

# **DATA PROTECTION LAWS OF THE WORLD**

India



Downloaded: 9 May 2024

## INDIA



Last modified 9 January 2024

### LAW

Until recently, India did not have a standalone law or framework to govern data protection. The Information Technology Act, 2000 (**IT Act**) and rules notified thereunder formed the basis around which the data protection framework revolved. This included the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (**Privacy Rules**).

In 2017, a constitutional bench of nine judges of the Supreme Court of India in *Justice K. S. Puttaswamy (Retd.) v. Union of India* [Writ Petition No. 494/ 2012] upheld that privacy is a fundamental right, which is entrenched in Article 21 [Right to Life & Liberty] of the Constitution of India. This led to the process of formulation of a comprehensive data protection framework for India. After releasing different draft versions of a data protection legislation and considering the recommendations from different stakeholders, the Ministry of Electronics and Information Technology (**MeitY**), Government of India, released the draft of the Digital Personal Data Protection Bill in 2022 (**DPDP Bill**).

The version of the DPDP Bill which was eventually passed by both houses of the Indian Parliament marked a few significant changes to the original draft of the DPDP Bill. On August 11, 2023, the Government of India published that version as the Digital Personal Data Protection Act, 2023 (**DPDP Act**), which is now part of the personal data protection and regulatory regime in India. The DPDP Act introduces several compliances with respect to the collection, processing, storage and transfer of digital personal data. However, further actions on behalf of the Government may be required to make the DPDP Act effective, including notifying the rules and regulations required for effective implementation and enforcement of the DPDP Act. The DPDP Act is applicable only to personal data in digital form and does not regulate non-personal and non-digital data. Considering this, collection and handling of non-personal data is currently unregulated in India.

### Note

The DPDP Act has been drafted on the following principles:

- usage of personal data by an organization is to be done in a manner that is lawful, fair and transparent to the individuals concerned;
- usage of personal data is to be limited to the purpose for which it was collected;
- only those items of personal data that are required for attaining a specific purpose are to be collected;
- reasonable efforts should be made to ensure that the personal data of the individual is accurate and kept up to date;
- storage of data is required to be limited to such duration as is necessary for the stated purpose for which personal data was collected;
- reasonable safeguards are to be undertaken to ensure that there is no unauthorised collection or processing of personal data. This is intended to prevent personal data breach; and
- the person who decides the purpose and means of processing of personal data i.e. Data Fiduciary is accountable for such processing.

## Scope and Applicability

The DPDP Act pertains to the processing of digital personal data within India, encompassing situations where the personal data is either (i) collected in a digital form or (ii) collected in a non-digitized form and subsequently converted into digital form.

Consequently, the DPDP Act does not apply to the processing of personal data in its non-digitized state. The DPDP Act defines **personal data** broadly to include any data about an individual who is identifiable by or in relation to such data. It also defines **digital personal data** as personal data in digital form.

While the DPDP Act is applicable to Indian entities which engage in the processing of personal data, it also has extra-territorial applicability, applying to foreign entities who offer goods and services to Data Principals (as defined below) located within the territory of India and process personal data in connection to such activities. The DPDP Act does not apply to (i) personal data utilized by an individual for personal or domestic purposes or (ii) personal data deliberately made publicly accessible by either the Data Principal to whom the personal data relates or any other individual or entity mandated by law to disclose personal data to the public.

## DEFINITIONS

### Definition of personal data

Under the DPDP Act, Personal Data refers to data about an individual who is identifiable either by such data or in relation to such data. This implies that anonymized data or non-personal data will not be covered by the DPDP Act.

The DPDP Act also defines **Data Fiduciary**, **Data Processor** and **Data Principal**, among other concepts:

### Definition of Data Fiduciary

Similar to **Controller** as defined under the European Union's General Data Protection Regulation (**EU-GDPR**), the DPDP Act defines Data Fiduciary as an individual or entity that, either independently or in conjunction with others, determines the purpose and means of processing of personal data.

### Definition of Data Processor

Data Processor is defined as any person who processes personal data on behalf of a Data Fiduciary.

### Definition of Data Principal

Similar to **Data Subject** under the EU-GDPR, the DPDP Act defines Data Principal as individual to whom the personal data relates. When dealing with personal data of a child under the age of eighteen years, the term Data Principal encompasses the child's parents or legal guardian. Likewise, for persons with disabilities, it includes their legal guardian, who acts on their behalf. The DPDP Act seeks to only protect personal data of natural persons and does not include data of companies.

