Technology Law Analysis

August 07, 2023

INDIA'S DIGITAL PERSONAL DATA PROTECTION ACT, 2023: HISTORY IN THE MAKING

INTRODUCTION

The Digital Personal Data Protection Act, 2023 ("**DPDPA**") was passed by Lok Sabha (lower house of the Indian Parliament) on August 7, 2023 , and by the Rajya Sabha (upper house of the Indian Parliament) on August 9, 2023. The DPDPA has also received the President's assent, and upon being enacted, it will bring in several significant changes to the existing data protection regime.

Since 2018, the Indian Government has been in the process of legislating a standalone data protection legislation. The DPDPA, once enacted, will replace the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011.

The DPDPA introduces several compliance requirements for collection and processing of personal data. These provisions are open-ended, leaving much to be prescribed by the Central Government. The DPDPA contains a memorandum regarding delegated legislation which enumerates the matters still to be prescribed by the Central Government via rules. The memorandum states that these are matters of detail and accordingly it is not practicable to provide them in the DPDA itself. This has likely been inserted following criticism that the earlier 2022 version ("**2022 Bill**") left a lot to be covered by rules enacted under the main statute. The matters subject to the delegated legislation include but are not limited to notice requirements; functions of the consent manager; procedure for data breach notifications; parental consent for children's data; grievance; exemptions for processing of personal data; redressal procedures.

The DPDPA also introduces several additional illustrations as compared to the 2022 Bill to explain its provisions.

The Data Protection Board of India ("**Board**") is proposed to be the adjudicatory body for enforcement of the DPDPA.

Our analysis of key provisions of the DPDPA has been discussed below.

1. Applicability

The DPDPA defines "personal data" broadly to include any data about an individual who is identifiable by or in relation to such data.[1] The DPDPA also introduces a definition of 'digital personal data,' defined to mean personal data in digital form.[2]

The DPDPA applies to the processing of **digital** personal data in India, where the personal data is either (i) collected in digital form; or (ii) collected in a non-digitized format and subsequently digitized.[3] The DPDPA shall not apply to processing of personal data in non-digitized form.

The DPDPA has **extra territorial application,** i.e.,it applies to the processing of personal data outside India (irrespective of the location of the entity processing) in connection with offering goods or services to data principals[4]located within the territory of India.[5]

The previous 2022 Bill also applied to processing of digital personal data outside of India, if processing was connected with the profiling of data principals within India. However, the DPDPA has omitted this provision. Hence, it appears that the DPDPA will not apply to 'profiling' of data subjects from outside the territory of India only to the extent that it is not in connection to providing any good or service to the data subject.[6] For example, profiling of data subjects located in India for research purposes should not trigger the compliances under this law.

The provisions of the DPDPA do not apply to (i) personal data processed by an individual for personal or domestic purposes, and (ii) personal data that is made or caused to be made publicly available by (a) the data principal to whom such personal data relates, or (b) any other person who is under a legal obligation to make personal data publicly available.[7]

2. Data Fiduciary, Data Principal and Data Processor

The key definitions under the DPDPA are as follows:

- Data Fiduciary" is defined as any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data.[8]
- "Data Principal" is the individual to whom the personal data relates. Where such an individual is a child, the term includes the parent or lawful guardian of the child. Where the individual is a person with disability, it includes their lawful guardian acting on behalf of such individual.[9] Thus, it is clear that the DPDPA covers Data of natural

Research Papers

Littler International Guide (India) 2024
November 08, 2024

Unmasking Deepfakes
October 25, 2024

Are we ready for Designer Babies
October 24, 2024

Research Articles

The Bitcoin Effect
November 14, 2024

Acquirers Beware: Indian Merger Control Regime Revamped!
September 15, 2024

Navigating the Boom: Rise of M&A in Healthcare
August 23, 2024

Audio

Digital Lending - Part 1 - What's New with NBFC P2Ps
November 19, 2024

Renewable Roadmap: Budget 2024 and Beyond - Part I
August 26, 2024

Renewable Roadmap: Budget 2024 and Beyond - Part II
August 26, 2024

NDA Connect

Connect with us at events, conferences and seminars.

NDA Hotline

Click here to view Hotline archives.

Video

"Investment return is not enough" Nishith Desai with Nikunj Dalmia (ET Now) at FII8 event in Riyadh
October 31, 2024

Analysing SEBI's Consultation Paper on Simplification of registration for FPIs
September 26, 2024

individuals only.

- "Data Processor" is any person who processes personal data on behalf of a data fiduciary.[10]

3. Notice and Consent

The DPDPA requires the data fiduciary to provide notice[11] and obtain consent[12] from the data principal on or before processing personal data.

The notice accompanying a request for consent must inform the data principal of: (i) the personal data to be processed and purpose for which such data is to be processed; (ii) the manner in which she may exercise her rights under the DPDPA; and (iii) the manner in whiboch the data principal may make a complaint to the Board. The manner of such notice will be prescribed in rules issued under the DPDPA.

Where a data principal has given consent to processing of their personal data prior to the commencement of the DPDPA, the data fiduciary is required to provide notice containing the above details "*as soon as it is reasonably practicable*".[13] Such data can be processed till such time the data principal withdraws their consent. The DPDPA does not clarify the timeline that may be considered "reasonably practicable". As a practice, data fiduciaries should document the efforts made to ensure that notice is provided in a timely manner.

