal data inside India.
- 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.
- **Not does apply** where the data is processed by an **individual for personal or domestic purpose**.
- **Not does apply** to **publicly available** data – (i) by the Principal or (ii) by another person obligated by law to do so.

DATA PROCESSING

Notice + Request to Data Principal for consent to process data



Data Principal gives consent



Data Fiduciary may process the said data

NOTICE

- Personal data
- Purpose
- Rights available – withdrawal rights and others.
- Grievance redressal mechanism
- Manner of complaint to Data Protection Board.
- Plain and clear.
- English or any other language.

CONSENT

- Free
- Specific
- Informed
- Unconditional
- Unambiguous
- Withdrawable.
- Consent Manager - give, manage, review or withdraw her consent.

LEGITIMATE USE

Used for:

- Purpose consented to.
- Purpose not indicated as not consented to.
- The State and any of its instrumentalities to provide or issue to the Data Principal such subsidy, benefit, service, certificate, licence or permit.
- Sovereign function of State.
- Responding to medical emergency.
- For compliance with judgment or order or decree.

LEGITIMATE USE

- For fulfilling obligation under law.
- For taking measures to provide medical treatment to an individual during epidemic.
- For taking measures to ensure safety, provide assistance to individual during disaster.
- For the purpose of employment - prevention of corporate espionage, maintenance of confidentiality of trade secrets, intellectual property, classified information.

DUTIES OF DATA FIDUCIARY

- Ensure accuracy, completeness and consistency – (i) when sharing and (ii) when making a decision which affects the DP.
- Data Processor will be engaged only under a valid contract.
- To take reasonable security safeguards to prevent personal data breach.
- Erase data when consent is withdrawn by the DP.
- To intimate about any breach to DP.
- Set up an effective grievance redressal mechanism.
- Data Protection Officer or any person on DF's behalf to answer the questions of the DP.

RIGHTS OF DATA PRINCIPAL

- Right to access information about personal data:
 - Summary of the personal data.
 - Identities of all other DF and Data Processors with whom shared.
 - Exception – sharing to DF authorised by law – request made in writing - for the purpose of prevention or detection or investigation of offences or cyber incidents, or for prosecution or punishment of offences.
- Right to correction and erasure of personal data
 - Request to DF for correction, completion or updating.
- Right to grievance redressal.
- Right to nominate – nominee to exercise rights of DP in the event of death or incapacity.