### Definition of Processing

The DPDP Act defines **processing** to mean a *wholly or partly automated operation or set of operations performed on digital personal data, and includes operations such as collection, recording, organisation, structuring, storage, adaptation, retrieval, use, alignment or combination, indexing, sharing, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction.* This definition closely aligns with the concept of **processing** as defined under the EU-GDPR. Nevertheless, it is important to note that while the EU-GDPR's definition encompasses both automated and specific non-automated processes, the DPDP Act confines the scope of processing solely to **automated** operations.

## NATIONAL DATA PROTECTION AUTHORITY

### Data Protection Board of India



The DPDP Act provides for the establishment of a Data Protection Board of India (**Board**), an independent body tasked with overseeing the implementation and enforcement of the DPDP Act. The Government of India is yet to establish the Board. The Board has been envisaged as an online complaint resolution mechanism, with all its proceedings being conducted online. Once established, the Board will conduct inquiries based on complaints, address personal data breaches, and issue directions and impose penalties for non-compliance. The Board is required to scrutinize the contravention, conduct an inquiry, and communicate its decision in writing. An appeal against any order of the Board will lie with the Telecom Disputes Settlement and Appellate Tribunal (TDSAT). Other civil courts are restricted from entertaining any suit or proceeding in respect of any matter for which the Board is empowered under the DPDP Act. Thereafter, a final appeal may be made to the Supreme Court of India. Hence, a three-tier appeal mechanism has been established under this regime.

## REGISTRATION

There is no registration requirement for Data Fiduciaries under the DPDP Act. However, Consent Managers are required to register themselves with the Board.

### Consent Managers

The DPDP Act provides for Consent Managers registered with the Board and defines them 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. A Data Principal may give, manage, review or withdraw their consent through a Consent Manager. Consent Managers are accountable to the Data Principal and act on behalf of the Data Principal in such manner and subject to obligations as may be prescribed. However, it is yet to be prescribed if all Data Fiduciaries are expected to integrate with the Consent Managers for seeking consent of the Data Principals and the way the Consent Manager is required to perform its functions. Additionally, the Board may impose penalties on Consent Managers, 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.

## DATA PROTECTION OFFICERS

Under the DPDP Act, Data Fiduciaries are required to appoint a contact person to address any questions that a Data Principal may have about the processing of their personal data. Significant Data Fiduciaries are required to appoint a Data Protection Officer for the same purpose. The Data Protection Officer is required to be based in India and will be responsible to the board of directors or any similar governing body of the Data Fiduciary. The Data Protection Officer will also be the point of contact for a Data Principal for the purpose of grievance redressal under the DPDP Act.

## COLLECTION & PROCESSING

### Legal Basis for Processing Personal Data

Under the DPDP Act, a Data Fiduciary can only process personal data for a lawful purpose and, barring limited exceptions as prescribed, is required to do so either on the basis of consent of a Data Principal or for certain legitimate uses.

### Consent and Notice

The DPDP Act requires Data Fiduciaries to provide notice and obtain consent from Data Principals on or before processing personal data. At the time of collecting the consent, a notice is required to be given to the Data Principal, conveying the following information:

- the personal data intended for processing and the purpose for such processing;
- the manner in which Data Principals can exercise their rights under the DPDP Act;
- the manner for filing a complaint with the Board; and
- the contact details of the Data Protection Officer or any other person responsible for responding to a Data Principal's requests to exercise their rights under the DPDP Act.

Data Fiduciaries are required to give an option to Data Principals to access the request for consent and the notice in English or any of the twenty-two (22) languages specified in the Eighth Schedule to the Constitution of India. The Government of India will prescribe the manner and form of the notice in subsequent legislations.

Under the DPDP Act, Data Fiduciaries may process personal data based on consent from Data Principals which is required to be:

- free, specific, informed, unconditional, and unambiguous;
- provided through clear affirmative action; and
- limited to the personal data that is necessary for the specified purpose.

Where a Data Principal has given consent to processing of their personal data prior to the commencement of the DPDP Act, the Data Fiduciary is required to provide notice containing the above details as soon as it is reasonably practicable;. The express timeline is yet to be prescribed.

