

# India's New Law: The Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection Act, 2023 (the “**DPDP Act**” or “**Act**”), was published in the official gazette pursuant to a notification dated August 11, 2023, after approval of both houses of the Indian parliament and the President of India. The DPDP Act is not effective as of the date hereof. It will become effective from the date(s) notified by the Central Government (“**Government**”), and different dates may be notified for different provisions of the Act. Also, the Government may notify rules in future, not inconsistent with the provisions of the Act, to carry out the purposes of the Act.

The DPDP Act seeks to overhaul the current legal framework governing personal data, which is based on Section 43A of the Information Technology Act, 2000, along with rules framed under such provision (“**IT Rules**”). Rapid developments in digital technology, the absence of a specific data privacy law, and the Supreme Court of India’s judgement to classify privacy as a fundamental right under the Indian constitution are among the factors that led to the adoption of the new legislation.

The DPDP Act defines data, personal data and digital personal data. “Personal data” is defined broadly to mean any data about an individual who is identifiable by or in relation to such data, and “digital personal data” means personal data in digital form.

Unlike the IT Rules or the General Data Protection Regulation (“**GDPR**”) of the European Union, the DPDP Act does *not* classify data into ‘sensitive’ or ‘special’ categories. Instead, entities that process any digital personal data will be required to implement appropriate technical and organizational measures to ensure compliance with the new law. As long as such data remains in their possession or control, entities will remain responsible for protecting it, including in respect of separate processing tasks undertaken by data processors on their behalf.

The DPDP Act distinguishes among a data principal, data fiduciary and data processor:

1. a **data principal** is an individual to whom the personal data relates and includes the parents or lawful guardian of such individual if the individual is a ‘child’ (*i.e.*, a person less than 18 years) or a person with disability.
2. a **data fiduciary** is any person who alone or in conjunction with another person determines the purpose and means of processing of personal data.
3. a **data processor** is any person who processes personal data on behalf of a data fiduciary.

The DPDP Act applies to:

- the processing of digital personal data within the territory of India, where the personal data is collected in (i) digital form or (ii) non-digital form and digitized subsequently.

- the processing of digital personal data outside the territory of India, if such processing is in connection with any activity relating to the offering of goods and services to data principals within the territory of India.

The DPDP Act does not apply to:

- personal data processed by an individual for any personal or domestic purpose.
- personal data that is made or caused to be made publicly available by (i) the data principal to whom such personal data relates; or (ii) any other person who is under an obligation under any Indian law to make such personal data publicly available. As an example of the former, if an individual makes available their personal data while blogging their views, the provisions of the Act will not apply.
- the processing of personal data (i) by Government-notified state instrumentalities for reasons of national or public interest; or (ii) if it is necessary for research, archiving or statistical purposes as long as such data is not used to take any decision specific to a data principal and such processing remains consistent with prescribed standards.

The DPDP Act defines “processing” in relation to personal data to mean a wholly or partly automated operation (or set of operations) performed on digital personal data, and includes operations such as collection, storage, retrieval, use, sharing, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction.

In summary, the DPDP Act establishes a legal framework to protect digital personal data, including by prohibiting the unauthorized use, alteration or sharing of information in a way that compromises the confidentiality, integrity and/or accuracy of such data.

The Act provides rights for data principals and imposes obligations on data fiduciaries such as the following:

## Collection and processing

- Personal data can be processed only under the provisions of the Act and for a lawful purpose (i) for which the data principal has provided free, specific, informed, unconditional and unambiguous consent with a clear affirmative action, thus signifying an agreement to such processing for a specified purpose (where processing is limited to the data necessary for such purpose); or (ii) for certain legitimate uses.
- The Act sets out certain grounds or legitimate uses for disclosure or processing of personal data without the data principal’s consent. For example, personal data may be processed non-consensually for the purpose of employment, including to safeguard the employer from loss or liability, such as to: (i) prevent corporate espionage; (ii) maintain confidentiality, trade secrets, intellectual property, classified information; or (iii) provide any service or benefit sought by an employee. In addition, certain acts of processing related to state services and/or sovereign functions, public/national interest, mandatory legal disclosures or judicial obligations, medical or public health emergencies may constitute legitimate use.

