DESAI & DIWANJI

The Digital Personal Data Protection Act, 2023

Mithali Kanchan

The Digital Personal Data Protection Act, 2023 (***DPDPA***) is a crucial legislative framework designed to oversee the processing and safeguarding of personal data. It received the assent of the President of India on 11 August 2023.

Object

The object of the DPDPA is processing of digital personal data in a manner that recognises both the right of individuals to protect their personal data and the need to process such personal data for lawful purposes and for matters connected therewith or incidental thereto.

Territorial & material scope

Its territorial scope[1] extends to (i) processing of data within the territory of India; and (ii) processing outside India in connection with any activity related to offering goods and services within India.

Its material scope[2] extends to (i) personal data that is collected in digitised form; and (ii) personal data that is collected in non-digital form and digitised subsequently.

- **Corporate and Commercial**
- **Regulatory and Compliance**
- **Technology**

www.desaidiwanji.com

Gurugram
Indore
Mumbai (Forbes)
Mumbai (Lentin)
New Delhi
Pune

[1] Section 3(a), DPDPA.
[2] Section 3(b), DPDPA.

Exempted personal data[3]

Personal data which is processed by individuals for any personal or domestic purpose, and personal data that is made available by (i) the Data Principal to whom such personal data relates; or (ii) any other person under obligation under legal obligation, is exempted and excluded from the ambit of the DPDPA.

Supersession

Upon implementation, the DPDPA will repeal Section 43A (*Compensation for failure to protect data*) of the Information Technology Act, 2000 and consequently, supersede the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011)[4].

Key definitions

The definitions[5] under the DPDPA which are fundamental to understanding its scope and provisions are:

1. '*Personal data*' is defined broadly to include any data about an individual who is identifiable by or in relation to such data.
2. '*Consent Manager*' means a person registered with the Data Protection Board (as constituted under the DPDPA), who acts as a single point of contact to enable a Data Principal to give, manage, review, and withdraw her consent through an accessible, transparent, and interoperable platform.
3. '*Digital personal data*' is defined to mean personal data in digital form.
4. '*Data Fiduciary*' is defined as any person who alone or in conjunction with other persons determines the purpose and means of processing personal data.
5. '*Significant Data Fiduciary*' means any Data Fiduciary or class of Data Fiduciaries as may be notified by the Central Government under Section 10 of the DPDPA.
6. '*Data Principal*' is the individual to whom the personal data relates. Where such individual is a child, it includes the parents or lawful guardian of such a child. Where such person is a person with disability, includes her lawful guardian, acting on her behalf.
7. '*Data Processor*' means any person who processes personal data on behalf of a Data Fiduciary.
8. '*Data* Protection *Officer*' means an individual appointed by the Significant Data Fiduciary under Section 10(2)(a) of the DPDPA.

Legal basis for processing personal data[6]

There are two grounds on which personal data may be processed under the DPDPA: 'consent' and 'certain legitimate uses'.

1. Consent[7]:
    - Freely given;
    - Specific;
    - Informed;
    - Unconditional;
    - Unambiguous; and
    - Clear affirmative action.

2. Certain Legitimate Uses[8]:
    - For the purpose for which the personal data has been voluntarily provided by the Data Principal;
    - For the purpose of provision/ issuance of a subsidy, benefit, service, certificate, licence or permit from the State/ its instrumentalities to provide or issue to the Data Principal as may be prescribed where (i) the Data Principal has previously consented to such personal data being processed; and (ii) such personal data is from any database, register, book or other document maintained;
    - For the purpose of performance of any function under any law or in the interest of sovereignty and integrity of India or security of the State;
    - For the purpose of fulfilment of any obligation under any law on any person relating to disclosure (in accordance with applicable law) of any information to the State or any of its instrumentalities;
    - For the purpose of compliance with any judgment or decree or order issued under any law or any judgment or order under any law relating to claims of a contractual or civil nature;
    - For the purpose of responding to a medical emergency involving threat to the life or immediate threat to the health Data Principal/ any other individual; and

[3] Section 3(c), DPDPA.
[4] The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 were promulgated in exercise of the powers conferred by Section 87(2)(ob) read with Section 43A of the Information Technology Act, 2000.
[5] Section 2, DPDPA.
[6] Section 4, DPDPA.
[7] Section 6, DPDPA.
[8] Section 7, DPDPA.

- For the purpose of taking measures to ensure safety of, or provide assistance or services to, any individual during any disaster[9], or any breakdown of public order.

