PRIMUS PARTNERS

Digital Personal Data Protection (DPDP)

Summary of the 2023 Bill

Date: 04 August 2023

Background

The Digital Personal Data Protection Bill 2023 was introduced in the Lok Sabha on 3rd August 2023 as an Ordinary Bill. The bill aims to enforce a lawful usage of online personal data (referred as PD in places), echoing the core principles that underpin digital personal data protection laws in various jurisdictions. This bill outlines the obligations for organizations and individuals who handle digital personal data and stipulates how they should navigate privacy rights. The Bill will come into force after it is passed by both the houses of the Parliament and thereafter receives assent of the President. It is important to note that the Law will not apply to personal data made or caused to be made publicly available by the user (for example, if an individual, while blogging her views, has publicly made available her personal data on social media, then processing of that data won't come under these regulations).

Key Definitions

- "Data Fiduciary" means any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data.
- "Significant Data Fiduciary" means any Data Fiduciary or class of Data Fiduciaries as may be notified by the Central Government based on the following factors: the volume and sensitivity of personal data processed, risk to the rights of Data Principal, potential impact on the sovereignty and integrity of India, risk to electoral democracy, security of the State; and public order.
- "Data Principal" means the individual to whom the personal data relates.
- "Data Processor" means any person who processes personal data on behalf of a Data Fiduciary.
- "Digital personal data" means personal data in digital form.
- "Personal data" means any data about an individual who is identifiable by or in relation to such data (where "person" might mean an individual, company, the state or an association).
- "Data Protection Officer" means an individual appointed by the Significant Data Fiduciary to represent it under the provisions of this Act; responsible to the Board of Directors or similar governing body of the Significant Data Fiduciary; and be the point of contact for the grievance redressal mechanism under the provisions of this Act.

Obligations of Data Fiduciary

- Obtain Consent - Data fiduciaries, which are entities collecting and processing personal data, are required to obtain free, informed, and unconditional consent from individuals before processing their data.
- Informed Consent - Requests must be communicated in clear and plain language, and the withdrawal process should be as easy as giving consent.
- Collection and Purpose of Data - Data fiduciaries must inform individuals about the data being collected and the purpose of collecting it.
- Consent Withdrawal - Data Fiduciaries will have to erase the personal data once the user withdraws their consent, or if the data is no longer required for the specified use. Data fiduciaries will have a certain period of buffer time given before they stop using or processing user data.
- Consent Manager - The Data Principal may give, manage, review or withdraw her consent to the Data Fiduciary through a Consent Manager. The Consent Manager shall be accountable to the Data Principal and shall act on her behalf in, and subject to such obligations as may be prescribed.
- Grievance Redressal Mechanism – Data Fiduciaries will have to form an "effective mechanism" to redress the grievances of users.
- Proof of burden lies with the Data Fiduciary: If challenged in the courts, Data Fiduciaries will have to

prove that a notice was given, and consent was obtained to carry out the processing of personal data.

- Obligation to Report Data Breaches - Data fiduciaries must report data breaches – which retains its broad definition from the 2022 Bill – to both the DPB and users. The liability for not reporting breaches or failing to institute safeguards falls on data fiduciaries only (and not data processors).
- Contract with Data Processors - Data fiduciaries will need to have a valid contract for engaging with data processors.
- Data Protection Officer or similar: Data Fiduciaries will be required to publish the business contact information of a Data Protection Officer or a person who can answer questions that a user might have about the processing of their personal data.

Processing Data without Consent or Exemptions

Data can be processed without consent in certain "legitimate" cases, such as -

- ➢ State providing benefits and services.
- ➢ State claiming data in the interest of sovereignty and integrity of India, or in situations of legal obligations or for health emergencies.
- ➢ Users voluntarily provide their personal data to the Data Fiduciary (including private) for a specified purpose.

The law may also provide exemptions for research, archiving or statistical purposes – if the data is not used to take any decision specific to a data principal.