The consent should be freely given, specific, informed and unambiguous, with clear affirmative action.[14] The consent should be limited to such personal data as is necessary for the specified purpose in the request for consent.[15] The DPDPA provides the following example: X, an individual, downloads Y, a telemedicine app, and Y requests the consent of X for (a) the processing of her personal data for making available telemedicine services, and (b) accessing her mobile phone contact list, and X signifies her consent to both. Since phone contact details are not necessary for making available telemedicine services, her consent shall be limited to the processing of her personal data for making available telemedicine services. Hence, when consent taken by the Data Fiduciary go beyond the specified purpose, then based on the above example it could be viewed that the Data Principal is deemed to have given limited consent whereby the Data Fiduciary may not be able to process other personal data not linked to the purpose.

Given this specific restriction, data fiduciaries should be able to justify specific purposes for data processing. For certain types of datasets, (such as location data) it may be difficult to justify the purpose of such collection unless it has a nexus with the service provided to the data subject (such as map services or delivery services).

It also remains to be seen whether broadly worded consent notices may justify multiple grounds for processing. For instance, taking consent for 'providing service' without specifying the purpose and use of each item of personal data collected towards providing the service may not satisfy the requirement of specific consent and specified purpose. It is also unclear whether consent to provide certain ancillary services (such as marketing services in relation to the primary purpose) may qualify as a purpose for which data processing may be justified. This could hugely impact data mining and data monetization activities which essentially functioned via broadly worded consents.

The DPDPA also renders consent invalid, which infringes the DPDPA or any other law, to the extent of such infringement.[16] For instance, a notice requiring a data principal to consent for waiving her right to file a complaint to the Board, shall be held invalid.

The data fiduciary is required to give an option to the data principal to access the request for consent and the notice in English OR any language specified in the Eighth Schedule to the Constitution.[17] This requirement may be difficult for some entities, such as online platforms which only support the English language. It is advisable that platforms should be required to provide consent only in the languages supported by the platform.

Withdrawal of consent

The data principal has the right to withdraw their consent where consent is the basis of processing of their data. The ease of such withdrawal should be comparable to the ease with which consent was given.[18] Upon withdrawal of consent, the data principal is required to cease and cause its data processors to cease processing of the personal data within "a reasonable time".[19]

Consent Managers

The DPDPA recognizes the role of 'consent managers.' Consent manager has been defined as a person registered with the Board, and acts as a single point of contact to enable a data principal to give, manage, review and withdraw their consent through an accessible, transparent and interoperable platform.[20] A data principal may give, manage, review or withdraw their consent to the data fiduciary through a Consent Manager.[21] Data fiduciaries will have to implement processes to enable the consent manager to take such actions on behalf of the data principal. Once the rules and regulations relating to consent managers are framed, further clarity is expected on the consent manager framework.

Consent managers will be accountable to the data principal and must act on behalf of the data principal in such manner and subject to obligations as may be prescribed.[22] The Board may impose penalties on Consent Managers in certain instances, as discussed in point 18 below.

Processing for Legitimate Purposes

The DPDPA permits the processing of personal data without seeking consent of the data principals, for certain specified 'legitimate uses,'[23] namely:

1. Where the data principal voluntarily provides personal data to the data fiduciary for the specified purpose and does not indicate to the data fiduciary that she does not consent to use of her personal data for such purposes;
2. For the state or any of its instrumentalities to provide or issue to the Data Principal such subsidy, benefit, service, certificate, license or permit as may be prescribed, subject to standards to be followed for processing of data, which are also yet to be prescribed Further, it is to be allowed only when:

Scope of judicial interference and inquiry in an application for appointment of arbitrator under the (Indian) Arbitration and Conciliation Act, 1996
September 22, 2024

1. she has previously consented to the processing of her personal data by the State or any of its instrumentalities for above mentioned such reasons, or
2. Such personal data of the data principal is available from any database, register, book or any other document maintained by the State or its instrumentalities and is notified by the Central Government to be digitized subsequently, or it is already available in the digital form;

3. For the performance of any function by the State or any instrumentality of the State under any law currently in force in India or in the interest of sovereignty and integrity of India or security of the State;
4. For fulfilling any obligation under any law for the time being in force in India on any person to disclose any information to the State or any of its instrumentalities, subject to such processing being in accordance with the provisions regarding disclosure of such information in any other law for the time being in force;
5. For compliance with any judgment or decree or order issued under any law for the time being in force in India, or any judgment or order relating to claims of a contractual or civil nature under any law for the time being in force outside India;
6. For responding to a medical emergency involving a threat to the life or immediate threat to the health of the Data Principal or any other individual;[24]
7. In case of taking measures to provide medical treatment or health services to any individual during an epidemic, outbreak of diseases or any other threat to public health;[25]
8. For taking measures to ensure safety of, or provide assistance or services to any individual during any disaster, or any breakdown of public order. The expression “disaster” has the same meaning as assigned to it under the Disaster Management Act, 2005;
9. For purposes related to employment or for safeguarding the employer from loss or liability such as prevention of corporate espionage, maintenance of confidentiality, intellectual property, classified information or provision of any service or benefit sought by a Data Principal who is an employee, etc.[26]

One of the legitimate uses prescribed is where the data principal voluntarily provides personal data for purposes that are specified (in all likelihood by the data principal). It appears here that this legitimate use would apply only in cases where personal data is provided without being asked for or prompted by the data fiduciary. Thus, the data principal is given a certain degree of autonomy to determine the purpose for which processing can be done without the data fiduciary complying with notice and consent requirements.

