India: India's New Data Protection Law. Where Does It Come From, and What Does It Mean?

17 August 2023

by Dhruv Singh , Shivalik Chandan and Arjun Khurana

G&W Legal

Your LinkedIn Connections with the authors

Background

In 2017, the Indian Supreme Court, in a landmark judgment (the "**Puttaswamy Judgement**"), found privacy to be a fundamental right granted to every person under the Indian Constitution. The right was read into the right to life and personal liberty granted under Article 21.

Fundamental rights, however, while enforceable against the state, are not necessarily so against private entities or individuals.[1] This created a need for a robust legislation setting out provisions on data protection for data subjects and data fiduciaries in India. In the Puttaswamy Judgement, reference was made to an Expert Group which had published a Report in 2012 regarding a framework for protection of privacy concerns which would expectedly be used to draft a legislation for India's data protection regime. Additionally, the Puttaswamy Judgement also referred to a memorandum submitted by the Government where the Government had constituted a Committee to review data protection norms and make recommendations. In light of these, the Puttaswamy Judgement stated that it would be appropriate for this committee to make

determinations for putting in place a robust data protection regime and called upon the Government to take all necessary steps to put such a law in place.

Prior to the Puttaswamy Judgement, India's data protection laws were limited to the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ("**SPDI Rules**"), a set of rules framed under the provisions of the Information Technology Act, 2000. The SPDI Rules provide a rudimentary set of data protection rules, with obligations for corporates who collect personal information to provide a privacy policy, obtain consent before collecting personal information, and put in place the prescribed security standards and procedures. An overhaul of the law had thus been long overdue.

The Committee constituted in 2017, chaired by Justice BN Srikrishna, presented the Draft Personal Data Protection Bill, 2018 to the Ministry of Electronics and Information Technology ("**MeitY**"), which was then further amended and formed the Personal Data Protection Bill, 2019 ("**PDPB 2019**"). The PDPB 2019 was presented in Parliament, where it was referred to a Joint Parliamentary Committee ("**JPC**") for further inputs. The JPC, in 2021, published its report along with a new Draft Data Protection Bill, 2021 ("**DPB 2021**") which contained amendments to the PDPB 2019.

In 2022, the Parliament withdrew the PDPB 2019, citing the JPC report and the need for a "comprehensive legal framework on digital ecosystem". A few months later, MeitY published the Digital Personal Data Protection Bill, 2022 for public consultation.

Becoming Law

On the 3rd of August 2023, five years after the first draft data protection law was introduced, the Digital Personal Data Protection Bill, 2023 ("**DPDPB 2023**"), was introduced in the Lok Sabha (the lower house of the Indian Parliament). Opposition leaders raised issues with the DPDPB 2023, calling it "cumbersome", and raising concerns about the ability of the government to exclude itself from the operation of the proposed new law. They also demanded that it be sent back to the Parliamentary Committee, and also alleged that Opposition members in the Committee had not been given a chance to properly analyse the DPDPB 2023 before it was presented in Parliament. However, due to the overwhelming majority of the BJP (the party in power at the centre), it was passed by the Lok Sabha on 7 August 2023. Subsequently, it was introduced and passed in the Rajya Sabha on 9 August 2023 by a voice vote, as members of the Opposition had walked out staging a protest against the ruling party.

Having been notified in the Official Gazette, the DPDPB 2023 has now become law- as 'The Digital Personal Data Protection Act, 2023' ("**DPDPA 2023**"). Though for the reasons discussed in the conclusion, it can't immediately be implemented.

Data Principal's Rights

The DPDPA 2023 defines Data Principals as individuals to whom the personal data relates. Data Principals include the parents or lawful guardians of children (under 18).