## Legitimate Uses

The DPDP Act permits the processing of personal data for certain legitimate uses and in such cases, Data Fiduciaries are not required to provide prior or post-facto notice to or obtain consent from the Data Principals. The legitimate uses are as follows:

- where a Data Principal voluntarily provides their personal data to a Data Fiduciary and has not indicated to the Data Fiduciary that they do not consent to the use of their personal data;
- for the State or any of its instrumentalities to provide or issue benefits or services to Data Principals where:
  - the Data Principals have previously consented to the processing of their personal data for availing any benefits or services from the State or any of its instrumentalities; or
  - such personal data is available in digital form or in non-digital form and digitized subsequently from any database, register, book or other document maintained by the State or any of its instrumentalities;
- for the performance of any function by the State or any of its instrumentalities under any law currently in force in India or in the interest of sovereignty and integrity of India or security of the State;
- for compliance with any judgment or order issued under the law in force in India, or any judgement or order relating to contractual claims of a civil nature under any law in force outside India;
- responding to a medical emergency involving threat to life or immediate threat to health;
- for taking measures to ensure safety of, or provide assistance or services to, any individual during disaster, or any breakdown of public order; and
- for purposes relating to employment or those related to safeguarding the employer from loss or liability.

## Retention of Personal Data

Data Fiduciaries are required to cease to retain personal data as soon as:

- it is reasonable to assume that the purpose for which personal data was collected is no longer being served;
- the Data Principal withdraws their consent; or
- upon a request for erasure by the Data Principal, unless retention of personal data is necessary under any other laws.

## Processing of Personal Data of Certain Classes of Individuals

The DPDP Act imposes additional obligations and responsibilities on Data Fiduciaries when they are processing the personal data of children and individuals with guardians. Data Fiduciaries, before processing the personal data of children or persons with disabilities, are required to obtain verifiable consent from a parent or legal guardian, as may be applicable. However, the procedure for obtaining such verifiable consent is yet to be prescribed.

While the DPDP Act explicitly defines a child as an individual below the age of eighteen years, it does not provide a definition for a person with a disability; However, reference may be made to the Rights of Persons with Disabilities Act, 2016 wherein this term is defined.

Specifically for children's data, a Data Fiduciary is required to refrain from:

- undertaking any processing that is likely to have a detrimental effect on the well-being of a child; and
- tracking, monitoring the behaviour of, or directing targeted advertisements at children.

These obligations related to children's data may be exempted by the Government under certain circumstances for prescribed purposes, class of Data Fiduciaries and for certain prescribed ages (further detailed in the section on Exemptions).

With respect to the processing of an employee's personal data, the DPDP Act considers it as a legitimate use wherein an employer will not have to obtain express consent in order to process personal data as long as the processing is carried out for employment purposes, or to protect employers from loss or liability, or to provide a benefit to an employee.

## Obligations of Data Fiduciaries

The DPDP Act prescribes certain obligations on Data Fiduciaries in collecting and processing personal data:

- complying with the DPDP Act in respect of any processing undertaken by a Data Fiduciary or on their behalf by a Data Processor, irrespective of any agreement to the contrary or failure of the Data Principal to carry out their duties provided under the DPDP Act;
- engaging a Data Processor to process personal data on its behalf only under a valid contract;
- implementing appropriate technical and organizational measures to ensure effective adherence with the provisions of the DPDP Act and any rules which may be notified;
- ensuring 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 to another Data Fiduciary;
- protecting all personal data in its possession or under its control by taking reasonable security safeguards to prevent personal data breach;
- in the event of a personal data breach, notifying the Board and each affected Data Principal;
- publishing the business contact information of the Data Protection Officer in the case of Significant Data Fiduciary, or the contact person who is able to answer Data Principals' questions regarding processing of their personal data;
- subject to compliance with other laws, deleting personal data by itself and ensuring such deletion by the Data Processor (if applicable), either when the Data Principal withdraws their consent or when it is reasonably assumed that the specified purpose is no longer being served, whichever is earlier; and
- establishing an effective grievance redressal mechanism to redress Data Principals' grievances.

