



NOTE ON DIGITAL PERSONAL DATA PROTECTION ACT, 2023

Objective. The primary purpose of The Digital Personal Data Protection Act, 2023 (“**DPDP Act**”) which was notified by the Central Government on August 11, 2023 is to regulate the processing of digital personal data and respect individuals' right to protect their data while recognising the necessity of processing and using such data for lawful purposes.

Important Definitions/Meaning.

- **Board** means the Data Protection Board of India established by the Central Government under the DPDP Act;
- **Data Fiduciary** means any Person who alone or in conjunction with other Persons determines the purpose and means of processing of Personal Data. Accordingly, if an entity collects Personal Data of Data Principals for a specified purpose and determines the manner in which such Personal Data should be processed digitally, then such entity shall be classified as a 'Data Fiduciary' and would have to comply with the obligations on Data Fiduciaries encapsulated under the DPDP Act;
- **Data Principal** means 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) an individual with disability, includes her lawful guardian, acting on her behalf;
- **Data Processor** means any person who processes personal data on behalf of a Data Fiduciary. Accordingly, if an entity only processes Personal Data on behalf of another entity, then the former entity would be categorised as a 'Data Processor'. In this case, the entity on whose behalf such former entity is processing such Personal Data, would be the Data Fiduciary;
- **Person** means and includes an individual; an HUF; a company; a firm; an association of persons or a body of individuals, whether incorporated or not; the State; and every artificial juristic person;
- **Personal Data** means any data by which an individual may be identified; and
- **Processing** means collecting, recording, organizing, structuring, storing, retrieving, using, sharing, disclosing, disseminating or any other wholly or partially automated operation on Personal Data.

Applicability of the DPDP Act.

- **Within India** - digital personal data, which is collected in digital form or non-digital data, which is digitized subsequently.
- **Extra territorial application (Overseas)** - digital personal data that is processed outside India, only if such processing is in connection with any activity related to offering of goods or services to Data Principals in India.
- **Exclusions** - The DPDP Act does not apply to: (i) personal data processed by an individual for any personal or domestic purpose; or (ii) personal data made publicly available by the Data Principal or any other Person under a legal obligation.

Principles for processing Personal Data.

- Personal Data should be processed only for a lawful purpose i.e., purpose which is not expressly forbidden by law, after obtaining the consent of the Data Principal.

Consent Requirement.

Legalite Advisors LLP

Legalite Advisors LLP | LLPIN : AAJ 8514 | Bar Council Reg. No. : MAH-LF-196/2018 |
E-mail : la.mumbai@legalite.co.in | Corporate office : 705, Simran Plaza, 7th Floor, Near 3rd & 4th Road Junction, Khar (West), Mumbai 400052, Maharashtra, India | 📞 : +91 9769022955/ +91 8454846257.

Helping business navigate the legal landscape



- **Notice** - The DPDP Act mandates explicit notice to be given before or at the time of seeking the consent or, in case where the consent was sought before the commencement of the DPDP Act, then as soon as practicable, a similar notice needs to be provided in a clear and plain language. The Data Principal should have the option to view the notice and consent form in English or in any other language specified in the Eighth Schedule of the Constitution of India (which includes Assamese, Bengali, Gujarati, Hindi, Kannada, Kashmiri, Konkani, Malayalam, Manipuri, Marathi, Nepali, Odia, Punjabi, Sanskrit, Sindhi, Tamil, Telugu, Urdu, Bodo, Santhali, Maithili and Dogri). This requirement may be difficult for some entities, such as online platforms which only support the English language but it aims at spreading maximum awareness amongst the Data Participants irrespective of what language they understand.

The notice should contain details about the Personal Data to be collected, the purpose of processing, and Data Principal's rights under the DPDP Act. The onus lies on the Data Fiduciary to prove that proper notice under the DPDP Act was given to the Data Principal and consent thereby was duly obtained. For individuals below 18 years of age, consent will be provided by their parents or the legal guardian. To comply with this provision, every Data Fiduciary will have to verify the age of everyone signing up for its services.

- **Withdrawal** - Consent may be withdrawn at any point in time. Such withdrawal of consent shall not affect the legality of the processing of Personal Data done before the said withdrawal. Data Fiduciary shall cease processing of the Personal Data after the withdrawal.
- **Legitimate Use (for processing without consent)** - Consent will not be required for 'legitimate uses' including: (i) specified purpose for which data has been provided by the Data Principal voluntarily, (ii) provision of benefit or service by the government, (iii) performance of any function by the government for the integrity, sovereignty and/or security of the government/India; (iv) fulfilling any obligations under the law; (v) compliance with any court order; (vi) responding to any medical emergency; (vii) taking any measures to provide medical treatment or health / assistance service during any disaster or breakdown of public order; and (viii) for the purpose of employment.
- **Consent Manager** – The DPDP Act recognizes the role of the 'Consent Manager', who is required to be registered with the Board, shall be accountable to the Data Principal and shall act on her behalf in such manner and subject to such obligations as may be prescribed.

