P | L | R
CHAMBERS
advocates & solicitors

Digital Personal Data Protection Act, 2023

Brief History

- 2017 landmark SC judgement (*K.S. Puttaswamy vs Union of India*) recognised **privacy as a fundamental right** in India.
- First iteration of the law (Draft Personal Data Protection Bill, 2018) made by the Justice BN Srikrishna Committee.
- Three more iterations of the draft bill - released for public consultations in 2018, 2019 and 2022.
- The fifth iteration was introduced and passed by the Parliament as the Digital Personal Data Protection Bill, 2023 ("**DPDP Act**").

Timeline of DPDP Act

Applicability

- Applies to the processing of digital personal data in India collected in:

01 digital form

02 non-digitized format and subsequently digitized

- Also applies to data processed outside in connection with any activity relating to the **offering of goods and services to individuals within India**.

- Does not apply to personal data that has been **made publicly available** either (a) by the individual to whom it relates, or (b) by a third party as required by law.

DEFINITIONS

Key Definitions

- **Data**: Representation of information, facts, concepts, opinions or instructions suitable for communication or processing by humans or automated means.
- **Personal Data ("PD")**: Any data about an individual who is identifiable by or in relation to such data.
- **Digital Personal Data**: PD in digital form (collected in digital form or digitized subsequently).
- **Data Fiduciary ("DF")** - any person who alone or in conjunction with other persons determines the purpose and means of processing of PD.
- **Data Principal ("DP")** - individual to whom the PD relates. In case of a child/person with disability, the term includes the parent or lawful guardian of the child.
- **Processing** - means a wholly or partly automated operation – on digital personal data – includes 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.
- **Data Processor** - any person who processes PD on behalf of a data fiduciary

OBLIGATIONS

General Obligations (1/2)

- **Baseline Compliance** – The DF has to comply with its obligations such as notice, consent etc. regardless of whether the DP has adhered to its duties.
- **Integrity of PD:** Take reasonable efforts to ensure that the PD is accurate and complete if it is likely to be used by the DF to make a decision that affects the DP or is likely to be disclosed to another DF.
- **Technical & Organizational Measures:** Implement appropriate technical and organizational measures to comply.
- **Security of PD:** Protect PD under its possession or control & implement reasonable security safeguards to prevent personal data breach.

General Obligations (2/2)

- **Grievance Redressal:**
  - Publish contact details of a person to answer questions from a DP.
  - Have effective grievance redressal mechanism.

- **Data retention:** Delete PD upon withdrawal of consent or as soon as it is reasonable to assume that the purpose is fulfilled (whichever is earlier).

Note: ***The central government has the power to exempt certain data fiduciaries, or classes of data fiduciaries, from various provisions of the Act (eg.- notice, general obligations, rights of DP) based on the volume and nature of data they process.***

Impact:

- Companies will need to assess its internal data processing practices and policies to ensure that the same is aligned with the requirements under this Act.
- The data retention policy must be periodically reviewed to determine the necessity for retention.
- All PD that does not need to be retained must be deleted.

Notice

- Notice to be provided to the DP.
- Should be in clear and plain language.
- Must give option to access the contents in English or any of the 22 languages specified in the 8th Schedule of the Constitution of India.
- Notice must contain following:
  - description of the PD sought to be collected and the purpose for its processing.
  - manner in which the DP may exercise her right to withdraw consent and to grievance redressal.
  - manner in which the DP may make a complaint to the Data Protection Board ("**Board**").
  - Manner in which this is to exercised to be prescribed
- For existing consent from a DP, notice to be given **as soon as it is reasonably practicable** after the DPDP Act becomes enforceable. Manner in which this is to exercised to be prescribed.

Impact:

- Reviewing existing notice mechanisms.
- Ensuring the notice is available in English and 22 Indian languages.
- Content of notice to be aligned with the DPDP Act.
- For existing users, notice to be given again with disclosures as per the DPDP Act.

Consent (1/2)

- Consent obtained should be:
  - **Free, specific, informed, unconditional and unambiguous.**
  - For the purpose disclosed in the notice and be limited to PD necessary for the **specified purpose.**
  - **Obtained along with notice before collection of PD.**
  - **Request to be clear and plain language.**
  - **Request to** contain the contact details of person authorised to respond to DP (Data Protection Officer in case of Significant Data Fiduciary).
- Process of withdrawal of consent to be as easy as the process to obtain consent.
- Upon withdrawal, DF to cease processing within reasonable time unless required/authorised under law.
- Burden of proof w.r.t. obtaining consent on DF.
- Consent may be managed by Consent Managers ("**CM**")
  - CM to provide DP with an accessible, transparent and interoperable platform to make decisions about their consent.