## Obligations of Significant Data Fiduciaries

The Government of India may classify a Data Fiduciary, or a class of Data Fiduciaries as a Significant Data Fiduciary (SDF) based on certain factors like the volume and sensitivity of personal data processed, the risk posed to the rights of a Data Principal, the potential impact on the sovereignty and integrity of India, the risk to electoral democracy, security of the State, and public order. Upon getting notified as an SDF, entities are required to follow additional obligations:

- to designate a Data Protection Officer situated in India to serve as the SDF's representative for compliance with the DPDP Act and the primary point of contact for addressing grievances. The appointed person should be an individual responsible to the board of directors or a similar governing body of the SDFs.
- to appoint an independent data auditor to assess the SDF's compliance with the DPDP Act. The subordinate legislations under the DPDP Act will specify the periodicity for conducting such audits, and the technical and operational qualifying criteria for auditors.
- to undertake Data Protection Impact Assessments, periodic audits, and other measures that will be prescribed by the Government of India.

## Rights and Duties of Data Principals

Under the DPDP Act, Data Principals have been given certain rights which include:

- **Right to access information about personal data:** A Data Principal has the right to request a Data Fiduciary for a summary of their personal data being processed and the processing activities being undertaken by the Data Fiduciary. A Data Principal also has the right to request the Data Fiduciary for the identities of other Data Fiduciaries and Data Processors with whom their personal data is being shared and a description of the personal data being shared. The Government of India may prescribe any other information which a Data Principal has the right to request from a Data Fiduciary in subsequent legislations.
- **Right to correction of personal data:** A Data Principal has the right to request for correction of personal data that may be inaccurate or misleading, completion of personal data that is incomplete and updating of their personal data.
- **Right to erasure:** A Data Principal has the right to request for erasure of their personal data, the processing of which was previously consented to, unless retention is necessary for compliance with any laws.
- **Right to withdraw consent:** A Data Principal has the right to withdraw consent from processing of their personal data at any time after they have provided their consent to a Data Fiduciary.
- **Right of grievance redressal:** A Data Principal has the right to grievance redressal provided by a Data Fiduciary or a Consent Manager, which is exercisable in respect to a Data Fiduciary's obligations and a Data Principal's rights under the DPDP Act. The time period within which a Data Fiduciary or Consent Manager is required to respond to the grievances will be prescribed in subsequent legislations.
- **Right to nominate:** A Data Principal has the right to nominate any other individual to exercise the rights of a Data Principal on their behalf, in the event of their death or incapacity.

The right to access information, correction and erasure will apply only in cases where the Data Principal has given consent or voluntarily provided their personal data to a Data Fiduciary for processing. These rights will not be available where personal data is being processed under the grounds of legitimate use. The manner in which these rights are to be exercised by a Data Principal will be prescribed by the Government of India.

Under the DPDP Act, certain duties have also been assigned to Data Principals, which include:

- complying with all applicable laws while exercising their rights under the DPDP Act;
- prohibition of impersonation of others while providing their personal data for a specified purpose;
- not suppressing any material information while providing their personal data for any document, unique identifier, proof of identity or proof of address issued by the State or any of its instrumentalities;
- not registering false or frivolous grievances or complaints with a Data Fiduciary or the Board; and
- furnishing information that is verifiably authentic while exercising the right to correction or erasure.

## TRANSFER

Under the DPDP Act, transfer of personal data for the purpose of processing is permitted to any country or territory outside India, except to countries which have been specifically blacklisted by the Government of India. The list of countries to which cross-border data transfers are not permitted will be notified by the Government of India. Further, Data Fiduciaries may transfer personal data to another Data Fiduciary or Data Processor only under a valid contract.

While the DPDP Act does not provide any guidelines or requirements with respect to the contract regulating the data transfer, such data transfer agreements may contain adequate indemnity provisions for a third-party breach and may specify a mode of transfer that is adequately secured and safe. Additionally, the DPDP Act provides for certain indirect obligations on Data Processors which may be incorporated in the data transfer agreements. These include:

- implementing reasonable security safeguards to prevent personal data breach;
- reporting of personal data breaches to the Data Fiduciary;
- erasing personal data upon receiving a communication to that effect by the Data Fiduciary; and
- restricting transfer of personal data to countries which have been blacklisted by the Government of India.

## Data Localisation

While the DPDP Act itself does not provide for data localisation requirements, it recognizes that other sector-specific statutes and regulations may have restrictions on storing certain classes of data, which may include personal data.