4. Data Principal Rights and Duties

The data principals may exercise certain rights[27] with respect to their personal data, which are discussed below:

1. **Right to access information about personal data**: The data principal has the right to obtain (i) a summary of personal data which is being processed by such data fiduciary and the processing activities undertaken by that data fiduciary with respect to personal data (ii) identities of all the data fiduciaries and data processors with whom the personal data has been shared by the data fiduciary along with the description of the personal data so shared and; (iii) any other information related to the personal data of such data principal and its processing as may be prescribed by the Central Government[28] The requirements (ii) and (iii) do not apply to any sharing of personal data by a data fiduciary with another data fiduciary who is authorized by law to obtain such personal information where such sharing is pursuant to a 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. The exemption related to investigation of offences, etc. suggests that in the event a law enforcement agency seeks the personal data of a data principal, the identity of such law enforcement agencies will not need to be disclosed to the data principal.

2. **Correction, completion, updation or erasure of personal data**: The data principal has the right to correction, completion, updation and erasure of their personal data.[29] Upon receipt of a request for correction/updation/completion/erasure, a data fiduciary is required to (i) correct inaccurate or misleading personal data; (ii) complete any incomplete personal data and (iii) update relevant personal data.[30] The data principal may also request for erasure of their personal data which is no longer necessary for the purpose for which it was processed unless retention is necessary for a legal purpose. Upon request of erasure, the Data Fiduciary shall erase the personal data unless retention of the same is necessary for the specified purpose or for compliance with any law for the time being in force.[31] As per the language of the DPDPA, a request for erasure does not need to be adhered to if the data is necessary to be retained for the purpose specified at the time of obtaining consent.[32] Therefore, if a data principal intends to prevent all processing of her data, instead of erasure, a request for withdrawal of consent must be made.

3. **Grievance redressal**: Data principals have the right to register their grievances with the data fiduciary or the consent manager in respect of any act or omission of such data fiduciary or consent manager regarding the performance of its obligations in relation to the personal data of such data principal or the exercise of their rights under the DPDP or rules made thereunder.[33] The timeline within which the data fiduciary or consent manager must respond to any grievance will be prescribed under rules to be framed under the DPDP. Further, the data fiduciary will need to exhaust the right to grievance redressal before approaching the Board.

4. **Right to nominate**: The data principal has the right to nominate (in the manner prescribed) any other individual to exercise the above-mentioned rights under the DPDPA in the event of the death or incapacity (unsoundness of mind or infirmity of body) of the data principal.[34] The manner in which this is prescribed will be very interesting, especially if there is an obligation to provide the option of a “nominee” while taking the initial consent.

There are also several duties[35] of data principals under the DPDPA as discussed: (i) to ensure not to impersonate another person while providing personal data; (ii) ensure not to suppress any material information while providing personal data for any document, unique identifier, proof of identity or proof of address issued by the State or any of its instrumentalities; (iii) not to register a false or frivolous grievance or complaint with a data fiduciary and (iv) furnish only such information as is verifiably authentic, while exercising the right to correction or erasure. The DPDPA

imposes a penalty of up to INR 10,000 for non-compliance by the data principal of its duties.[36]

The prohibition on providing false information seems to overlap with the prohibition under the Indian Penal Code, 1100%[37] ("**IPC**") which prohibits the furnishing of false information to any public servant. However, failure of a Data Principal to carry out the said duties would not dilute the obligations of the Data Fiduciary under the DPDPA.

5. Data Fiduciary Obligations

Data fiduciary may appoint, engage, use or involve a data processor to process personal data on its behalf for any activity related to offering of goods and services to the data principal.[38]

A snapshot of the data fiduciary obligations[39] are provided below:

1. Compliance with the DPDPA irrespective of whether processing is undertaken by another processor/data fiduciary on its behalf or; if the data principal is non-compliant with their duties;[40]
2. Implement appropriate technical and organizational measures to ensure effective adherence with the provisions of the DPDPA;
3. Ensure the accuracy, completeness and consistency of the personal data when such personal data is processed to make a decision that affects the data principal or if the personal data is likely to be disclosed another data fiduciary;[41]
4. Protect personal data in its possession or under its control by taking reasonable security safeguards to prevent personal data breach. *The DPDPA does not prescribe or recommend the standards that should be implemented*;[42]
5. In the event of a personal data breach; notify the Board and each affected data principal in the form and manner as may be prescribed;[43]
6. Publish, in such manner as may be prescribed, the business contact information of a Data Protection Officer ("**DPO**"), if applicable, or a person who is able to answer on behalf of the data fiduciary, the data principal's questions about the processing of their personal data;[44]
7. Subject to compliance of laws, deletion of data by itself and cause deletion by the data processor(as applicable), upon the data principal withdrawing her consent or as reasonably assumed that the specified purpose is no longer being served, whichever is earlier.[45]

From an overall perspective, the obligations of the data fiduciaries do not seem excessive and the same should largely protect the interests of the data principal. Further, the DPDPA **does not** specify the technical and organizational measures/security safeguards required to be implemented which is a welcome move. Industry specific standards can develop over time based on factors such as sensitivity of the data, risk involved, nature of the industry etc. These standards can be adhered to by entities in the industry.