## Notice and consent

- Where consent is the basis of processing, the data principal will have the right to withdraw such consent at any time, and the data fiduciary must ensure that withdrawing is as easy to do as the giving of consent.
- Every request for consent is required to contain certain specified information and must be presented in clear and plain language, including by giving data principals the option to access it in English or any language specified in the Eighth Schedule to the Constitution of India.
- Each request for consent must be preceded or accompanied by a notice that sets out certain specified information in a manner to be prescribed through rules, including the way which the data principal may make a complaint to the Data Protection Board of India (“**Board**”).
- Where the data principal has given consent prior to the commencement of the DPDP Act, the above notice is required to be sent as soon as reasonably practicable, although the data fiduciary may continue processing such data until the corresponding consent is withdrawn.

## Data Principals have Certain Rights, Including:

- accessing information about their personal data;
- having their personal data corrected or erased;
- accessing a grievance redressal mechanism; and
- nominating another person to exercise their rights in the event of death or incapacity.

## Transfer of Personal Data outside India

A transfer of personal data outside India is allowed except to countries/territories restricted by the Government through notification. However, the DPDP Act specifies that the provisions are in addition to, and not in derogation of, any other law in force. Therefore, other regulations may also apply to the transfer of data outside India. For instance:

- the Reserve Bank of India issued a directive in April 2018 with respect to the storage of payment system data, directing such data to be stored in a system located in India alone.
- the Securities and Exchange Board of India issued a circular in March 2023 in connection with the framework for adopting cloud services by regulated entities, which requires data to reside and be processed within the legal boundaries of India, subject to certain conditions.
- the Insurance Regulatory and Development Authority of India framed regulations in April 2017 related to the outsourcing of activities by Indian insurers, which require original policyholder records to be maintained in India.

## Data Fiduciaries have Certain Obligations Including:

- ensuring the completeness, accuracy and consistency of personal data;
- undertaking reasonable security safeguards to prevent a data breach;
- informing the Board and the affected data principal in the event of a breach; and

- erasing personal data as soon as the specified purpose has been met and retention is not necessary for legal purposes.

## Exemptions from Most Such Obligations may be Available in Cases of:

- enforcement of legal rights or claims;
- processing of personal data by a court, tribunal, or any other judicial or quasi-judicial body;
- prevention, detection, investigation or prosecution of an offence;
- a scheme of merger or amalgamation or demerger; and
- for defaults in payment due on account of a loan from a financial institution.

## Data Fiduciary and Data Processor

- In general, a data processor may be engaged by a data fiduciary to process personal data on the latter's behalf for any activity relating to the offering of goods or services to data principals under a valid contract.
- In case of processing of personal data of individuals outside India pursuant to a contract between a person resident in India and a person resident outside India, the obligations of data fiduciaries, the rights of data principals and restrictions on cross-border transfers under the DPDP Act will generally not apply.

## Significant data fiduciary

The Government has been empowered to notify any data fiduciary (or a class of data fiduciaries) as a 'Significant Data Fiduciary' ("**SDF**") pursuant to an assessment of factors prescribed under the DPDP Act, along with other factors as deemed necessary by the Government.

Additional obligations apply to SDFs such as appointing a data protection officer ("**DPO**") and an independent data auditor and undertaking periodic data protection impact assessments and audits. The DPO is required to be an individual based in India who will be responsible to the board of directors or similar governing body of the SDF for the purpose of representing such SDF under the provisions of the Act. These additional obligations will apply to SDFs over and above the general obligations which are applicable to all data fiduciaries.