India's central bank, the Reserve Bank of India (**RBI**) has made it mandatory from October 15, 2018, for all payment system providers and their service providers, intermediaries, third party vendors and other entities in the payment ecosystem to ensure that all data relating to payment systems operated by them are stored in a system only in India. Interestingly, by virtue of this regulation, RBI is seeking storage of all payment system data in India, which includes the entire payment processing cycle from request to final payout, such as customer data (name, mobile number, Aadhaar number, PAN number, etc.), payment sensitive data (customer and beneficiary account details), payment credentials (OTP, PIN, passwords, etc.), and transaction data (originating and destination information, transaction reference, timestamp, amount, etc.). However, for cross border transactions which consist of both foreign and domestic components, data pertaining to the foreign leg may be stored outside India. While data pertaining to the domestic leg should be stored in India, a copy may be stored abroad.

The Securities Exchange Board of India (**SEBI**) has issued an advisory for financial sector organizations such as merchant bankers, credit rating agencies, STP service providers, debenture trustee, depository participants and other financial institutions which are availing the Software as a Service (SaaS) based solution for managing their governance, risk and compliance functions. This advisory also lists certain critical data sets such as credit and liquidity risk data, market risk data, system and sub-system information, supplier information, system configuration data, audit / internal audit data, network topography and design, which must be stored in India. More recently, the SEBI has issued a Framework for Adoption of Cloud Services by regulated entities. If the regulated entities are engaging cloud service providers to conduct their business functions and any data pertaining to the regulated entities is on the cloud in any form, it is required to be stored within the legal boundaries of India. However, if the regulated entity has a foreign parent entity, the original data is required to be available and readily accessible in India. This implies that a copy of such data which is on the cloud may be stored abroad.

Separately, the Insurance Regulatory and Development Authority of India (Maintenance of Insurance Records) Regulations, 2015, require insurance providers to store data related to policies and claim records of insurers on systems in India (even if this data is held in an electronic form).

Additionally, while Section 128 of the Companies Act, 2013, requires every company to prepare and store, at its registered office, books of account, other relevant books and papers and financial statements for every financial year, on August 5, 2022, the Ministry of Corporate Affairs amended this rule whereby all such relevant books and papers maintained in an electronic mode are required to remain accessible in India, at all times.

Further, the Indian Computer Emergency Response Team (**Cert-In**), issued directions on information security practices, procedure, prevention, response and reporting of cyber incidents (Cyber Security Directions) dated April 28, 2022 (in force since June 28, 2022), and the frequently asked questions released on the Cyber Security Directions, require service providers offering services to users in the country to enable and maintain logs and records of financial transactions within India.

## SECURITY

Under the DPDP Act, Data Fiduciaries are required to protect the personal data under their control, with respect to any processing undertaken by them or on their behalf by a Data Processor, by taking reasonable security safeguards to prevent any kind of personal data breach. Notably, the highest quantum of financial penalty prescribed under the DPDP Act, being INR 250 Crores, is for failure on the part of a Data Fiduciary to take reasonable security safeguards to prevent personal data breach. Under the DPDP Act, there are no such prescribed standards or codes of best practices regarding security practices that have been recommended or mandated by the Government of India. It is possible that these standards and codes of best practice will be prescribed in due course.

In the absence of any guidance under the DPDP Act, the reasonable security practices and procedures may comply with the IS/ISO /IEC 27001 standard.

## Data Protection Impact Assessment

Under the DPDP Act, Significant Data Fiduciaries are required to appoint an independent data auditor who will undertake periodic Data Protection Impact Assessments, which has been described as a process comprising a description of the rights of



Data Principals and the purpose of processing their personal data. It also includes an assessment and management of the risks to the rights of Data Principals. The Government of India will elaborate on the process of conducting Data Protection Impact Assessments in subsequent legislations.

## BREACH NOTIFICATION

Under the DPDP Act, in the event of a personal data breach, Data Fiduciary is required to inform each affected Data Principal and the Board. The specific format and method of reporting is yet to be prescribed. Personal data breach is broadly defined under DPDP Act 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. Therefore, Data Fiduciaries are required to report all types of personal data breaches, regardless of the sensitivity of the breach or its impact on the Data Principal. Under the DPDP Act, neither materiality thresholds nor express timelines have been prescribed for the reporting requirement.

The DPDP Act is not the sole regulation imposing reporting requirement for data breaches. The existing cybersecurity framework also mandates reporting of cybersecurity incidents, which may include personal data breaches, to the Cert-In. In the absence of any conflicting information, both sets of regulations will be applicable.