Rights and Duties of the Data Principal.

- **Right to:** (i) obtain information about processing, (ii) seek correction and erasure of Personal Data, (iii) revoke consent for processing of Personal Data; (iv) nominate another Person as a consent manager to manage their data related requests and any individual to exercise rights in the event of death or incapacity, and (v) grievance redressal.
- **Duty to not:** (i) register a false or frivolous complaint, (ii) furnish any false particulars or impersonate another individual in specified cases; (iii) suppress any material information while providing Personal Data for any document, unique identifier, proof of identity or proof of address issued by the government or any of its instrumentalities. Violation of these duties will be punishable with a penalty of up to INR 10,000.

Legalite Advisors LLP

Legalite Advisors LLP | LLPIN : AAJ 8514 | Bar Council Reg. No. : MAH-LF-196/2018 |
E-mail : la.mumbai@legalite.co.in | Corporate office : 705, Simran Plaza, 7th Floor, Near 3rd & 4th Road Junction, Khar (West), Mumbai 400052, Maharashtra, India | 📞 : +91 9769022955/ +91 8454846257.

Helping business navigate the legal landscape



Obligations of the Data Fiduciary.

- To make reasonable efforts to ensure the accuracy and completeness of Personal Data to be processed,
- To implement appropriate technical and organizational measures to ensure effective observance of the provisions of the DPDP Act;
- To build reasonable security safeguards to prevent a data breach,
- To notify the Board and affected persons in the event of a breach,
- To erase Personal Data as soon as the purpose has been met and retention is not necessary for legal purposes (storage limitation) and that your Data Processor also erases any Personal Data of the Data Principal. In case of government entities, storage limitation and the right of the Data Principal to erasure will not apply;
- To publish the business contact information of the nominated data protection officer to address, on its behalf, the questions raised by the Data Principal about the processing of Personal Data; and
- To establish an effective mechanism to redress the grievances of Data Principals.

Significant Data Fiduciary (“SDF”).

- The Central Government may notify any Data Fiduciary as an SDF based on the assessment of relevant factors such as the volume and sensitivity of Personal Data processed, risk to the rights of Data Principal, the potential impact on the integrity of India, risk to electoral democracy, security of the state and public order.
- Such an SDF shall: appoint a Data Protection Officer, appoint an Independent Data Auditor, undertake compliance measures including data protection impact assessment.

Exemptions.

- Rights of the Data Principal and Obligations of Data Fiduciaries (except data security) will not apply in the following cases where:
- The processing of Personal Data is necessary for enforcing any legal right or claim or is to be done by any court or tribunal in India which is entrusted by law with the performance of any judicial or quasi-judicial or regulatory or supervisory function;
- Personal Data is processed in the interest of prevention, detection, investigation or prosecution of any offence;
- Personal Data of Data Principals not in India is processed pursuant to any contract entered into with any Person outside India by any Person based in India;
- The processing is necessary for a scheme of compromise or arrangement or merger or amalgamation of two or more companies or a reconstruction or otherwise of a company, approved by a court or tribunal, etc.
- The processing is to ascertain the financial information and assets and liabilities of any Person who has defaulted in payment due on account of a loan or advance taken from a financial institution, subject to such processing being in accordance with the provisions regarding disclosure of information or data under any applicable law.
- The Central Government, by notification, exempt the processing: (i) if to be done by government entities in the interest of the sovereignty, integrity and security of the state and public order, (ii) necessary for research, archiving, or statistical purposes; or (iii) as it deems reasonable.

Legalite Advisors LLP

Legalite Advisors LLP | LLPIN : AAJ 8514 | Bar Council Reg. No. : MAH-LF-196/2018 |
E-mail : la.mumbai@legalite.co.in | Corporate office : 705, Simran Plaza, 7th Floor, Near 3rd & 4th Road Junction, Khar (West), Mumbai 400052, Maharashtra, India | 📞 : +91 9769022955/ +91 8454846257.

Helping business navigate the legal landscape



Data Protection Board of India.

- The Central Government will establish an adjudicatory body - the Data Protection Board of India, which shall function as a digital office with the receipt of complaints and the allocation, hearing and pronouncement of decisions in respect of the same being digital by design, and adopt other prescribed techno-legal measures. The Board shall consist of chairperson and such other members as may be prescribed by Central Government. The Board members will be appointed for 2 (two) years and will be eligible for re-appointment.
- **Key functions of the Board** include monitoring compliance, carrying out investigations and adjudicating penalties, directing Data Fiduciaries to take necessary measures in the event of a data breach, and hearing grievances made by affected persons. The Board has the power, upon receipt of intimation or complaint of Personal Data breach, to direct any urgent remedial or mitigation measures, inquire into such breach, and impose penalty as provided in the DPDP Act.
- The Board shall take action after determining whether there are sufficient grounds to proceed, exercising the principles of natural justice and after recording reasons in writing. For the purposes of discharging its functions under the DPDP Act, the Board shall have the same powers as are vested in a civil court under the Code of Civil Procedure, 1908.
- If the Board is of the opinion that any complaint may be resolved by mediation, it may direct the parties concerned to attempt resolution of the dispute through such mediation by such mediator as the parties may mutually agree upon, or as provided for under any applicable law.
- Civil courts do not have the jurisdiction to hear matters that fall within the purview of the Board.

