btg::advaya

INDIA BRIEFING: DIGITAL PERSONAL DATA PROTECTION ACT, 2023

NOVEMBER 2023

Privileged & Confidential

Evolution of India's Data Protection Law

2017

Supreme Court of India in a landmark judgment recognises informational privacy as a fundamental right.

2018

Draft Personal Data Protection Bill, 2018 recommended by SriKrishna Committee.

2019

Revised Personal Data Protection Bill, 2019 tabled in Parliament by the Ministry of Electronics and Information Technology ("MeitY) and sent for examination to the Joint Parliamentary Committee.

2022

2019 bill withdrawn after Joint Parliamentary Committee's comments.

On November 18, 2022, MEiTY released a new draft Digital Personal Data Protection Bill, 2022 which was available for public comments until January 2, 2023.

2023

Digital Personal Data Protection Bill, 2023 **("DPDP Bill, 2023")** was tabled before Parliament on August 3, 2023, and was passed in the Lower House on August 7, 2023, and thereafter passed by Upper House on August 9, 2023. The bill has obtained assent from the President and is awaiting implementation. Rules under the DPDPA will be released for public consultation soon with 45 days being allocated for receipt of public comments. MeitY has indicated that 6 months to a year can be treated as the outerlimit for the full implementation of the DPDP ACT, 2023

Principle-Based Approach

MeitY has drafted the DPDP Act, 2023 on the following **7 foundational principles**:

- **Use**: should be lawful, fair, and transparent.
- **Purpose**: Data collected should only be used for the purpose for which it was collected.
- **Minimization**: Only data required for a specific purpose should be collected.
- **Accurate**: The personal data collected should be accurate and updated.
- **Retention**: Personal data be retained for only as long as needed for purpose of collection.
- **Protect**: The personal data should be reasonably safeguarded to prevent personal data breaches, unauthorised collection, or processing of personal data.
- **Accountability**: The person who decides the purpose and means of processing of personal data should be accountable.

Paradigm Shift

In addition to how personal data will be handled from here on out, the new Act also brings with it a paradigm shift in India's digital economy:

- **The creation of an independent Data Protection Board of India**
- **Omission of Section 43A from the IT Act** – the right to claim compensation has been taken away.
- **All personal data will be treated the same.** No categorization of personal data.
- **Introduction of a Consent Manager** – a person/entity registered with the Board who enables a Data Principal to give, review and withdraw their consent *via* a transparent platform.
- The Central Government can call for the **furnishing of information from the Board and any Data Fiduciary or intermediary.**
- **Processing of personal data by a Data Processor** on behalf of a Data Fiduciary is now permitted under a valid contract.
- The Central Government, after giving an opportunity to be heard, can direct the **blocking of the public's access to a Data Fiduciaries platform.**
- **No criminal sanctions have been provided in the new Act.**

Material & Territorial Scope – The What, Who & Where

- **Where:** The DPDP Act, 2023 applies in the main to data processed within India.

  It applies to to personal data *outside* of India only if the processing of *such personal data is in connection with the offering of goods and services to data principals within India.*

- **What:** The DPDP Act, 2023 in its material scope applies to personal data that is collected in digital form and in non-digital form but subsequently digitized. *The DPDP Bill, 2023 has done away with the use of ambiguous words such as "online data" and "offline data" which had been used in the 2022 Bill.*

- **Who:** The DPDP Act, 2023 does not apply to (i) non-digital data; (ii) data processed for personal or domestic purposes; and (iii) data made available by a data principal or any other person under a legal obligation. *The categories of such data have been narrowed down from the 2022 Bill offering much-needed clarity.*

Obligations of Data Fiduciary

- There are substantial obligations placed on data fiduciaries (same as data controllers) under the DPDP Act, 2023. They have to (*inter alia*):

  - *obtain consent for data processing;*
  - *set up grievance redressal mechanism;*
  - *ensure accuracy and completeness of data particularly if such data is shared with third-parties; and*
  - *delete the data of data principals when the data principal has withdrawn consent or if specified purpose is not served.*

- Data Fiduciaries must while obtaining consent from a data principal notify her of *the type of personal data being processed and its accompanying purpose; details of the way data principals may exercise their rights to withdraw consent etc*

- The DPDP Act, 2023 has moved away from the ***deemed consent framing of non-consent-based processing of data.***

- The Act now provides a narrow list of legitimate uses that include **employment purposes, safety measures during disasters**, or e**nforcing judgments or decrees.**

Obligations of Data Fiduciary (Contd.)