Specific rights are granted to Data Principals under the DPDPA 2023, which are:

1. The right to obtain from the Data Fiduciary upon request –
    - a summary of the data being processed.
    - The processing activities being carried out.
    - Identities of each Data Fiduciary and Data Processor with whom data has been shared and specifics of what this data consists of.
    - other information the government may prescribe in rules that are to follow.
2. The right to correction, completion, updating, and erasure of personal data, for which consent to processing has already been given.
3. The right to withdraw consent given for processing personal data.
4. The right to an easily accessible grievance redressal mechanism to be provided by the Data Fiduciary
5. The right to nominate any other person who shall, in the event of the Data Principal's death or incapacity, exercise the rights of the Data Principal under the DPDPA 2023.

Grounds for Processing of Data

Personal Data under the DPDPA 2023 is defined as data about an individual who is identifiable by or in relation to that data. The law explicitly excludes its applicability to such data processed for individual or domestic purposes (though these terms haven't been defined therein), and personal data which has been made publicly available by the person to whom the personal data relates or by any other person in accordance with applicable law (this may have an impact on the legality of scraping of such Personal Data).

Interestingly, the DPDPA 2023 does not make any distinction between categories of personal data, as was the case with the SPDI Rules. All types of personal data (ranging from names and phone numbers to financial information) will be subject to the same standards as prescribed under the DPDPA 2023.

The DPDPA 2023 provides for two grounds by which personal data can be processed.

i) Consent

The primary ground for processing of personal data is still the consent of the Data Principal. Provisions of the DPDPA 2023 dictate requirements to be met while making a request to obtain consent for processing. Essentially, any such request must contain the following:

- Specifics of the personal data being collected and the purpose for which the data is proposed to be processed
- The manner in which the Data Principal may exercise their rights (as described above), and how they may withdraw their consent to the processing of their personal data
- The manner in which the Data Principal may make a complaint to the Data Protection Board

The DPDPA 2023 places a requirement for Data Fiduciaries to intimate Data Principals who have consented to the processing of their data prior to the enactment of the law of the aforementioned aspects.

The form of both these notices may be prescribed by subordinate legislation (rules). However, the DPDPA 2023 does state that the request must be made in "clear and plain language", and the Data Principal must be given the option to access the request in English or in any language specified in the Eighth Schedule of the Indian Constitution. Additionally, the contact details of the Data Protection Officer (in the case of Significant Data Fiduciaries) or any other person authorised by the Data Fiduciary to respond to requests of Data Principals must be provided in the request for consent as well.

Consent, if granted, must be specific, free, informed, unconditional, and unambiguous. It must be granted through a clear affirmative action and shall signify the processing of personal data for the specified purpose only. Additionally, the consent shall be limited to the processing of such personal data as is necessary to fulfil the specified purpose. If any part of the consent infringes the provisions of the DPDPA 2023, it shall be invalid to the extent of the infringement.

Since the consent provision states specifically that consent must be "free" and "unconditional", consent granted by an employee to an employer would, due to the nature of that relationship, not be free or unconditional. As such, it would seemingly imply that all such processing may be undertaken under legitimate uses as a part of "purposes of employment" (as discussed below), but in the absence of clarity with respect to the extent of this provision, it remains to be seen whether this aspect will be clarified in the future, either through rules or through decisions of the Data Protection Board or the courts.

ii) Legitimate uses

Apart from consent-based processing, the DPDPA 2023 provides certain "legitimate uses" for which personal data can be processed without obtaining consent as outlined above. These legitimate uses are:

1. For a specified purpose for which a Data Principal has shared personal data with a Data Fiduciary and has not indicated that they do not consent to the use of their personal data,

2. For the State in providing benefits, subsides, services, certificates, licenses or permits to the Data Principal, where the Data Principal has previously consented to the processing of their personal data by the State or instrumentality for the above mentioned,
3. For the performance of any function by the State in the interest of India's sovereignty and integrity, or the security of the State,
4. For fulfilling any obligation under any applicable law upon a person to disclose any information to the State or its instrumentalities,
5. For compliance with any judgement, decree or order,
6. For responding to a medical emergency,
7. For taking measures to provide medical and health services to any individual during an epidemic, disease outbreak, or any threat to public health,
8. For taking measures to ensure safety of individuals or to provide assistance or support to them during any disaster or breakdown of public order,
9. For the purposes of employment or those related to safeguarding the employer from loss or liability. Examples given in the DPDPA 2023 include prevention of corporate espionage, maintenance of confidentiality of trade secrets, or provision of any service or benefit sought by a Data Principal who is an employee. However, there is no guidance provided in the DPDPA 2023 as to how this provision would be applicable, and what the determining factors would be. Even though illustrations have been provided for quite a few other provisions, none have been provided here.