DUTIES OF DATA PRINCIPAL

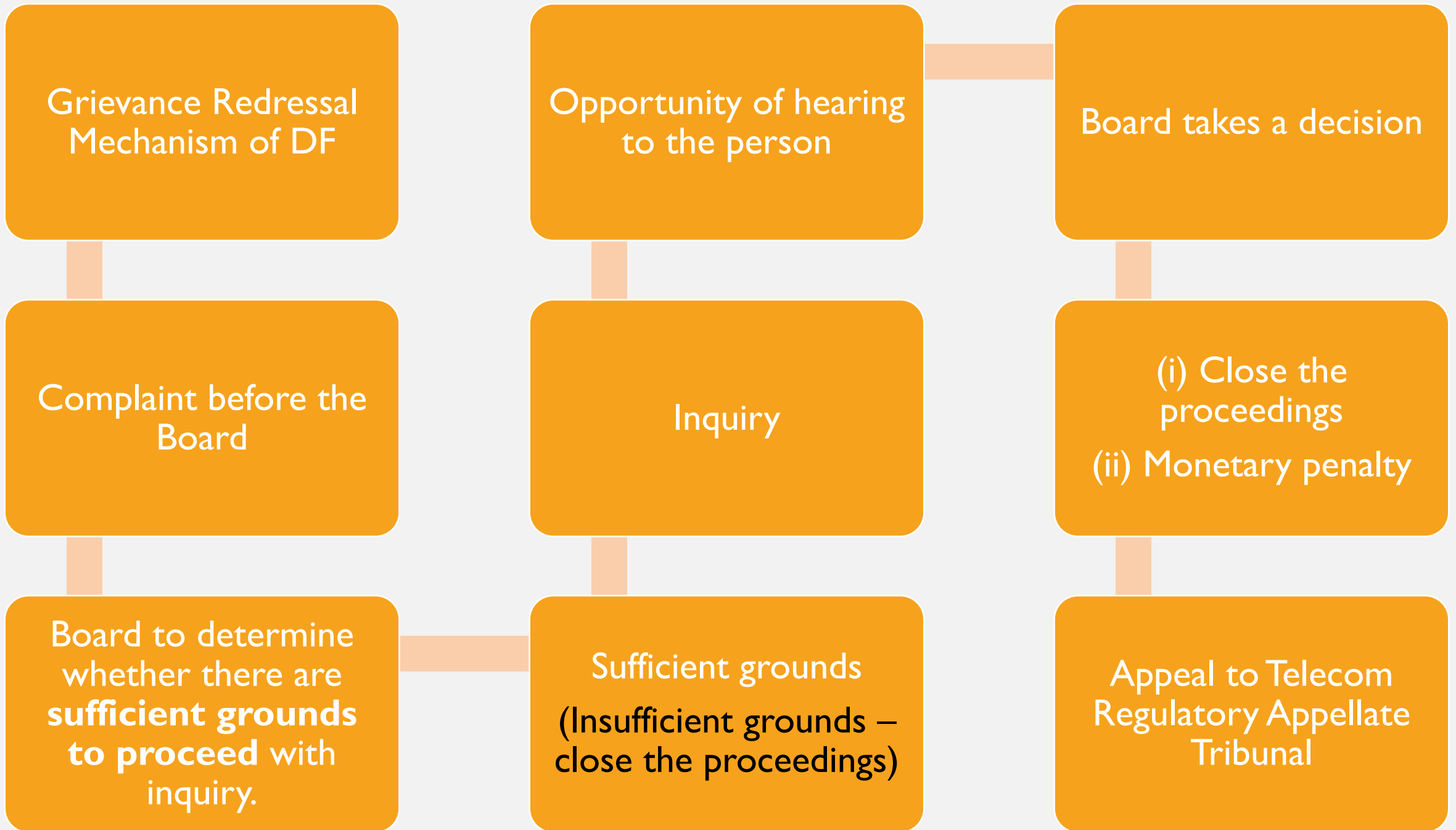
- Ensure not to impersonate another.
- Not to suppress any material information.
- Not to raise any false or frivolous complaints.
- While exercising the right to erasure – provide only verifiably authentic information.

PERSONAL DATA OF CHILDREN AND PWDs

- Consent of parent/guardian necessary.
- No processing of personal data that is detrimental to the well-being of a child.
- No tracking or behavioural monitoring of children.
- No targeted advertisement directed at children.

DATA PROTECTION BOARD

- DP must first go for the grievance redressal mechanism of the DF.
- Independent body.
- Digital office as far as possible.
- In case of data breach – (i) urgent remedial or mitigation measures, (ii) inquiry, (iii) penalty.
- On receipt of complaint – (i) inquiry and (ii) penalty.
- Board may recommend mediation.
- Appeal from the decisions to Telecom Appellate Tribunal.



Grievance Redressal Mechanism of DF

Complaint before the Board

Board to determine whether there are **sufficient grounds to proceed with inquiry.**

Opportunity of hearing to the person

Inquiry

Sufficient grounds
(Insufficient grounds – close the proceedings)

Board takes a decision

(i) Close the proceedings
(ii) Monetary penalty

Appeal to Telecom Regulatory Appellate Tribunal

EXCEPTIONS

- Necessary for enforcing legal right or claim.
- Necessary for judicial, quasi-judicial, supervisory or regulatory function by an court or tribunal.
- For the prevention, detection, investigation or prosecution of any offence or contravention of any law
- Contract between a person outside India and another based in India about a DP outside India.
- For amalgamation or merger of companies, etc.
- For ascertaining the financial information of person who defaulted a loan, etc.