- **Some other prominent obligations applicable to Data Fiduciaries:**

  - *Ensuring the completeness, accuracy, and consistency of the processed personal data.*
  - *Implementing technical and organizational measures and reasonable security safeguards to prevent personal data breach.*
  - *Intimating the Data Protection Board in the event of a personal data breach.*
  - *Taking reasonable security safeguards to protect personal data under its control or that which is processed by a Data Processor.*
  - *Erasing all personal data upon withdrawal of consent or when retention has served its purpose and further ensuring that the same is done by the Data Processor.*
  - *Establishing effective grievance redressal mechanisms for Data Principals.*

Special Obligations on Children's Data

- **New restrictions apply on processing data of children.**
- A Data Fiduciary is now additionally responsible for:
  - Obtaining **verifiable** parental consent.
  - In case of processing the personal data of a person with disability, obtaining verifiable consent of lawful guardian.
  - Not undertake processing of data likely to cause any detrimental effect on the child's well-being.
  - Not undertake tracking or behavioural monitoring of children, or targeted advertising directed at children.

1. Your IT systems may need recalibrating to enable verifiable age-gating for access.

2. How and when you store children's data should be denoted in a policy.

3. Have robust processes in place to deal with breaches and anomalies involving children's data.

Obligations of a Significant Data Fiduciary

btg::advaya

- A Data Fiduciary or *Class* of Data Fiduciaries may be notified by the Central Government as Significant Data Fiduciary. They will have the following additional obligations:

  - Appoint a **Data Protection Officer** as point of contact for grievance redressal.
  - Appoint **Independent Data Auditors** to evaluate their compliance.
  - Undertake **periodic data audits.**
  - Undertake periodic **Data Protection Impact Assessment** - a process comprising the description, purpose, assessment and management of risk to the rights of Data Principals.

Significant Data Fiduciaries will be determined based factors such as the *volume and sensitivity of data processed, risk of harm, risk to rights of Data Principal, security of the State, public order*, etc.

Cross Border Transfers

The DPDP Act, 2023 abandons the white-list approach of the 2022 Bill and ***instead adopts a negative list -*** meaning that data can be transferred to all countries except those barred by the Central Government by notification.

Where foreign companies are offering goods/ services to Indian data principals, and in a situation where their incorporation country is a part of the negative-list, then transfer of data to companies in such a country may not be permissible. It could also mean that primary collection of data by companies from negative list countries may not be permissible at all.

No hard localization requirement. No localization/ mirroring by default requirement.

Any localization requirements contained in other sectoral laws or regulations are not affected and will continue.

For example, the Reserve Bank of India has required local storage of payment data since April 2018.

Data Principal's Rights and Duties

Data Principals are provided with the:

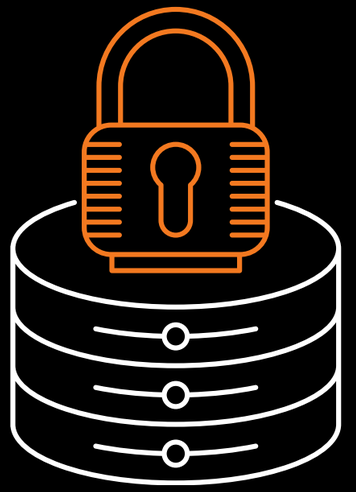
- **Right to information**: to obtain a summary of their personal data processed by the Data Fiduciary, the processing activities carried out, and identities of other Data Fiduciaries with whom their data has been shared.
- **Right to correction and erasure of data.**
- **Right to grievance redressal.**
- **Right to nominate**: Data Principals can nominate an individual to exercise rights on their behalf, in case of death, etc.
- **Right to withdraw consent**: at any time, but without impacting the legality of past-processing activities.