6. Significant Data Fiduciaries

The Central Government may classify a Data Fiduciary or a class of Data Fiduciary as a Significant Data Fiduciary ("**SDF**") based on certain factors like the volume and sensitivity of the data processed by them, the risk of harm to the data principal, potential impact on the sovereignty and integrity of India etc.[46] A SDF would have additional obligations including appointing a DPO in India[47] and an independent Data Auditor[48], along with undertaking certain additional measures such as data protection impact assessments.[49]

7. Exemptions

The DPDPA exempts data fiduciary from certain obligations (except for being responsible for its data processor and taking reasonable security safeguards), such as notice and consent requirements for certain specified circumstances including (i) where processing of personal data is necessary for enforcing any legal right or claim; (ii) processing of personal data by any court or tribunal or any other body in India which is entrusted by law with the performance of any judicial or quasi-judicial function or regulatory or supervisory function,; where such processing is necessary for the performance of such function; (iii) where personal data is processed in the interest of prevention, detection, investigation or prosecution of any offence or contravention of any law; (iv) where the personal data of data principals not within the territory of India is processed pursuant to any contract entered into with any person outside the territory of India by any person based in India; (v) for processing necessary for a merger/amalgamation or similar arrangement as approved by a court or tribunal or other authority competent; and (vi) for ascertaining the financial situation of a person who has defaulted on a loan or advance given by a financial institution.[50]

Additionally, the DPDPA also enables the Central Government to exempt the applicability of the DPDPA by way of notification under the following circumstances:

- Exempt an instrumentality of the State (which could include entities that are financially, functionally and administratively dominated by or under the control of the Central Government) from compliance with this law in the interest 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. The DPDPA also exempts the processing by the Central Government of any personal data that such instrumentality may furnish to it.

  This exemption should ideally be subject to procedural safeguards of necessity, proportionality, and legality.[51]
- Exempt applicability of the DPDPA to the processing of personal data 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 and such processing is carried on in accordance with standards as may be prescribed.[52]

Additionally, the DPDPA states that the Central Government may notify certain data fiduciaries or class of data fiduciaries, such as start-ups, to whom the provisions of Section 5 (Notice), Section 8(3) (Obligations of data fiduciary while processing personal data in cases where it is used to make a decision which may affect the data principal, or where it is disclosed to another data fiduciary), Section 8(7) (Obligations of data fiduciary in related to erasure of

personal data) and Sections 10 (Additional obligations of significant data fiduciary) and 11 (Right to access information about personal data) of the DPDPA will not apply. The term "startup" has been defined as a private limited company or a partnership firm or a limited liability partnership incorporated in India, which is eligible to be and is recognised as such in accordance with the criteria and process notified by the department to which matters relating to startups are allocated in the Central Government.

The reason for selection of these specific provisions is not clear in the DPDPA. Additionally, it is unclear currently what other types of data fiduciaries may be excluded by way of this provision. Since "start-ups" have specifically been called out, it is possible that the intent is to cover other similar entities such as micro, small and medium enterprises.

It should also be clarified that the exemption for processing of personal data by courts/tribunals also applies to judicial bodies outside India. Litigation proceedings involving Indian multinational companies may take place globally. Disputes involving Indian parties are also increasingly referred to foreign institutional arbitrations.

The DPDPA exempts outsourcing activities[53] i.e., where personal data of individuals outside India is processed in India on the basis of a contract. However, any cross-border transfer restriction that may be applicable to particular countries could continue to apply in respect of such data as well.[54] Further, We note that the State and its instrumentalities have been absolved from the requirement to erase data at the end of processing and when the purpose of collection of the personal data has been fulfilled[55] (see *Data Retention* below). This may lead to arbitrary retention of data for extended periods of time without reasonable justification. In addition, exemption of compliances for processing of personal data for research, archiving or statistical purposes (if the data is not used for any decision in relation to a data principal) seems excessive as it could lead to the government becoming a central repository of personal data.

8. Retention of Personal Data

The data fiduciary must erase and cause its data processor to erase the personal data, (i) upon receipt of a withdrawal request, or (ii) as soon as it is reasonable to assume that the specified purpose is no longer being served, whichever is earlier, unless retention is necessary for compliance of any law in force.[56]

9. Transfer and Cross-border Transfers of Data

The DPDPA empowers the Central Government to restrict the transfer of personal data by a data fiduciary to notified countries or territories outside of India.[57] Hence, transfer would be permissible to all countries until any of them are blacklisted by the government.

However, if any Indian law (especially sectoral laws) provides for a higher degree of protection or restriction on transfer of personal data outside India, then such laws would continue to apply and will prevail over the DPDPA.[58]

Since "personal data" is broadly defined, this Section will apply to all types of data, irrespective of whether it is sensitive or not.

Since the DPDPA has extraterritorial applicability in cases where foreign companies are offering goods / services to Indian data principals and in situations where a country is blacklisted, then transfer of data to companies in such a country would not be permissible. It could also be extended to mean primary collection of data by companies from such a blacklisted country may not be permissible. End result, foreign companies from such a blacklisted country may be restricted from directly undertaking business in India (especially online models) as basic personal data would be required by all for providing goods / services.