EXCEPTIONS

- Necessary for **research, archiving or statistical** purposes if the personal data is **not to be used** to take any **decision specific to a Data Principal**.
- In the interests of **sovereignty and integrity of India**, security of the State, friendly relations with foreign States, maintenance of public order or preventing incitement to any cognizable offence relating to any of these.

40. (1) The Central Government may, by notification, and subject to the condition of previous publication, make rules not inconsistent with the provisions of this Act, to carry out the purposes of this Act.

(2) In particular and without prejudice to the generality of the foregoing power, such rules may provide for all or any of the following matters, namely:—

(a) the manner in which the notice given by the Data Fiduciary to a Data Principal shall inform her, under sub-section (1) of section 5;

(b) the manner in which the notice given by the Data Fiduciary to a Data Principal shall inform her, under sub-section (2) of section 5;

(c) the manner of accountability and the obligations of Consent Manager under sub-section (8) of section 6;

(d) the manner of registration of Consent Manager and the conditions relating thereto, under sub-section (9) of section 6;

(e) the subsidy, benefit, service, certificate, licence or permit for the provision or issuance of which, personal data may be processed under clause (b) of section 7;

(f) the form and manner of intimation of personal data breach to the Board under sub-section (6) of section 8;

(g) the time period for the specified purpose to be deemed as no longer being served, under sub-section (8) of section 8;

(h) the manner of publishing the business contact information of a Data Protection Officer under sub-section (9) of section 8;

(i) the manner of obtaining verifiable consent under sub-section (1) of section 9;

(j) the classes of Data Fiduciaries, the purposes of processing of personal data of a child and the conditions relating thereto, under sub-section (4) of section 9;

(k) the other matters comprising the process of Data Protection Impact Assessment under sub-clause (i) of clause (c) of sub-section (2) of section 10;

(l) the other measures that the Significant Data Fiduciary shall undertake under sub-clause (iii) of clause (c) of sub-section (2) of section 10;

(m) the manner in which a Data Principal shall make a request to the Data Fiduciary to obtain information and any other information related to the personal data of such Data Principal and its processing, under sub-section (1) of section 11;

(n) the manner in which a Data Principal shall make a request to the Data Fiduciary for erasure of her personal data under sub-section (3) of section 12;

(o) the period within which the Data Fiduciary shall respond to any grievances under sub-section (2) of section 13;

(p) the manner of nomination of any other individual by the Data Principal under sub-section (1) of section 14;

(q) the standards for processing the personal data for exemption under clause (b) of sub-section (2) of section 17;

(r) the manner of appointment of the Chairperson and other Members of the Board under sub-section (2) of section 19;

(s) the salary, allowances and other terms and conditions of services of the Chairperson and other Members of the Board under sub-section (1) of section 20;

(t) the manner of authentication of orders, directions and instruments under sub-section (1) of section 23;

(u) the terms and conditions of appointment and service of officers and employees of the Board under section 24;

(v) the techno-legal measures to be adopted by the Board under sub-section (1) of section 28;

(w) the other matters under clause (d) of sub-section (7) of section 28;

(x) the form, manner and fee for filing an appeal under sub-section (2) of section 29;

(y) the procedure for dealing an appeal under sub-section (8) of section 29;

(z) any other matter which is to be or may be prescribed or in respect of which provision may be, made by rules.

COMPARISON

SPDI RULES

DPDP ACT

Responsibility	Body corporates	Data Fiduciary – any person
Grievance redressal	Grievance Officer	Data Fiduciary/Consent Manager/Data Protection Officer – to answer questions/ Board
Collection	No such mention	digital or non-digital digitised subsequently
Format	Simple rules alone	Illustrations
Applicability	Prospective effect	Retrospective effect
Process data	More clear about purpose	“Certain legitimate uses”
Notice	Reasonable steps to ensure	Notice for consent

SPDI RULES

DPDP ACT

Children	No specific protection	Special provision
Duties of Data Principal	No duty	S. 15 lays down duties
Exemption	Very few	Many exemptions
Board	No such instrumentality	Data Protection Board – digital office
Assign	No such provision	Consent Manager/ Nominee
Accuracy	No obligation on body corporate	Data Fiduciary is responsible at times