The new law imposes certain duties on Data Principals, including duty to not submit false details, or impersonate another person, to furnish 'verifiably' authentic information, and not file frivolous / false grievances.

Exemptions

- The DPDP Act, 2023 identifies both entities and instances to ***which provisions of Chapters 2 and 3 (except for reasonable security obligations) do not apply***. These include processing data for :

a. Exercising legal rights / claim.
b. Court proceedings, law enforcement agencies, etc.
c. A **foreigner's personal data** by Data Processors in India under a contract with an overseas entity.
d. For merger or amalgamation of 2 or more companies, or reconstruction by way of demerger, etc.
e. For ascertaining the financial information of a person from whom a claim is due on debt owed by them.
f. For prevention, detection, investigation or prosecution of an offence.



Overall exemptions in the Act are provided for:

(a) Data processing done by an instrumentality notified by the Central Govt. in the interest of sovereignty and integrity of India.
(b) Processing data for research, archiving or statistical purposes if the personal data is not to be used to take any decision specific to a Data Principal.

Data Protection Board of India

- The DPDP Act, 2023 envisages the establishment of a ***new Data Protection Board of India*** as an independent body.

- **Composition:**

  - The Board will be composed of a Chairperson and Members who possess special knowledge or practical experience in the fields of data governance and administration, information and communication technology, etc.

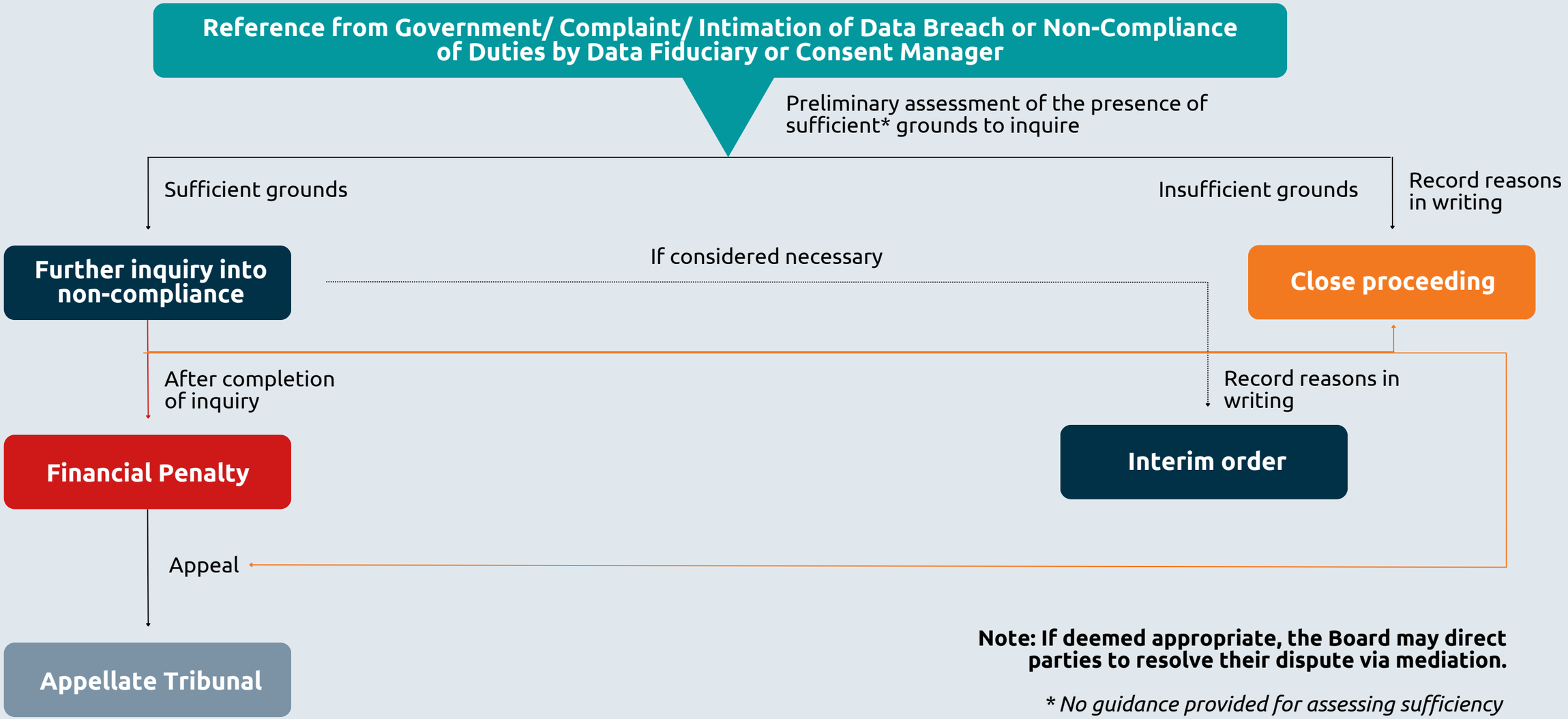
  - One Member will be an expert in the field of law.