Impact:

- Reviewing existing consent obtaining processes
- Provide a consent withdrawal mechanism and record the reasons of such withdrawal of consent. Once withdrawn, Companies to abstain from processing.
- Enable/integrate CMs to manage consent on behalf of DP.
- For child (Below 18) DP or DP with incapacity, ensure consent of parent/guardians is obtained.

Consent (2/2) – Legitimate Use/Exemptions

No consent is necessary for processing PD in the following instances:

- Where a DP voluntarily provides PD to a DF.
- Where a DF will be acting on behalf of the State:
  - provision of any service or benefit to DP by the State,
  - issuance of any government documents,
  - performance of function under law or in the interest of sovereignty and integrity of India or,
  - security of state,
- For fulfilling any obligation under law w.r.t. disclosing information to State or its instrumentalities.
- Compliance with court order.
- Medical emergency.
- Employment related processing.
- Natural disaster, epidemic, threat to public health.
- Breakdown of public order.
- Merger/Acquisition/other restricting of business.
- Assessing financial position of DP in case of default in loan/advance repayment.
- Processing PD of DP outside of India, by person based in India, pursuant to a contract with a foreign party.

Processing of PD of Children & Person With Disability

- For processing the PD of a child (less than 18 years) /person with disability:
    - Obtain the verifiable consent of the parents or lawful guardians prior to processing.
        - Manner of 'verifiable consent' to be prescribed.
    - Prohibition to process any PD of a child in a manner which may be detrimental to the well-being of the child.
    - No behavioural monitoring or targeting advertisement directed at children.
- Central Government can exempt certain data fiduciaries from complying with these obligations if it is satisfied DF processes PD in a manner that is 'verifibaly safe'.

Impact:

- Additional level of protection for processing PD of children and persons with disability.
- User Accounts to be created only for persons above age of 18.
- Internal policy on monitoring by companies will have to be aligned

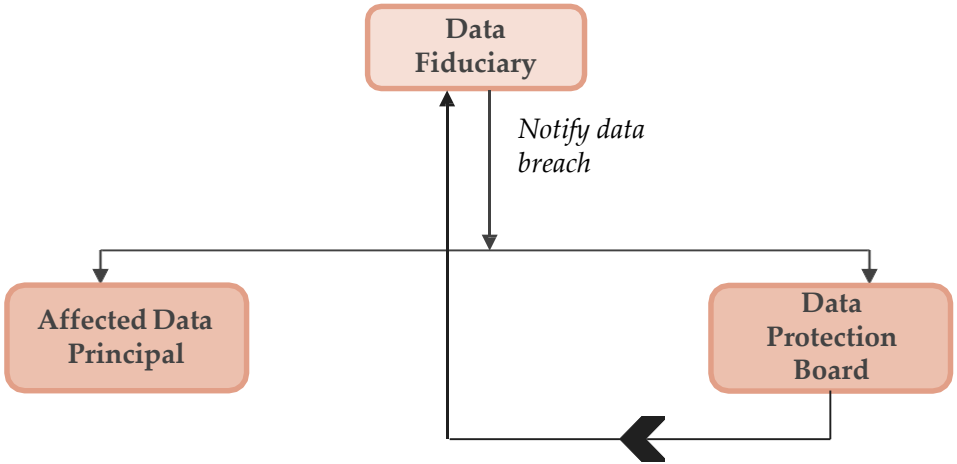
Cross-border transfer of PD

- No blanket prohibition of cross-border transfer of PD.
- Central government to publish list of countries/territories for which transfer is restricted.
- Additional obligation under any other legislation would still apply such as data localisation requirements that have been imposed in relation to payments data, etc.

Impact:

- Companies must review and update policies related to the cross-border transfer of PD and ensure that PD is not transferred to blacklisted countries.
- Companies must be mindful of sector-specific laws on transfer of PD. For instances, financial data cannot be transferred outside India under RBI laws.

Obligations relating to Personal Data Breach



- Compromise the confidentiality, integrity or availability of personal data by -
  - Unauthorised processing.
  - Accidental disclosure.
  - Accidental acquisition.
  - Accidental sharing.
  - Accidental use.
  - Accidental alteration.
  - Accidental destruction/ loss of access.
- DF and data processor to have reasonable security safeguards to prevent personal data breaches

Impact:

- Companies must proactively monitor for all Personal Data breaches.
- Companies must inform Board & DP of all breaches regardless of sensitivity.