10. Personal Data and Data of Persons with Disability

Data fiduciaries must obtain verifiable consent prior to processing the child's personal data (from the parent), or personal data of a person with disability (from the lawful guardian) who has a lawful guardian, in a form as may be prescribed.[59]

Under the DPDPA, a 'child' is an individual below eighteen years.[60] However, the DPDPA does not require data fiduciaries to undertake KYC to determine if a user is in fact a child. It is also unclear how data fiduciaries will ascertain whether a person has a disability.

Accordingly, it is unclear whether the obligations in relation to processing of personal data of children, or persons with disability, would apply only upon users disclosing they are children or have disabilities.

Data fiduciaries processing personal data of children have to comply with additional obligations:

1. Data fiduciaries are prohibited from undertaking processing of personal data of children which is likely to cause detrimental effect to a child, as may be prescribed by the Central Government;[61]
2. Data fiduciaries are prohibited from, tracking and behaviorally monitoring children, and directing targeted advertising at them.[62]

However, Central Government may exempt data fiduciaries from one or more of the above restrictions, in respect of children above a certain age, if it is satisfied that a data fiduciary has ensured that processing of personal data of such children is done in a manner that is verifiably safe.[63] This exclusion may be limited to certain classes of data fiduciaries, and subject to specified conditions.

There appears to be a drafting error in the wording of the prohibition on tracking and targeted advertising, which is not linked to processing of personal data of a child, unlike the previous sub-section.

In any case, the Guidelines for the Prevention of Misleading Advertisements and Endorsements for Misleading Advertisements, 2022 ("**Misleading Ads Guidelines**") issued by the Central Consumer Protection Authority, already contain exhaustive provisions regulating advertisements that address or target children. The Misleading Ads Guidelines apply to all forms, format, or mediums of advertisements. The provisions under the Misleading Ad Guidelines, being a special law dealing with such DPDPA should be deleted.

11. Data Protection Board of India

An adjudicatory body - the Board - is proposed to be established under the DPDPA. The DPDPA provides that the Central Government will establish the Board as a body corporate and notify the effective date of establishment.[64] The Board will comprise a Chairperson and a certain number of members, which will be notified by the Central Government.

Civil courts are barred from entertaining suits or proceedings for any matter in respect of which the Board is empowered to adjudicate under the DPDPA. Courts are barred from granting injunctions in respect of any action taken or to be taken by the Board under the DPDPA.

The Board will function digitally as far as practicable, and will be digital by design in terms of receipt of complaints, hearings, pronouncement of decisions, and other functions, and adopt such techno-legal measures as may be prescribed.[65]

Other important aspects of the Board are discussed below:

1. Independence of the Board

While it is stated to be an 'independent body,' the composition of the Board, process of selection, removal, terms and conditions of appointment and services, are left to be prescribed by the Central Government. Chairperson, members, officers and employees of the Board are deemed to be public servants.

In addition, it may be noted that the chairperson appointed to manage the affairs of the Board, will be appointed by the Central Government, and the Central Government will determine the terms and conditions of service. Accordingly, the scope of the Board's independence in view of these provisions is unclear.

2. Qualifications of the Board Members

Typically, legislations creating statutory bodies specify the composition and qualifications of the members of the body as opposed to including it in the rules and regulations. However, save for providing that the Chairperson and Members shall be persons of ability, integrity and standing who possess special knowledge or practice experience in certain fields, and have at least one expert in the legal field, the DPDPA does not set out the qualifications of the Board members. Since the Board is proposed to perform an adjudicatory function it is recommended that the Board should comprise of at least one judicial person and also one technical member for every determination. Certain people are also disqualified from being members of the Board, such as if they have acquired a financial or other interest which may prejudicially affect their functions as a member.

12. Proceedings before the Board

Important aspects of conducting proceedings before the Board has been listed out below:

1. Power to inquire

Upon receipt of an intimation, complaint by a data principal or reference by the Central Government, the Board will determine whether there are sufficient grounds to proceed with an inquiry.[66] If it does not believe there are sufficient grounds, it may, for reasons recorded in writing, close the proceedings.

If the Board believes it has sufficient grounds to proceed with inquiry, it has powers to inquire into the affairs of any person to determine compliance with the DPDPA, after recording reasons in writing. The Board is required to follow principles of natural justice.

2. Powers of the Board during proceedings

The Board is vested with the same powers as a civil court to summon, receive evidence, and require production of data, books, etc., during proceedings.[67] The Board may also obtain the services of a police officer for discharge of its functions.

However, the Board cannot prevent access to any premises or take any equipment into custody that may adversely affect the day-to-day functioning of a person.

3. Orders passed by the Board

1. Interim Orders[68]: During the course of inquiry, the Board may issue interim orders if it believes necessary, for reasons recorded in writing and after giving the person concerned an opportunity of being heard.
2. Final Orders[69]: On completion of the inquiry, and after providing the persons an opportunity of being heard, the Board may, for reasons recorded in writing, either close the proceedings or impose monetary penalties. We have discussed the penalties which may be imposed by the Board in point 18 below.
3. Orders in case of data breaches[70]: Upon being intimidated by a data fiduciary that there has been a personal data breach, the Board may direct any urgent remedial or mitigation measures, in addition to inquiring and imposing penalties.
4. Orders referring parties to ADR[71]: The DPDPA encourages alternative dispute resolution mechanisms, and the Board is empowered to direct parties concerned to try mediation for resolving any dispute, if it believes complaints may be resolved through mediation.
5. Orders accepting voluntary undertakings[72]: The Board may accept voluntary undertakings. We have discussed this in point 14 below.