Privacy notice

The Data Fiduciary processing personal data based on 'consent' of a Data Principal is required to serve a notice to such Data Principal[10]. Such privacy notice should:

1. Include details of personal data obtained;
2. Include purpose for which such personal data is being processed;
3. Include the manner in which the Data Principal can exercise their rights under the DPDPA;
4. Specify the modes through which the Data Principal can file complaints before the Data Protection Board (as constituted under the DPDPA); and
5. Be formulated in English or any of the 22 regional languages specified in the Constitution of India.

Data Protection Officer[11]

Significant Data Fiduciaries are required to appoint an India-based Data Protection Officer, responsible to the Board of Directors of such Significant Data Fiduciary, to represent the Significant Data Fiduciary under the provisions of the DPDPA. Such Data Protection Officer must be the point of contact for the grievance redressal mechanism to the Data Principals.

Compliance roadmap for Data Fiduciaries

1. Identify legal basis: Data Fiduciaries to determine the legal basis for processing personal data.
2. Consent management mechanism: Data Fiduciaries to obtain consent from Data Principals, wherever required, through a consent management mechanism to collect, maintain, track and update consent from Data Principals.
3. Implementation of technical/ security measures: Data Fiduciaries to develop and implement reasonable technical & organisation-wide security measures to safeguard personal data obtained from Data Principals and prevent personal data breach.

[9] Explanation to Section 7, DPDPA - *"Disaster" has the same meaning as assigned to it in Section 2(d) of the Disaster Management Act, 2005; or for the purposes of employment or those related to safeguarding the employer from loss or liability, such as prevention of corporate espionage, maintenance of confidentiality of trade secrets, intellectual property, classified information or provision of any service or benefit sought by a Data Principal who is an employee.*

[10] Section 5, DPDPA.

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

4. Provision of privacy notice[12]: Data Fiduciaries to provide a privacy notice while obtaining consent from Data Principals.
5. Rights request mechanism: Data Fiduciaries to deploy mechanisms to be able to respond to requests made by Data Principals to exercise their rights under the DPDPA, for example, for erasure of personal data.
6. Grievance redressal mechanism[13]: Data Fiduciaries to put in place a robust grievance redressal mechanism for management of queries received from Data Principals.
7. Complete erasure of personal data after expiry of purpose/ withdrawal of consent[14]: At the time of expiry of purpose for which personal data has been collected or at the time of withdrawal of such consent, Data Fiduciaries are required to erase such personal data or cause their Data Processors to erase such personal data.
8. Data breach management mechanism: Data Fiduciaries to notify the Data Protection Board (as constituted under the DPDPA) and each of the Data Principals in the prescribed form and in accordance with the prescribed timelines.
9. Execution of valid contracts with Data Processors: Data Fiduciaries may choose to hire, involve, use, or appoint a Data Processor to handle personal data on its behalf if necessary under a valid contract, to provide goods and services to the Data Principal[15].
10. Publish business contact information of a representative: Data Fiduciaries are required to publish business contact information of a person who is able to answer, on behalf of the Data Fiduciary, the Data Principal's questions about processing of their personal data[16].
11. Liaising with a Consent Manager[17]: Data Fiduciaries to collaborate with a registered Consent Manager appointed by the Data Protection Board (as constituted under the DPDPA) to facilitate consent-related requests from Data Principals.
12. Consent of children and persons with disability: Data Fiduciaries to secure verifiable consent of the parent of a child or the lawful guardian of a person with disability[18].

[12] Section 5, DPDPA.
[13] Section 8(10), DPDPA.
[14] Section 8(7), DPDPA.
[15] Section 8(1), DPDPA - *A Data Fiduciary shall, irrespective of any agreement to the contrary or failure of a Data Principal to carry out the duties provided under this Act, be responsible for complying with the provisions of this Act and the rules made thereunder in respect of any processing undertaken by it or on its behalf by a Data Processor.*
[16] Section 8(9), DPDPA.
[17] Section 6(7), DPDPA.
[18] Section 9(1), DPDPA.

13. Protection of children[19]: Data Fiduciaries to abstain from undertaking (i) processing of personal data that is likely to cause any detrimental effect on the well-being of a child; and (ii) tracking or behavioural monitoring of children or targeted advertising directed at children.

Additional compliances for Significant Data Fiduciaries

1. Appointment of a Data Protection Officer[20]: Significant Data Fiduciaries are required to appoint a Data Protection Officer.
2. Publish business contact information of a Data Protection Officer[21]: Significant Data Fiduciaries are required to publish business contact information of its appointed Data Protection Officer.
3. Appointment of independent data auditor: Significant Data Fiduciaries are required to carry out periodic data audits through an independent data auditor for evaluation of compliance of the Significant Data Fiduciary with the DPDPA[22].
4. Conduct audits[23]: Significant Data Fiduciaries to conduct (i) periodic Data Protection Impact Assessment, comprising a description of the rights of Data Principals and the purpose of processing of their personal data, assessment and management of the risk to the rights of the Data Principals; and (ii) periodic audit.