Duties of Data Fiduciaries and Data Principals

The DPDPA 2023 draws a distinction between Data Fiduciaries (Controllers) and Data Processors. Data Fiduciaries are defined as those persons who determine the purpose and means of processing of the personal data, while Data Processors are those persons who simply process personal data on behalf of a Data Fiduciary.

The DPDPA 2023 places obligations on Data Fiduciaries only. Essentially, responsibilities regarding personal data, even when processed by Data Processors, have to be fulfilled by Data Fiduciaries as per the legislation. Obligations to be met by Data Fiduciaries in addition to the ones regarding consent (discussed above) are as follows:

1. Where personal data being processed is likely to be used to make a decision that affects the Data Principal, or disclosed to another Data Fiduciary, the Data Fiduciary shall be required to ensure its completeness, accuracy, and consistency.
2. Data Fiduciaries shall implement "appropriate technical and organisational measures" to ensure effective compliance with the provisions of the DPDPA 2023 and any rules made thereunder. These measures however haven't been specified.
3. In a similar vein, the DPDPA 2023 requires Data Fiduciaries to "take reasonable security safeguards" to prevent personal data breaches, in furtherance of the protection of personal data under its possession and control, including data

which is being processed on its behalf by a Data Processor. However, no clarifications are provided as to what these reasonable security safeguards should be.
4. Data Fiduciaries are to inform the Data Protection Board and each affected Data Principal in the event of a personal data breach, in a manner and form which is to be prescribed by rules.
5. If a Data Principal withdraws consent, or as soon as it is reasonable to assume that the specified purpose for data processing is no longer being served (whichever is earlier), the Data Fiduciary shall delete the personal data. However, this deletion shall not be carried out if the retention of that data is required by any applicable law in India. Additionally, Data Fiduciaries are obligated to ensure that Data Processors processing data on their behalf delete the data on the occurrence of the events mentioned hereinabove.
6. Data Fiduciaries are to publish contact details of the Data Protection Officer (in the case of Significant Data Fiduciaries) or the person responsible for answering questions raised by Data Principals regarding the processing of their data on behalf of the Data Fiduciary. The manner of the publishing is to be prescribed by the rules.
7. Data Fiduciaries are to establish an "effective mechanism" for grievance redressal of Data Principals. The specific nature and details of this mechanism are not expanded upon in the DPDPA 2023.
8. There is no restriction on transferring personal data outside of India for the purposes of processing. However, the DPDPA 2023 does grant the Central Government the power to notify any countries to which such transfer is prohibited.

The DPDPA 2023 also provides for a special class of Data Fiduciaries called Significant Data Fiduciaries. Essentially, the Government may notify specific Data Fiduciaries or a class of Data Fiduciaries as Significant Data Fiduciaries keeping in mind factors such as the volume and sensitivity of the personal data processed, the risk to the rights of Data Principals, the potential impact on India's sovereignty and integrity, security of the State, and public order. Significant Data Fiduciaries are obligated to comply with certain enhanced requirements in addition to those already listed above, which are:

1. Appointing a Data Protection Officer, an individual based in India who shall be responsible to the Board of Directors (or such similar governing body) of the Data Fiduciary, and who shall act as the point of contact for the grievance redressal mechanisms under the DPDPA 2023
2. Appointing an independent data auditor to carry out data audits, who shall ensure the compliance of the Significant Data Fiduciary with the provisions of the DPDPA 2023
3. Undertaking periodic Data Protection Impact Assessments, a process comprising a description of the rights of Data Principals and the purpose of data processing, assessment and management of the risk to the Data Principal rights, and other matters as may be prescribed by rules
4. Other obligations may be imposed on Significant Data Fiduciaries through rules.