The Central Government may also notify certain data fiduciaries (or classes of data fiduciaries), including start-ups, as exempt from certain provisions of the law. Further, within 5 years from commencement of the law, it may notify any provision(s) that will not apply to certain data fiduciaries (or classes of data fiduciaries) for a specified period.

Additional Obligations for Significant Data Fiduciaries (SDFs)

The government may notify 'significant data fiduciaries' (SDFs) by assessing factors like:

- ✓ Volume and sensitivity of the personal data processed.
- ✓ Risk to the rights of the data principals (this was previously harm to DPs)
- ✓ Potential impact on the sovereignty and integrity of India,
- ✓ Risk to electoral democracy, security of the State; and public order.

The 2022 Bill allowed the government to also consider 'other factors', but this has been removed.

SDFs are obligated to:

1. Appoint a designated Data Protection Officer (DPO) based in India who will be responsible to the board of directors of the SDF.
2. Appoint an independent data auditor to evaluate the SDF's compliance with the Bill.
3. Undertake data protection impact assessments (DPIA) and periodic audits, as may be prescribed under rules.
4. Other measures "as may be prescribed" later.

Processing Personal Data of Children

The DPDP Bill 2023 continues to define a 'child' as an individual who has not completed 18 years of age. The law envisions following obligations for data fiduciaries with respect to personal data of children or person with

disability with a legal guardian -

- Data fiduciaries involved in processing PD belonging to a child or a person with disability with a legal guardian (new to DPDP 2023) are required to obtain verifiable parental or guardian consent prior to processing such PD.
- Data fiduciaries are barred from tracking or behaviourally monitoring children or directing targeted advertising at them.

The Government can exempt certain data fiduciaries from the above obligations with some conditions. The Government can also decide to exempt data fiduciaries from these obligations by notifying a different age cap, if they are satisfied that the data is handled in a 'verifiably safe' way.

Cross Border Data Transfers

The Bill moves from the white-list approach (recommended in the 2022 Bill) to a negative list. This means that data transfers are allowed to all jurisdictions except those barred by the government through notification. The principles/conditions under which such countries will be barred are not specified yet. Any stricter sectoral restrictions on data transfers – like the Reserve Bank of India's payments data localization mandate or MeitY 2017 Guidelines of localisation of state data (to be read with the fact that "state" comes under the definition of "person" in DPDP 2023) – will continue to apply.

Data Principal (User) Rights

Key rights (except for the right to data portability) that were available to data principals under previous iterations of the DPDP Bill 2023 have been retained. For example, data principals have the right to:

- ✓ Access information about their PD processed by a data fiduciary to whom consent has been given or where consent is assumed.
- ✓ Seek correction, completion, updation, or erasure (under certain circumstances) of PD; and
- ✓ Avail grievance redressal within timelines to be prescribed by the Central Government, including escalating complaints to the Board. Few of these rights may be limited in certain instances of processing on the grounds of 'legitimate use'.

Data Protection Board

The Board's functions include: (a) inquiring into PD breaches and directing urgent remedial or mitigation measures in such cases; (b) inquiring into and imposing penalties in case of a person's non-compliance with the law; and (c) issuing binding directions to any person for the effective discharge of its functions under the law. The Board, however, does not have the power to enact subordinate legislation under the DPDP Bill 2023.

The DPDP Bill 2023 contains a detailed mechanism on appeals. Persons who are aggrieved by any order or direction passed by the Board may file an appeal before the Telecom Disputes Settlement and Appellate Tribunal, and thereafter to the Supreme Court within specific timelines. (This provision is new to the DPDP Bill 2023).

The Bill also details out the composition of the Board, which will encompass a Chairperson and Members, the number of which will be specified separately by the Government.

The Chairperson and other Members shall be a person of ability, integrity and standing who possesses special knowledge or practical experience in the fields of data governance, administration or implementation of laws related to social or consumer protection, dispute resolution, information and communication technology, digital economy, law, regulation or techno-regulation, or in any other field which in the opinion of the Central Government may be useful to the Board, and at least one among them shall be an expert in the field of law.