The Government of India has established and authorized the Cert-In to collect, analyze and disseminate information on cyber incidents, provide forecasts and alerts of cybersecurity incidents, provide emergency measures for handling cybersecurity incidents and coordinate cyber incident response activities. The Information Technology (the Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013 (Cert-In Rules) along with the Cyber Security Directions impose mandatory notification requirements on service providers, intermediaries, data centers and corporate entities, upon the occurrence of certain cybersecurity incidents.

Cyber security incidents have been defined to mean any real or suspected adverse events, in relation to cybersecurity, that violate any explicitly or implicitly applicable security policy, resulting in:

- unauthorized access, denial or disruption of service;
- unauthorized use of a computer resource for processing or storage of information;
- changes to data or information without authorization.

Under the Cyber Security Directions, the occurrence of the following types of cybersecurity incidents are to be reported:

- targeted scanning / probing of critical networks / systems;
- compromise of critical systems / information;
- unauthorized access of IT systems / data;
- defacement of website or intrusion into a website and unauthorized changes such as inserting malicious code, links to external websites, etc;
- malicious code attacks such as spreading virus / worm / trojan / bots / spyware / ransomware / cryptominers;
- attack on servers such as databased, Mail and DNS and network devices such as routers;
- identity theft, spoofing and phishing attacks;
- denial of service and distributed denial of service attacks;
- attacks on critical infrastructure, SCADA and operation technology systems and wireless networks;
- attacks on applications such as e-governance, e-commerce, etc;
- data breach;
- data leak;
- attacks on internet of things devices and associated systems, networks, software and servers;
- attacks or incident affects digital payment systems;
- attacks through malicious mobile applications;
- fake mobile applications;
- unauthorized access to social media accounts;
- attacks or malicious / suspicious activities affecting cloud computing systems / servers / software / applications;

- attacks or malicious / suspicious activities affecting systems / servers / networks / software / applications related to Big Data, block chain, virtual assets, virtual asset exchanges, custodian wallets, robotics, 3D and 4D printing, additive manufacturing, drones;
- attacks or malicious / suspicious activities affecting systems / servers / software / applications related to artificial intelligence and machine learning.

These incidents can be reported to Cert-In via (i) email ([incident@cert-in.org.in](mailto:incident@cert-in.org.in)), (ii) phone (1800-11-4949), or (iii) fax (1800-11-6969). The reporting methods and formats are available at [www.cert-in.org.in](http://www.cert-in.org.in) and will be updated from time to time. The compliance obligations under the Cyber Security Directions extend to all entities which have computer systems, networks and / or resources in India, irrespective of whether the entity is incorporated in or outside India.

Data Fiduciaries may review their data breach reporting protocols and assess each incident in accordance with the guidelines outlined in the DPDP Act and the Cert-In Rules to ascertain whether it necessitates reporting under either or both regulatory frameworks.

## ENFORCEMENT

Under the IT Act, civil penalties are prescribed. If an entity that possesses, manages or handles any sensitive personal information in a computer resource that it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures, and its negligence causes wrongful loss or wrongful gain to any person, the entity was liable for damages to the affected person(s). In the event of unlawful disclosure of personal information, the IT Act prescribes civil penalties which may extend up to INR 2,500,000 or approximately ₹27,455 (as at January 9, 2024).

Separately, the Cyber Security Directions have introduced penalty of a term of imprisonment extendable to 1 year or a fine up to INR 10,000,000 or approximately ₹109,822 (as at January 9, 2024), or both, for failure to provide information to Cert-In or non-compliance with the Cyber Security Directions.

Under the DPDP Act, civil monetary penalties on Data Fiduciaries ranging from INR 50,000,000 or approximately ₹5,498,135 to INR 2,500,000,000 or approximately ₹27,490,675 (as at January 9, 2024) have been prescribed for different contraventions. The DPDP Act also provides for a penalty of up to INR 10,000 or approximately ₹110 (as at January 9, 2024) for the contravention of duties by a Data Principal. The quantum of monetary penalty will be determined by the Board, taking into consideration the following factors:

- the nature, gravity, and duration of the breach;
- the type and nature of the personal data affected by the breach;
- repetitive nature of the breach;
- whether the person, as a result of the breach, has realised a gain or avoided any loss;
- whether the person took any action to mitigate the effects and consequences of the breach, and the timeliness and effectiveness of such action;
- whether the financial penalty to be imposed is proportionate and effective, having regard to the need to secure observance of and deter breach of the provisions of this Act; and
- the likely impact of the imposition of the financial penalty on the person.