If the Board is of the opinion, at any point after receipt of a complaint, that the complaint is false or frivolous, it may issue a warning or impose costs on the complainant.[73]

It also has the power to issue directions for effective discharge of its functions.[74]

The Board may, upon receipt of a representation by an affected person or a Central Government representation,

modify, suspend, withdraw or cancel any direction, subject to imposition of conditions as it deems fit.[75]

4. Appeals

The Telecom Disputes Settlement and Appellate Tribunal ("**TDSAT**") (established under the Telecom Regulatory Authority of India Act, 1997) has been designated as the Appellate Tribunal under the DPDPA as well.[76] Any appeals from orders and directions of the Board will be required to be made before the TDSAT within 60 days from receipt of such order / direction, or a longer period if the TDSAT is satisfied that there was sufficient cause for the delay.[77] The manner and form of the appeal and the procedure to be followed by TDSAT will be prescribed through rules.

The TDSAT is empowered to, after providing parties to the appeal the opportunity of being heard, pass orders to confirm, modify, or set aside the order appealed against.[78]

The DPDPA also requires the TDSAT to adjudicate on the appeal as expeditiously as possible, and endeavor to dispose of the appeal finally within 6 months from the date that the appeal is presented before it.[79] If there is a delay beyond this period, the TDSAT is required to record its reasons in writing for the delay.[80] Interestingly, the TDSAT is required to function as a "digital office" such that receipt of appeal, hearing, and pronouncements of decisions are "digital by design", i.e., conducted in online or digital mode.[81]

The TDSAT's order will be considered as a decree of a civil court, and for execution purposes, the TDSAT will have the powers of a civil court.[82] The TDSAT may also transmit its orders to a civil court to execute. Appeals against any order of the TDSAT would be before the Supreme Court, and would be required to be made within 90 days of such order.

13. Voluntary Undertaking

The DPDPA also introduces the concept of 'voluntary undertaking.'[83] The Board may accept a voluntary undertaking in respect of any matter related to compliance with provisions of DPDPA from any person at any stage of complaint proceedings. The voluntary undertaking may require any person to take or refrain from taking certain actions.[84] The terms of the voluntary undertaking may also subsequently be varied by the Board.

The voluntary undertaking would operate as a bar on proceedings pertaining to the subject matter of the undertaking, unless a person fails to adhere to its terms. If a person does not adhere to the terms of the undertaking, such breach is treated as a breach of the DPDPA, and the Board may impose a penalty for such breach.[85]

The Board may also require such undertaking to be publicized.[86]

14. Personal Data Breaches

"Personal Data Breach" has been defined as any unauthorized processing of personal data or accidental disclosure, acquisition, sharing, use, alteration, destruction of or loss of access to personal data, **that compromises the confidentiality, integrity or availability of personal data**.[87]

The DPDPA obligates the data fiduciary or the data processor to notify the Board and the affected data principals in the event of a personal data breach.[88] The obligation to notify data principals does not exist under Indian law currently. It is unclear why both the Board as well as the data principal must be informed in the first instance. Ideally, the obligation should be limited to informing the Board, and upon the Board requiring notification to the data principal depending on the severity of the issue or the likely impact upon the data principal, they may be informed. Even if data principals are to be informed at the first instance, this should be limited to situations where certain action is required on part of the data principal for security, such as changing of password.

Currently, reporting obligations in case of "cyber security incidents" exist under the Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013 ("**2013 Rules**") and the recently introduced direction relating to "information security practices, procedures, prevention, response, and reporting of cyber incidents for Safe & Trusted Internet" issued by the Indian Computer Emergency Response Team ("**CERT-In**"). Under the Information Technology Act, 2000 ("IT Act"), CERT-In, which is a statutory body empowered to deal with cyber security issues, has the powers to issue guidelines, directions, etc. to entities in response to cyber security incidents. On a similar note, the DPDPA also empowers the Board to direct data fiduciaries to adopt urgent measures to remedy personal data breaches or mitigate harm caused to data principals and inquire into such breaches. Therefore, in cases of incidents reportable under both laws, an entity may need to not only report the breach to two statutory bodies but may also need to comply with directions issued by two separate bodies. Additionally, the question arises if the Board will have the expertise to understand the complexity of data breaches to be able to issue measures that will help remedy a breach or mitigate harm.

15. Furnishing of information and blocking powers

The Central Government has been empowered to require not only the Board but also any Data Fiduciary or intermediary to furnish information.[89]

No safeguards or guidance has been provided here such as on the nature of information that may be called for, the circumstances under which such information may be requested, or whether these entities can refuse to provide such information. These aspects should be provided expressly in the Act itself, while the procedure for making such requests may be prescribed in the rules, similar to the scheme under the IT Act.