Rights of Data Principals

1. Right to access information about personal data[24]: Data Principals have the right to obtain confirmation from the Data Fiduciary regarding the following personal data processed: (i) summary of personal data; and (ii) identities of all Data Fiduciaries and Data Processors.
2. Right to correction and erasure of personal data[25]: Data Principals have the right to reach out to the Data Fiduciary in order to exercise their right to correct, complete, update and erase their personal data.
3. Right of grievance redressal[26]: The Data Fiduciary and Consent Manager are required to respond to the grievances of the Data Principals within the time period prescribed. On exhaustion of this remedy, the Data Principals have the right to approach the Data Protection Board (as constituted under the DPDPA).

[19] Section 9(2) and Section 9(3), DPDPA.
[20] Section 10(2)(a), DPDPA.
[21] Section 8(9), DPDPA.
[22] Section 10(2)(b), DPDPA.
[23] Section 10(2)(c), DPDPA.
[24] Section 11, DPDPA.
[25] Section 12, DPDPA.
[26] Section 13, DPDPA.

4. Right to nominate[27]: Data Principals have the right to nominate any other individual as their representative, who shall, in the event of death or incapacity of the Data Principal, exercise the rights of the Data Principal.
5. Right to withdraw consent[28]: Data Principals have the right to withdraw their consent at any time and ensure stoppage of processing of their personal data.

Duties of Data Principals[29]

1. Duty to comply with applicable laws: Data Principals have the obligation to comply with all the provisions of applicable laws while exercising their rights under the DPDPA.
2. Duty not to impersonate: Data Principals are obligated not impersonate another person while providing personal data to the Data Fiduciaries for a specified purpose.
3. Duty not to suppress material information: Data Principals cannot suppress any material information when submitting personal data for any document, unique identifier and government-issued address/ identity proof.
4. Duty to abstain from making frivolous complaints: Data Principals have the obligation not to file false or frivolous complaints with the Data Fiduciary or the Data Protection Board (as constituted under the DPDPA).
5. Duty to provide authentic information: Data Principals are obligated to furnish authentic and verifiable information to the Data Fiduciaries when exercising their right to correction or erasure of personal data.

Cross border transfers[30]

Under the DPDPA, cross border data transfers are generally permissible. The DPDPA shifts to a blacklisting approach from the erstwhile data localisation requirements. Data Fiduciaries can now transfer personal data to other countries unless the Central Government restricts the transfer of personal data to such countries vide a notification. Therefore, unless a country has been specifically identified by the Central Government, personal data can be freely transferred to different locations.

Punitive measures[31]

The DPDPA only prescribes financial penalties as punitive measures which range from ₹ 10,000 to ₹ 2,50,00,000. The penalties for non-compliance of the DPDPA are as follows:

[27] Section 14, DPDPA.
[28] Section 6(4), DPDPA.
[29] Section 15, DPDPA.
[30] Section 16, DPDPA.
[31] Section 13 read with the Schedule, DPDPA.

	Non-compliance	Penalties
1.	Failure to prevent a personal data breach	*Up to ₹ 250 crores*
2.	Failure to notify the breach to the Data Protection Board (as constituted under the DPDPA) and each of the Data Principals	*Up to ₹ 200 crores*
3.	Non-fulfilment of obligations by Data Fiduciary while processing children's personal data	*Up to ₹ 200 crores*
4.	Non-fulfilment of obligations by a Significant Data Fiduciary	*Up to ₹ 150 crores*
5.	Breach in observance of the duties by Data Principals	*Up to ₹ 10,000*
6.	Breach of any voluntary undertaking given to the (as constituted under the DPDPA)	*Penalty up to the extent applicable for the breach*
7.	Miscellaneous non-compliance with provisions of the DPDPA	*Up to ₹ 50 crores*

Conclusion

In conclusion, the DPDPA represents a significant milestone in India's regulatory environment for safeguarding of personal data. Notably, Data Fiduciaries face heightened compliance requirements, such as data audits, impact assessments and restrictions on marketing and advertisements. Further, what truly underscores the gravity of the DPDPA is its penalty framework which ensures all non-compliance is met with substantial fines. While this strengthens the position of Data Principals, it is imperative for organisations to acquaint themselves with the intricacies of the DPDPA, as non-compliance carries the risk of severe financial repercussions.