The Government of India may amend the penalties that have been prescribed under the DPDP Act by issuing a notification in the future. However, the penalties cannot be modified to exceed double of the amount that has been specified under the DPDP Act currently. Therefore, financial penalty may not be more than INR 500 Crores even after amendment by the Government of India.

## Exemptions

The DPDP Act provides for exemptions from the application of certain provisions, which are available to Data Fiduciaries in certain circumstances:

- a. **Exemptions for certain Data Fiduciaries or class of Data Fiduciaries, including startups:** The Government of India will issue a notification exempting certain Data Fiduciaries or class of Data Fiduciaries, including startups, from certain provisions of the DPDP Act. This notification will be based on the volume and nature of personal data processed. Such Data Fiduciaries will not be required to comply with the following obligations:
- issuing a notice before seeking consent of a Data Principal;
  - ensuring the accuracy and completeness of personal data;
  - erasing personal data after the purpose for which it was collected is served;
  - obtaining verifiable parental consent before processing children's data and no behavioural tracking of children or targeted advertising directed at children;
  - the obligations applying to SDFs; and
  - providing a Data Principal with the right to information about their personal data.
- b. **Exemptions where personal data is processed for certain specified uses:** The DPDP Act exempts entities from complying with the provisions pertaining to obligations of Data Fiduciaries, rights and duties of Data Principals and transfer of personal data outside India in cases where:
- the processing of personal data is necessary for enforcement of any legal right or claim;
  - the processing of personal data is necessary to perform judicial or quasi-judicial, regulatory or supervisory functions by a court, tribunal or any other such body entrusted by the law to perform such functions;
  - the processing of personal data is necessary in the interest of prevention, investigation or prosecution for offences or contraventions of any law;
  - personal data of Data Principals who are not within the territory of India is processed by any person based in India, pursuant to a contract with any person outside the territory of India;
  - the processing of personal data is necessary for carrying out mergers, acquisitions and other such transactions between two or more companies which have been approved by a court, tribunal or any other competent authority; or
  - the processing of personal data is done in relation to debt-recovery activities.
- c. **Exemptions for research and statistical purposes:** The DPDP Act will not apply to the processing of personal data which is necessary to carry out research, archiving or statistical activities, provided that the personal data is not being used to take any decision specific to a Data Principal. The Government of India will prescribe the standards in accordance with which such processing is to be carried out.
- d. **Exemptions for the Government of India:** The DPDP Act will not apply to certain instrumentalities of the Government of India in the interest of sovereignty and integrity of India, security, friendly relations with foreign countries and maintenance of public order. The Government of India will notify the instrumentalities to which this exemption is available.

The Government of India may notify additional exemptions from the provisions of the DPDP Act for any Data Fiduciary or class of Data Fiduciaries in the following five years.

## ELECTRONIC MARKETING

Under the DPDP Act, Data Principals have the right to withdraw their consent and restrict their personal data from being processed by an entity for specified purposes such as email marketing. Furthermore, Data Fiduciaries are required to refrain from engaging in tracking or behavioral monitoring of children, as well as from conducting targeted advertising aimed at children.

However, in a related development, the Food Safety and Standards Authority of India (FSSAI) has made it mandatory for E-commerce FBOs (Food Business Operators) to obtain a license from the Central Licensing Authority. E-commerce FBO means any Food Business Operator carrying out any of the activities under section 3(n) of Food Safety & Standards Act, 2006, through the medium of e-commerce. Interestingly, section 3(n) covers the entire food chain as it defines 'food business'; as any undertaking, whether for-profit or not, and whether public or private, carrying out any of the activities related to any stage of manufacture, processing, packaging, storage, transportation, distribution of food, import and includes food services, catering services, sale of food or food ingredients. Similarly, another set of legal Rules being referred as 'E-commerce & the Legal Metrology (Packaged Commodities) Amendment Rules, 2017'; effective from January 1, 2018, has made it mandatory for e-commerce entities to ensure mandatory declarations about the commodity displayed on the digital and electronic network used for e-commerce transactions.