Moreover, if the Board has (a) held a Data Fiduciary liable for penalty on more than two instances, and (b) is of the opinion that any information generated, hosted, stored, etc. on a computer resource, which enables such Data Fiduciary to carry out any activities for offering its goods or services to data principals in India, should be blocked in the interest of the general public, it may refer such matter to the Central Government.[90]

If the Central Government is satisfied it is necessary to block access to such information in the interest of the general public, it may, after providing such data fiduciary an opportunity to be heard, direct any Government agency or

intermediary to block access to such information. Intermediaries are expressly bound to comply with such blocking orders.

Under Section 69A, the Central Government is already authorised to direct intermediaries to block access to information on the certain specified grounds specified therein, which are relatable to the restrictions on freedom of speech and expression under Article 19(2) of the Constitution of India (however, these grounds do not include the interest of the general public). Intermediaries such as ISPs and TSPs have been directed in the past to block access to websites with unlawful content under Section 69A.

Under Article 19(6), the Central Government is also empowered to impose reasonable restrictions on the right to carry out occupation, trade and business, in the interest of the general public. Hence, reasonable restrictions can be imposed on data fiduciaries' rights to carry out occupation, trade and business in the interest of the general public.

The ambit of the ground "in the interest of the general public" appears vague and will have to be interpreted taking into account judicial precedents. For e.g., the Supreme Court has interpreted this phrase to include public health and morals, economic stability, prevention of fraud, and even implementation of the Directive Principles in Part IV of the Constitution of India. The Supreme Court has also held that Government policy in the public interest would override business interests. If there is no public interest purpose warranting blocking of websites in exercise of this provision, such blocking orders may be challenged.

16. Exclusion of jurisdiction of civil courts

The DPDPA expressly excludes the jurisdiction of civil courts to entertain any suit or proceeding which pertains to any matter for which the Board is empowered. Moreover, no court or any other authority has jurisdiction to issue injunctions with respect to any action taken or to be taken in pursuance of powers granted under the Act.[91]

17.Penalties

1. Quantum of Penalties and factors to be taken into account while imposing penalties

Upon the conduct of an inquiry, if the Board finds a breach of any provision of the DPDPA by a person to be significant, it may impose a monetary penalty as per the Schedule.[92] The Schedule prescribes different penalties for different types of breaches, with the maximum penalty of INR 2.5 billion (approx. USD 30 million) for failure by a Data Fiduciary in taking reasonable security safeguards to prevent personal data breach.[93] The failure to report a personal data breach entails a maximum penalty of INR 2 billion (approx. USD 24 million).[94] The Central Government may subsequently amend the schedule and increase penalties subject to a maximum of twice of the amounts specified.

While determining the amount of monetary penalty, the Board will have regard to factors[95] such as (a) the nature, gravity and duration of the breach, (b) the type and nature of personal data affected by the breach, (c) repetitive nature of the breach, (d) whether a person has realised a gain or avoided a loss as a result of the breach, (e) whether a person has taken any action to mitigate the effects of the breach, and the effectiveness of such steps, and (f) the likely impact of the penalty on the person.

2. Parties on whom penalties may be imposed

The DPDPA empowers the Board to impose penalties in the following scenarios and on the following parties:

a) On a data fiduciary, in respect of a personal data breach or a breach in observance of its obligations in relation to personal data, or exercise of data principal's rights.

b) On a consent manager, in respect of breach in observance of its obligations in relation to data principal's personal data, or breach of any condition of registration of the consent manager.

c) On an intermediary, for breach of its obligation to block access to information when directed to do so by the Central Government. The Board will inquire into such breach upon reference by the Central Government.

Unlike the previous drafts, the DPDPA does not enable affected data principals to seek compensation for breaches by data fiduciaries. This may disincentivize individuals from pursuing costly adjudication before the Board. The sums realised as penalties imposed by the Board, are required to be credited to the Consolidated Fund of India.

The Act should provide that the Board should publish guidance notes for determination of the quantum of penalties (to bring in transparency). Additionally, the reasoned decisions of the Board should be made publicly available.

18. Delegated Legislation

In total, Section 40 refers to twenty five matters with respect to which the Government has rule-making powers, and the list is not exhaustive.[96] Therefore, the scope of obligations and restrictions remains open ended for now. These aspects include form and manner of personal data breach notifications; registration and obligations of consent managers; parental consent for processing of personal data of children; composition of the Board; conduct of data protection impact assessments and audits etc. It is recommended that appropriate legislative guidance be provided for each rule making power.

The DPDPA contains a *memorandum regarding delegated legislation* which enumerates the matters still to be prescribed by the Central Government via rules under the DPDPA, which states that these are matters of detail and accordingly it is not practicable to provide them in the DPDPA itself. This has likely been inserted following criticism that the 2022 Bill left a lot to be covered by rules enacted under the main statute.

19. Timelines for Compliance and Conflict with Other Existing Laws

There are no specific timelines for compliance prescribed for the implementation of the DPDPA. This should have been clearly indicated, so that businesses can plan their compliances accordingly. It should also be clarified that the DPDPA will only apply prospectively.

The DPDPA states that in the event of any conflict between a provision of this Act and a provision of any other law for

the time being in force, the provision of this Act shall prevail to the extent of such conflict.[97]

There are sectoral laws which may be applicable in addition to the DPDPA. This may create confusion in terms of compliance. Hence, clarity is required in this regard.