Blocking or Call for Information Directives by the Central Government

In addition to the aforementioned powers, the Central Government can direct the Board or any intermediary (as defined under the Information Technology Act, 2000) to, for the purposes of the law, furnish any information to it. The Central Government can also issue a blocking order to a Government agency or intermediary to, in public interests, prevent a data fiduciary from offering goods or services to data principals within India, upon receiving a reference from the Board. Both these powers of the Central Government are new to the DPDP Bill 2023.

Penalties

The DPDB can issue monetary penalties to data fiduciaries in case of non-compliance. Penalties are only applicable to data fiduciaries, which is a departure from the 2022 Bill. The maximum penalty that can be issued is INR 250 crore. In the 2022 Bill, the DPB could have levied a maximum penalty of INR 500 crore. The government has the power to amend the schedule to increase the penalties but cannot increase to more than double of the existing figures.

Additional Provisions

Change in RTI Act: The DPDP Bill, 2023, amends Section 8(1)(j) of the RTI Act to state that "the Indian state is not obliged to disclose information which relates to personal information," essentially removing the power of the Public Information Officer or an appellate authority to override this, thus diluting to the power of citizens to seek information under the RTI Act.

Power to remove any difficulties: If any difficulty arises in giving effect to the provisions of this Act, the Bill allows the government to, within 3 years of the Act going into effect, issue an order to add provisions to the Act to remove the difficulties as long as the new provisions are not inconsistent with the existing provisions of the Act. Any such changes must be presented to the parliament.

--x--

A Quick Preview: What the Bill Means for Tech Companies or Entities Processing Personal Data?

Such companies will be required to present a notice to users and seek consent before processing any personal data, maintain the accuracy and completeness of the personal data, implement safeguards to prevent data breaches (the onus of ensuring reasonable security safeguards to prevent personal data breach will lie with the company), delete personal data once the purpose is served or if the users ask so, set up a grievance redressal mechanism, among other things. The company won't be required to inform principals (users) about the third parties with whom their data will be shared (including data processors), or the duration for which their data will be stored, and if their data will be transferred to other countries. The "verifiably safe" clause for children's data is also a relaxation for companies.

The company, if classified as a "Significant Data Fiduciary" will have to publish the business contact information of a designated Data Protection Officer (DPO) who can answer questions that a user might have about the processing of their personal data.

In case of a company designated only as a "Data Fiduciary", it can be any person undertaking similar role. The DPO will represent the company, be based in India, and be responsible to the Board of Directors or similar governing body. This person will also serve as the "point of contact" for the grievance redressal mechanism. The tech entity will also have to appoint an independent data auditor. *DPDP, while based on 'user consent' creates too many compliance steps and possible issues for businesses.*

In case of failure to fulfil these obligations, companies can be fined anywhere between Rs 50 crores to Rs 250 crores depending on the nature and severity of the non-compliance. The provision that the Board can also recommend the government to block access to an entity's website (say, the company's service site) or content in case of repeated offences or in the "interests of the general public" is concerning.