The Central Government has been granted the power to notify Data Fiduciaries or classes of Data Fiduciaries, including "startups"[2], to be exempted from certain provisions of the DPDPA 2023. Additionally, within five years of the enactment of the DPDPA 2023, the Central Government may notify the non-applicability of any provisions of the Act to any Data Fiduciary or class of Data Fiduciary for such period as may be specified in the notification.

Under the DPDPA 2023, Data Principals are required to abide by certain obligations as well. These are:

1. Complying with provisions of applicable laws while exercising their rights under the DPDPA 2023
2. Not impersonating another person while providing their personal data for a specified purpose
3. Not suppressing any material information while providing personal data for any document, unique identifier, proof of identity or proof of address issued by the State or its instrumentalities
4. Not registering a false or frivolous complaint with the Data Protection Board
5. Ensuring that while exercising the right to correction/erasure of personal data, they only furnish information which is verifiably authentic

Personal Data of Minors

The DPDPA 2023 prescribes certain special provisions as to the processing of data where the Data Principal is a minor. Consent of the parent or legal guardian must be obtained prior to such processing in a manner which is to be prescribed by rules. Processing of personal data of minors for purposes which may cause detrimental effects to the child's well-being, or involves tracking, behavioural monitoring, or target advertising towards children, is prohibited.

However, the DPDPA 2023 also allows for two ways through which exceptions can be granted. Firstly, rules framed under the DPDPA 2023 may exempt certain classes of Data Fiduciaries, or certain purposes of processing data. Secondly, the Central Government has the right to exempt specific Data Fiduciaries by way of a notification if it is satisfied that the Data Fiduciary has ensured that data processing of children's personal data is "done in a manner that is verifiably safe". However, there is no guidance as to what factors are to be taken into account while making this determination. Exemptions, if granted, would be from the requirement of consent from parents/legal guardians and the prohibition on tracking, behavioural monitoring, or targeted advertisements.

Data Protection Board

The DPDPA 2023 prescribes the institution of the Data Protection Board of India ("**DPB**"), a body exclusively empowered to hear complaints regarding violations of the

provisions of the DPDPA 2023 and to impose penalties. The composition and members of the DPB are entirely determined by the Central Government.

The powers and functions of the DPB as provided in the DPDPA 2023 are:

1. Directing any remedial or mitigation measures required upon receipt of intimation of a personal data breach by a Data Fiduciary, inquiring into such breach, and imposing penalties if required
2. Inquiring into a violation of the DPDPA 2023 by a Data Fiduciary as a result of a complaint made by a Data Principal, on reference from the Central Government, or in compliance with the directions of a court, and imposing penalties if required
3. Inquiring into a Consent Manager's[3] violation of obligations regarding personal data upon a complaint from the Data Principal in relation to whom such violation has taken place, and imposing penalties if required
4. Imposing a warning or issuing costs to a complainant, if the DPB believes at any stage after receipt of the complaint, that it is false or frivolous

The DPB is required to give all persons concerned an opportunity to be heard and conduct the inquiry in accordance with the principles of natural justice. The DPB has been granted with the powers of a civil court under the Code of Civil Procedure with regard to summoning witnesses, inspecting data, books, documents, registers or other documents, and receiving affidavits requiring the discovery and production of these documents. However, the DPB is prohibited from preventing access to any premises or taking into custody equipment or items which may adversely affect the day-to-day functioning of a person.