Once the DPDPA is enacted, Section 43A of the IT Act (this provision provides for the compensation for failure to protect data and specifically, the SPDI Rules has been enacted for this purpose) will be omitted.[98] The DPDPA does not repeal Section 72A of the IT Act, which prescribes a penalty (including imprisonment and fines) for service providers disclosing personal information about a person without their consent, or in breach of contract, with intent to cause, or knowledge that such breach is likely to cause wrongful loss to the person, or wrongful gain to the service provider.

The DPDPA seeks to amend the Right to Information Act, 2005 ("**RTI Act**") which bars the disclosure of personal data if its disclosure has no relationship to any public activity or interest or if it would cause unwarranted invasion of the privacy of the individual, unless the larger public interest justifies the disclosure of such information.[99] Through the amendment, the qualification with respect to public activity and interest is removed, and accordingly, *any* information which relates to personal information will be exempted from disclosure obligations to a citizen under the RTI Act. [100]

– Technology Law Team

You can direct your queries or comments to dataprotection.nda@nishithdesai.com

---

[1]Section 2(t), DPDPA.

[2]Section 2(n), DPDPA.

[3]Section 3(a), DPDPA.

[4]The DPDPA defines data principal as the individual to whom the personal data relates and where such individual is — (i) a child, includes the parents or lawful guardian of such a child; (ii) a person with disability, includes her lawful guardian, acting on her behalf;

[5]Section 3(b), DPDPA.

[6]Section 4(2), DPDPA.

[7]Section 3(c), DPDPA

[8]Section 2(i), DPDPA.

[9]Section 2(j) DPDPA.

[10]Section 2(k), DPDPA.

[11]Section 5, DPDPA.

[12]Section 6, DPDPA.

[13]Section 5(2), DPDPA

[14]Section 6(1), DPDPA

[15]Section 6(1), DPDPA

[16]Section 6(2), DPDPA

[17]Section 5(3), DPDPA.

[18]Section 6(4), DPDPA

[19]Section 6(6), DPDPA

[20]Section 2(g), DPDPA.

[21]Section 6(7), DPDPA

[22]Section 6(8), DPDPA

[23]Section 7, DPDPA

[24]Section 8(4), DPDPA.

[25]Section 8(5), DPDPA.

[26]Section 8(7), DPDPA.

[27]Section 11, DPDPA.

[28]Section 12, DPDPA.

[29]Section 12(1), DPDPA.

[30]Section 12(2), DPDPA.

[31]Section 12(3), DPDPA.

[32]Section 12(3), DPDPA.

[33]Section 13(1), DPDPA.

[34]Section 14, DPDPA.

[35]Section 15, DPDPA.

[36]The Schedule, DPDPA.

[37]Section 177, IPC.

[38]Section8(2), DPDPA.

[39]Section 8, DPDPA.

[40]Section 8(1), DPDPA.

[41]Section 8(3), DPDPA.

[42]Section 8(5), DPDPA.

[43]Section 8(6), DPDPA.

[44]Section 8(9), DPDPA.

[45]Section 8(7), DPDPA.

[46]Section 10(1), DPDPA.

[47]Section 10(2)(a), DPDPA.

[48]Section 10(2)(b), DPDPA.

[49]Section 10(2)(c)(1), DPDPA.

[50]Section 17(1), DPDPA.

[51]Section 17 2(a), DPDPA.

[52]Section 17 2(b), DPDPA.

[53]Section 17(1)(d), DPDPA.

[54]Section 16, DPDPA.

[55]Section 17(4), DPDPA.

[56]Section 8(7), DPDPA.

[57]Section 16(1), DPDPA.

[58]Section 16(2), DPDPA.

[59]Section 9(1), DPDPA.

[60]Section 2(f), DPDPA.

[61]Section 9(2), DPDPA.

[62]Section 9(4), DPDPA.

[63]Section 9(5), DPDPA.

[64]Section 18, DPDPA.

[65]Section 28, DPDPA.

[66]Section 27(1)(a), DPDPA.

[67]Section 28(7), DPDPA.

[68]Section 28(10), DPDPA.

[69]Section 28(11), DPDPA.

[70]Section 27(1)(a), DPDPA.

[71]Section 31, DPDPA.

[72]Section 32(1), DPDPA.

[73]Section 28(12), DPDPA.

[74]Section 27(2), DPDPA.

[75]Section 27(3), DPDPA.

[76]Section 2(a), DPDPA.

[77]Section 29(2), DPDPA.

[78]Section 29(4), DPDPA.

[79]Section 29(6), DPDPA.

[80]Section 29(7), DPDPA.

[81]Section 29(10), DPDPA.

[82]Section 30(2), DPDPA.

[83]Section 32, DPDPA.

[84]Section 32(2), DPDPA.

[85]Section 32(5), DPDPA.

[86]Section 32(2), DPDPA.

[87]Section 2(u), DPDPA.

[88]Section 8(6), DPDPA.

[89]Section 37, DPDPA.

[90]Section 37(1), DPDPA.

[91]State of Orissa v. Radhey Shyam Meher, (1995) 1 SCC 652.

[92]Section 33(1), DPDPA.

[93]Section 33(1), DPDPA.

[94]Section 33(1), DPDPA.

[95]Section 33(2)(a), DPDPA.

[96]Section 40, DPDPA.

[97]Section 38(2), DPDPA.

[98]Section 44(2)(a), DPDPA.

[99]Section 44(3), DPDPA.

[100]Section 8(1), DPDPA.