  - The Members of the Board will be entirely appointed by the Central Government.

The Data Protection Board of India has the power to :

- Independently enquire into complaints or intimations of breach.
- Impose monetary penalties.

Data Protection Board of India: Inquiry Procedure



Note: If deemed appropriate, the Board may direct parties to resolve their dispute via mediation.

** No guidance provided for assessing sufficiency*

Penalties

Non-Compliance	Penalty (in INR)
Failure of Data Processor or Data Fiduciary to take reasonable security safeguards to prevent personal data breach	Up to Rs. 250 Cr.
Failure to report data breach to the Board	Up to Rs. 200 Cr.
Processing of personal data of child in violation of Bill	Up to Rs. 200 Cr.
Failure on part of Significant Data Fiduciary to comply with incremental obligations	Up to Rs. 150 Cr.
Data Principal not complying with their duties	Up to Rs. 10,000
Breach of any term of voluntary undertaking	Up to amount of breach for which proceedings were instituted
Residuary	Up to Rs. 50 Cr

Factors to be considered while imposing penalty:

- Nature, gravity and duration
- Type and nature of the personal data affected
- Repetitive nature
- Realization of gain or avoidance of any loss
- Mitigation efforts, its timeline and effectiveness
- Likely impact of the financial penalty

What Should Businesses Do Next?

btg::advaya

Step 1: Baseline Applicability

- Identify if you process any data on behalf of your Indian entity or business, for e.g., human resources, procurement, etc.
- Determine if you already comply with GDPR/CCPA or equivalent law.

Step 2: Initial Assessment

- Conduct DPDP assessments on the flow and life cycle of your data, i.e., collection points, where its stored, retention periods, etc.
- A questionnaire based approach will help you think through all “pain points” they can foresee.

Step 3: Gap Analysis

- Identify prioritize gaps (by colour coding them) based on how significant they are to your current business operations.
- Track long-lead items to be drafted from scratch, e.g., age-gating policies.

Step 4: Develop and Execute a Plan

- Embed your privacy compliance plan within your organization.
- Appoint local champions, assign timelines, track progress, and revisit the plan periodically.

Have Questions?

btg advaya

www.btgadvaya.com

Vikram Jeet Singh
Partner
vikram.singh@btgadvaya.com

Kalindhi Bhatia
Principal Associate
kalindhi.bhatia@btgadvaya.com

Ayan Sharma
Head - Policy and Advocacy
ayan.sharma@btgadvaya.com

Thank you!

Mumbai
2nd Floor, Hague Building,
SS Ram Gulam Marg,
Ballard Estate, Fort,
Mumbai, Maharashtra
400001

Delhi
C Block, 242,
Defence Colony,
New Delhi
110024

Begaluru
5/8, Brunton Cross Road,
Off Magrath Road,
Bengaluru, Karnataka
560 025

www.btgadvaya.com

For more information about **BTG Advaya**, the partners and their qualifications, see www.btgadvaya.com