Appeals against the DPB's decisions lie with the Telecom Disputes Settlement and Appellate Tribunal ("**Appellate Tribunal**") established under the Telecom Regulatory Authority of India Act, 1997. Any appeal against the DPB's decision must be made within sixty days of receipt of the order or decision, with the Appellate Tribunal being granted the discretion to hear an appeal submitted after the deadline if sufficient reasons are provided. Appeals against the decisions of the Appellate Tribunal will lie with the Supreme Court, and such appeals must be made within ninety days of the decision of the Appellate Tribunal (with the Supreme Court retaining the discretion to accept appeals made after the deadline subject to sufficient reasons).

The DPB also has the power to refer a dispute to mediation if it is of the opinion that a complaint may be resolved through mediation. The procedure may be mutually agreed upon by the parties to the dispute, or in accordance with any applicable law.

Additionally, at any stage during the inquiry proceeding, the DPB may accept a voluntary undertaking in respect of a violation of the provisions of the DPDPA 2023, and the acceptance of this voluntary undertaking shall constitute a bar to any further proceedings regarding that matter (unless the party fails to abide by the terms of the voluntary undertaking).

Any penalties collected by the DPB under the DPDPA 2023 are to be deposited into the Consolidated Fund of India. Additionally, the DPDPA 2023 repeals section 43A of the Information Technology Act, 2000, which was the only provision which granted compensation to the affected data subject (or Data Principal). In the event of a breach of a Data Principal's right to privacy, there is no provision in law for any recompense being awarded to them.

Penalties

The DPDPA 2023 prescribes monetary penalties for the violation of its provisions. The DPDPA 2023 also prescribes that the DPB should, while determining the quantum of penalty, take the following into consideration:

1. The nature, gravity, and duration of breach
2. The type of personal data affected by the breach
3. Repetitive nature of the breach
4. Whether the person, as a result of the breach, has realised a gain or evaded a loss
5. Whether the person took any action to mitigate the effects of the breach, and if so, the timeliness and effectiveness of the action
6. Whether the penalty is proportionate and effective (with regard to the need to deter breach of the DPDPA 2023)
7. The likely impact of the penalty on the person

The thresholds for the penalties as prescribed in the DPDPA 2023 are as follows:

1. Breach of obligation of Data Fiduciary to take reasonable security safeguards for preventing personal data breaches – up to INR 250,00,00,000
2. Breach of obligation of Data Fiduciary to inform the DPB and affected Data Principals in the event of a personal data breach – up to INR 200,00,00,000
3. Breach of additional obligations regarding personal data of minors – up to INR 200,00,00,000
4. Breach of additional obligations on Significant Data Fiduciaries – up to INR 150,00,00,000
5. Breach of provisions of voluntary undertaking accepted by the DPB – up to the threshold of penalty for the breach for which the voluntary undertaking was accepted
6. Breach by Data Principal of any obligations imposed upon them – up to INR 10,000
7. Breach of any other provisions of the DPDPA 2023 or rules made thereunder – up to INR 50,00,00,000

Conclusion

The DPDPB 2023 has since been notified on the 11th of August 2023, being made effective immediately. However, a large number of the provisions may only become

effective once the subordinate laws (rules) are notified by the government. Furthermore, a plain reading of section 39 of the DPDPA 2023 shows that the law can't be enforced until the DPB has been appointed, as it would have exclusive jurisdiction to decide matters relating to the law.

Footnotes

1. The Supreme Court, in January 2023, has held that rights under article 19 and 21 of the Constitution can in fact be enforced against private individuals. (*Kaushal Kishore vs State of Uttar Pradesh & Ors.*)

2. Defined in the DPDPA 2023 as a private limited company, partnership firm, or limited liability partnership incorporated in India which is eligible to be and is recognised as such in accordance with criteria and processes notified by the department of the Central Government to which matters relating to startups are allocated.

3. The DPDPA 2023 defines 'Consent Managers' as such entities that have been registered with the DPB that act as a single point of contact with the Data Principal to manage the giving, withdrawal, review and management of the Data Principal's consent for the processing of his/her data.

AUTHOR(S)

Dhruv Singh
G&W Legal

Shivalik Chandan
G&W Legal

Arjun Khurana
G&W Legal