PASSION

for providing solutions to help clients achieve their goals

RESPECT

for all and alternate viewpoints

INTEGRITY

of thoughts and actions

MASTERY

of our chosen subject to drive innovative and insightful solutions

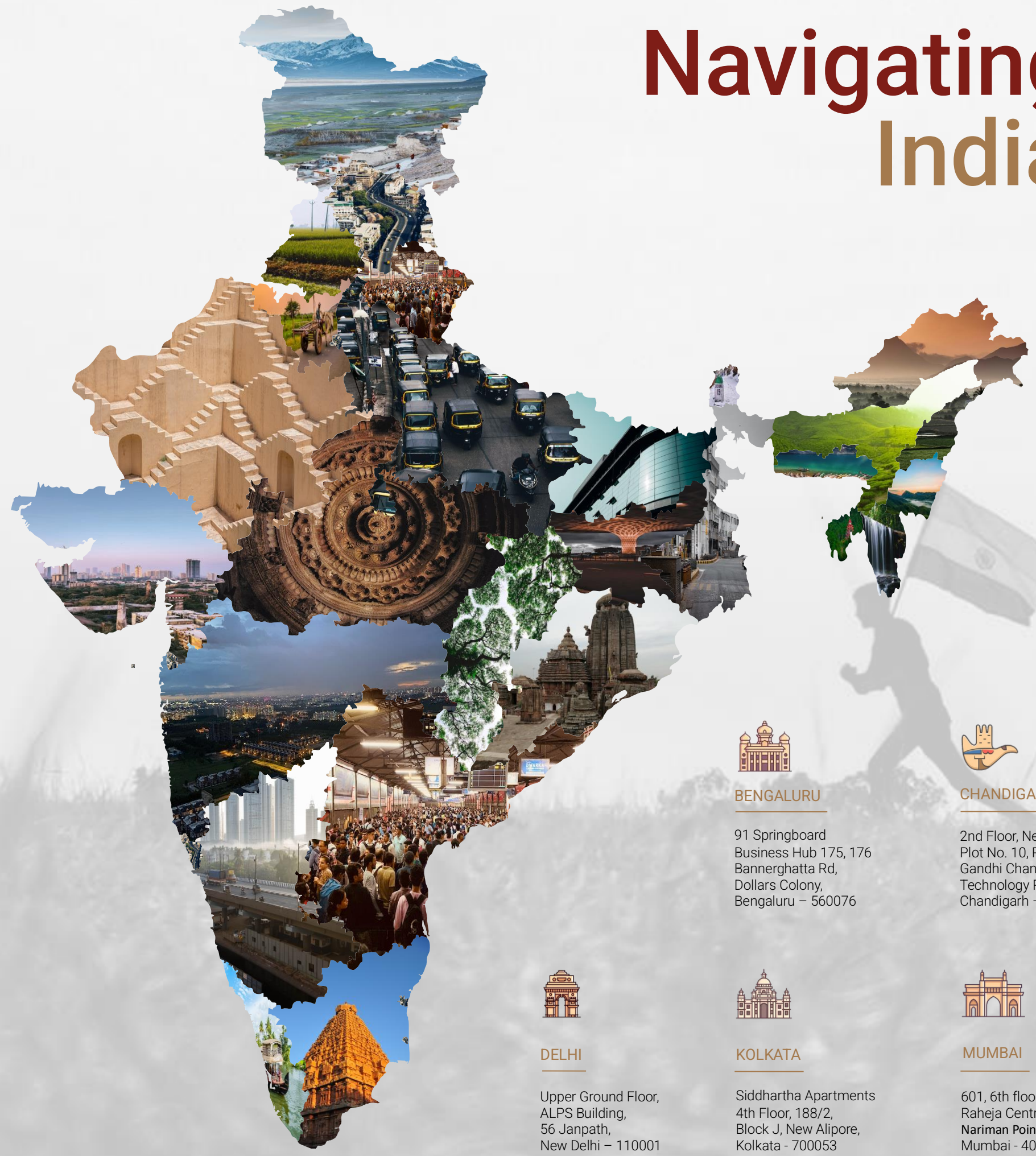
US

representing the Primus collective, where each individual matters

STEWARDSHIP

for building a better tomorrow

Navigating India



BENGALURU

91 Springboard
Business Hub 175, 176
Bannerghatta Rd,
Dollars Colony,
Bengaluru – 560076

CHANDIGARH

2nd Floor, Netsmartz,
Plot No. 10, Rajiv
Gandhi Chandigarh
Technology Park,
Chandigarh – 160019

DELHI

Upper Ground Floor,
ALPS Building,
56 Janpath,
New Delhi – 110001

KOLKATA

Siddhartha Apartments
4th Floor, 188/2,
Block J, New Alipore,
Kolkata - 700053

MUMBAI

601, 6th floor,
Raheja Centre,
Nariman Point,
Mumbai - 400021