Additional Obligations on Significant DF

SDF is DF notified by Central Govt. basis-

- Vol. & sensitivity of PD.
- Risk to rights of the DP.
- Potential impact on the sovereignty and integrity of India & security of the state.
- Risk to electoral democracy.
- Public order.

- Appoint a Data Protection Officer **("DPO")** — based out of India
- Publish DPO contact details on website.
- DPO will report to the Board of Directors.
- DPO- single point of contact for the grievance redressal.
- Appoint an Independent Data Auditor to evaluate the compliance of the SDF with the Act.
- Conduct Data Protection Impact Assessment.

Impact:

- Companies may be categorised as SDF on account of the volume & sensitivity of PD processed.
- If categorised as SDF, companies will need to ensure compliance with the additional obligations indicated above.

RIGHTS & DUTIES OF DP

Rights of Data Principals

- **Right to obtain information from the DF-** A DP has the right to – (i) obtain a summary of PD and details of processing (ii) a list of entities processing PD and the type of PD shared, (iii) any other information as maybe prescribed.

  Exception - Point (ii) and (iii) shall not apply in respect of sharing any PD with other DF, *IF authorized by law for prevention, detection or investigation of a cyber incident or for prosecution or punishment of offences.*

- **Right to ask for correction and erasure -**
  - DF must correct inaccurate or misleading data, complete a DP's incomplete data, update the DPs PD, and erase the PD of the DP that is no longer necessary unless retention is required for a legal purpose.

- **Right to ready and available grievance redressal-**
  - DP has the right to readily available grievance redressal mechanism by a DF or CM.
  - DF or CM must reply within prescribed period.
  - Mandatory to exhaust this remedy before approaching the Board.

- **Right to nominate-** The right of a DP to nominate another person who will be eligible to exercise the DP's right in the event of the DP's death or incapacity.

Duties of Data Principals

- Comply with applicable law while exercising rights under the DPDP Act.
- Not register false or frivolous grievances.
- Not furnish false data or suppress material facts or impersonate another person when applying for any document, service, unique identifier, proof of identity or proof of address.
- Furnish only verifiably authentic information while exercising right to correction and erasure.

Impact of rights & duties of data principals:

- Companies will have to maintain – i) a list of persons with whom the it shares any DP's PD; ii) summary of types of PD being processed and the types of processing being done on any DP's PD.
- Create effective responsive systems and mechanisms to address DP rights requests and grievances in the an effective & timebound manner.
- Adherence to the timelines for responding to requests, existing mechanisms in place needs to be relooked at.

DATA PROTECTION BOARD

Data Protection Board

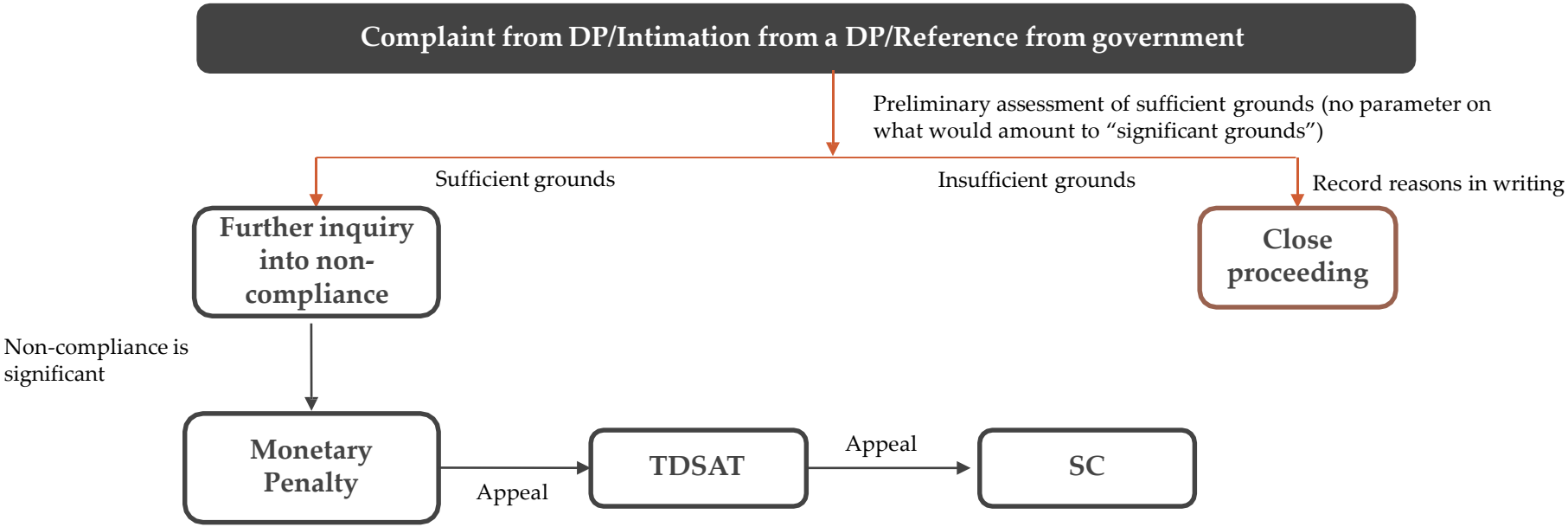
- Board to function as an **independent body**.
- **Powers:**
  - Conduct inquiry
  - Impose penalty
  - Advise the government regarding blocking of information
  - Issue interim orders
  - Powers of civil court
- **Functions:**
  - Inquire into non-compliances upon complaint, intimation or reference by Central Govt.
  - No *suo moto* power
  - Direct DF to adopt urgent, remedial or mitigation measures in case of personal data breaches
  - Issue directions to any person for effective discharge of its functions