Appeal.

- The decisions of the Board can be appealed to Telecom Dispute Settlement and Appellate Tribunal (“**TDSAT**”) within a period of 60 (sixty) days from the date of receipt of the order together by such fee as may be prescribed.
- TDSAT shall send a copy of every order made by it to the Board and to the parties to the appeal.
- The appeal filed before TDSAT to be disposed off within 6 (six) months from the date on which the appeal is presented to it, and in case it is not possible then TDSAT shall record its reasons in writing for not disposing of the appeal within that period.
- An order passed by TDSAT under the DPDP Act shall be executable by it as a decree of civil court, and for this purpose, TDSAT shall have all the powers of a civil court. However, TDSAT may transmit any order made by it to a civil court having jurisdiction for execution thereof.

Penalties.

- **Monetary Penalty** - The DPDP Act specifies penalties for various offences with minimum as INR 50 crores and maximum as: (i) INR 200 crore for non-fulfilment of obligations for children, and (ii) INR 250 crore for failure to take security measures to prevent data breaches. Breach in observance of the duties of Data Principal shall lead to a penalty of INR 10,000.
- Penalties will be imposed by the Board after conducting an inquiry.

Legalite Advisors LLP

Legalite Advisors LLP | LLPIN : AAJ 8514 | Bar Council Reg. No. : MAH-LF-196/2018 |
E-mail : la.mumbai@legalite.co.in | Corporate office : 705, Simran Plaza, 7th Floor, Near 3rd & 4th Road Junction, Khar
(West), Mumbai 400052, Maharashtra, India | 📞 : +91 9769022955/ +91 8454846257.

Helping business navigate the legal landscape



- All sums realized by way of penalties imposed by the Board under the DPDP Act, shall be credited to the Consolidated Fund of India.

Special Provisions.

- The DPDP Act does not permit processing which is detrimental to well-being of a child or involves their tracking, behavioral monitoring or targeted advertising directed at children. The DPDP Act however has neither defined as to what constitutes 'detrimental effect' nor provided any guidance for determining such effect.
- The DPDP Act allows transfer of Personal Data outside India, except to the countries restricted by the Central Government through notification.
- No civil court shall have the jurisdiction to entertain any suit or proceeding in respect of any matter for which the Board is empowered under the provisions of the DPDP Act and no injunction shall be granted by any court or other authority in respect of any action taken or to be taken in pursuance of any power under the provisions of the DPDP Act.
- The DPDP Act has provided for amendments in the following statutes:
 - o Under the Telecom Regulatory Authority of India Act, 1997.
*In clause (c) of Section 14, for sub-clauses (i) and (ii), the following sub-clauses shall be substituted, namely:
the Appellate Tribunal under the Information Technology Act, 2000;
the Appellate Tribunal under the Airports Economic Regulatory Authority of India Act, 2008; and
the Appellate Tribunal under the Digital Personal Data Protection Act, 2023.*
 - o Under Information Technology Act, 2000.
*section 43A shall be omitted;
in section 81, in the proviso, after the words and figures "the Patents Act, 1970", the words and figures "or the Digital Personal Data Protection Act, 2023" shall be inserted; and
in section 87, in sub-section (2), clause (ob) shall be omitted.*
 - o Right to Information Act, 2005.
*In sub-section (1), for clause (j), the following clause shall be substituted, namely:
"(j) information which relates to personal information;"*

There are no specific timelines for compliance prescribed for the implementation of the DPDP Act. This should be clearly indicated, so that businesses can plan their compliances accordingly. The DPDP Act contains the term 'as may be prescribed' meaning that the scope of obligations and restrictions remains open ended for now and the effective implementation of the provisions of the DPDP Act can only be undertaken once rules are made under the DPDP Act or circulars/notifications are released under the DPDP Act from time to time. The organizations need to (i) revisit their protocols on data protection to align the same with DPDP Act (ii) implement a consent mechanism by making requisite alterations to the user interface of their digital platforms, for the same (iii) identify all third parties including Data Processors who are storing or processing Personal Data on behalf of an organisation. Requisite amendments need to be carried out in the third-party agreements/contracts with respect to their obligations and align the same with DPDP Act.

Legalite Advisors LLP

Legalite Advisors LLP | LLPIN : AAJ 8514 | **Bar Council Reg. No.** : MAH-LF-196/2018 |
E-mail : la.mumbai@legalite.co.in | **Corporate office** : 705, Simran Plaza, 7th Floor, Near 3rd & 4th Road Junction, Khar (West), Mumbai 400052, Maharashtra, India | 📞 : +91 9769022955/ +91 8454846257.

Helping business navigate the legal landscape