The consumer protection regime in India was recently overhauled by way of enactment of the Consumer Protection Act, 2019 (notified in July 2020) (**CPA 2019**). Under CPA 2019, sellers and service providers have the obligation to, among others, not engage in unfair trade practices including by way of misleading advertisements. Further, Consumer Protection (E-Commerce) Rules, 2020 (**E-Commerce Rules**) have been notified under the CPA to regulate e-commerce entities in India. An e-commerce entity has been defined to mean any person who owns, operates, or manages digital or electronic facility or platform for electronic commerce, but does not include a seller offering his goods or services for sale on a marketplace e-commerce entity. E-commerce entities are required to set up a proper grievance redressal mechanism and consumer complaints should be acknowledged by the grievance officer within a stipulated timeline. E-commerce entities are further required to, among others, provide information in relation to refund, exchange, warranty, delivery, mode of payment, fees and charges, grievance process and other relevant information on their platform. The price (total and a break-up) of goods or services should be mentioned clearly and misleading advertisements and misrepresentations are prohibited.

In June 2022, the Central Consumer Protection Authority (**CCPA**), issued Guidelines on Prevention of Misleading Advertisements and Endorsements for Misleading Advertisements, 2022 (**the Guidelines**). The Guidelines lay down the conditions for non-misleading and valid advertisements and conditions for bait advertisements. The Guidelines prohibit surrogate advertising, and also lay down conditions for advertisements targeted at children. Moreover, the Guidelines lay down the duties of manufacturers, service providers, advertisers, and advertising agencies.

In November 2023, the CCPA further issued Guidelines for Prevention and Regulation of Dark Patterns, 2023 (**Dark Pattern Guidelines**) to restrict the use of dark patterns or manipulative practices by online platforms in designing their user interface and user experience that impair user autonomy, influence decision making, and work to the detriment of users. The Dark Pattern Guidelines apply to sellers, advertisers, and all platforms that systematically offer goods and services in India. The Dark Pattern Guidelines list certain specified dark patterns that are prohibited, including practices such as false urgency, subscription trap or confirm shaming.

Further, the National Do Not Call (**NDNC**) Registry is effectively implemented by the Telecom Regulatory Authority of India (**TRAI**). TRAI has also established the Telecom Commercial Communication Customer Preference Portal, i.e. a national data base containing a list of the telephone numbers of all subscribers who have registered their preferences regarding the receipt of commercial communications. Telemarketing companies may lose their license for repeated violation of DNC norms.

## ONLINE PRIVACY

There is no regulation of cookies, behavioural advertising, or location data. However, this may include personal data and it is advisable to obtain user consent, such as by using appropriate disclaimers.

The IT Act contains both civil and criminal penalties and offences for a variety of computer crimes. Under the IT Act, if any person introduces or causes to be introduced, any computer contaminant (like viruses etc.), into any computer, computer system or computer network, they may be liable to pay damages to the affected person(s). Under the IT Act, a computer contaminant is defined as any set of computer instructions that are designed:

- to modify, destroy, record, or transmit data or programs residing within a computer, computer system or computer network, or
- by any means to usurp the normal operation of the computer, computer system or computer network.

Further, under the IT Act, any person, who fraudulently or dishonestly makes use of the electronic signature, password or any other unique identification feature of any other person, may be subject to a prison term of up to three years and a fine up to INR 100,000 or approximately ₹1,098 (as at January 9, 2024).

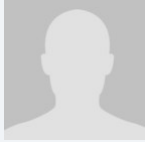
## KEY CONTACTS

**J. Sagar Associates**

[www.jsalaw.com/](http://www.jsalaw.com/)

**Sajai Singh**





Partner  
J. Sagar Associates  
T +91 80 435 03627  
sajai@jsalaw.com

## DATA PRIVACY TOOL

You may also be interested in our [Data Privacy Scorebox](#) to assess your organization's level of data protection maturity.

## Disclaimer

DLA Piper is a global law firm operating through various separate and distinct legal entities. Further details of these entities can be found at [www.dlapiper.com](http://www.dlapiper.com).

This publication is intended as a general overview and discussion of the subjects dealt with, and does not create a lawyer-client relationship. It is not intended to be, and should not be used as, a substitute for taking legal advice in any specific situation. DLA Piper will accept no responsibility for any actions taken or not taken on the basis of this publication.

This may qualify as 'Lawyer Advertising' requiring notice in some jurisdictions. Prior results do not guarantee a similar outcome.

Copyright © 2022 DLA Piper. All rights reserved.