- **Flow of appeal:**

Order of the Board >> TDSAT >> Supreme Court (only when substantial question of law involved)

- Civil courts cannot entertain suits or take action under the Act, although certain remedies, such as writs (where applicable) cannot be precluded.

Process of Inquiry & Adjudication



In case of repeat instances of monetary penalty being imposed, in the interest of general public, the Govt. may block an entity upon an advise received from the Board in this regard.

Voluntary Undertaking & Alternate Dispute Resolution

Voluntary Undertaking

- During a proceeding before the Board, for non-compliance, any person can give a voluntary undertaking to undergo all such compliances.
- Once undertaking given – it bars any other proceedings vis-a-vis that case.
- Failure to comply with undertaking attracts penalty.
- Voluntary undertaking may include specified action within a specified time, an undertaking to refrain from taking specified action, and an undertaking to publicize the voluntary undertaking

ADR

- Board can refer for Mediation, Mediator can be agreed upon by the parties

Impact:

- Positive step to include mediation to avoid courts; time and cost effective.
- Voluntary undertaking may be given by an entity in case of any complaint against it before the Board. This bars any other proceedings to be initiated against the entity.

Penalties

The Board, in arriving at the quantum of the penalties, may consider a number of factors such as the **nature, gravity and duration of the contravention, types of personal data affected, implications of the contravention and mitigating measures adopted by the contravening party**.

Non-Compliance	Penalty (in INR)
Failure of Data Processor or Data Fiduciary to take reasonable security safeguards to prevent personal data breach	Up to 250 Cr. (3 Bn USD)
Failure to report data breach	Up to 200 Cr. (2.41 Bn USD)
Processing of PD of child in violation of Bill	Up to 200 Cr (2.41 Bn USD)
Failure on part of SDF to comply with incremental obligations	Up to 150 Cr (1.8 Bn USD)
DP not complying with their duties	Up to 10,000 (120 USD)
Breach of voluntary undertaking accepted by Board	Up to the extent applicable for the breach
Residuary	Up to 50 Cr (60 Mn USD)

Recent Updates

- Digital India Dialogue (20 Sept 2023) with Mr. Rajeev Chandrasekhar (MoS, MeitY)
    - Speedy implementation a priority. The Data Protection Board to be setup at the earliest.
    - Unless key architectural changes or third party collaboration is necessary, DFs must comply within specified timelines.
    - Staggered implementation for government DF, MSMEs, medical institutions, business not fully digital
- Central Govt. doing consultation with Big Tech companies to develop age-gating mechanism.
- Latest news reports state rules for DPDP Act ready. To be released for public consultation mid November. Unlikely to be tabled before Parliament for winter session.

THANK YOU

P | L | R
CHAMBERS
advocates & solicitors

E: suhaan.mukerji@plrchambers.com
Office: Suite 1-B, Plot No. 8-B, Main Mathura Road, New Delhi – 110014