## Processing children's data

While processing children's personal data, a data fiduciary is required to: (i) obtain verifiable parental consent (or consent of lawful guardian, where applicable); (ii) not undertake tracking, behavioral monitoring or targeted advertising; and (iii) not undertake processing of personal data which is likely to cause a detrimental effect on the well-being of a child. Under certain circumstances, the Government may lower the age limit for a particular data fiduciary.

## Administrative Framework

In terms of the administrative framework, the Board will be established by the Government, comprising technical and subject-matter experts. The Board can be approached by aggrieved individuals once options under the mandated grievance redressal mechanism have been exhausted. Decisions of the Board will be appealable to the Telecom Disputes Settlement and Appellate Tribunal (“TDSAT”), with a final appeal to the Supreme Court of India. The Board and the TDSAT are proposed to be ‘digital’ in design, as far as practicable. Further, the DPDP Act contemplates an alternative dispute resolution process conducted by mediators chosen by the disputing parties pursuant to mutual agreement.

Upon being informed by a data fiduciary about a personal data breach, the Board may direct any urgent remedial or mitigation measure. In addition, it has the power to inquire into breaches and impose penalties. The Board’s powers of inquiry (based on principles of natural justice) and imposition of penalty may get triggered pursuant to a complaint made by a data principal in respect of alleged instances of non-observance relating to a data fiduciary’s obligations, a reference made by the Government, or the directions of a court. After giving the person concerned an opportunity of being heard and after recording its reasons in writing, the Board may issue such binding directions as it may consider necessary.

For the purposes of discharging its functions under this Act, the Board will have the powers of a civil court in respect of matters relating to: (i) summoning and enforcing the attendance of any person and examining them on oath; (ii) receiving evidence of affidavit requiring the discovery and production of documents; (iii) inspecting any data, book, document, register, books of account or any other document; and (iv) such other matters as may be prescribed.

## Government Powers

The Government has given itself wide powers under the DPDP Act, ranging from:

- rule-making and legal immunity (subject to a ‘good faith’ qualifier);
- granting exemptions to, and imposing additional obligations upon, certain entities via notification on the basis of prescribed factors;
- setting up, and overseeing the operations of the DPBI;
- calling upon entities to provide information as deemed necessary;
- taking strict measures such as blocking commercial online platforms from public access when they are owned and/or operated by repeat offenders.

## Consent Manager

In addition to data principals, data fiduciaries and data processors, **consent managers** constitute another important entity category under the DPDP Act. Data principals will be allowed to give, manage, review or withdraw their consent through a consent manager, which is required to be registered with the Board to act as a single point of contact for providing consent-related options to multiple individuals through an interoperable platform. Consent managers will remain accountable to data principals, including through technical, operational, financial and other eligibility conditions pursuant to which their registration and duties will oblige them to provide grievance redressal options.

## Penalties

Monetary penalties for non-compliance can range from INR 10,000 to INR 2.5 billion, depending upon the contravention. If the Board determines upon conclusion of an inquiry that non-compliance by a person is significant, it may, after giving the person a reasonable opportunity of being heard, impose a monetary penalty as specified in the DPDP Act according to the nature of offence having regard to certain factors such as: (i) the nature, gravity, duration and repetitive nature of breach; (ii) the type and nature of the personal data affected by the breach; (iii) realization of gain or avoidance of loss as a result of the breach; (v) mitigation actions undertaken in respect of the breach; and (vi) proportion, likely impact and effectiveness of the monetary penalty. If an SDF fails to fulfil its additional obligations under the DPDP Act, a monetary penalty of up to INR 1.5 billion may be imposed.

## Conclusion

The DPDP Act defines both 'personal data' and 'processing' in broad terms. As a result, various partially automated operations that companies routinely perform on (or with respect to) digitized data are likely to come under the ambit of India's new law – even if such data is only indirectly related to specific individuals.

Organizations need to check whether and to what extent the Act applies to them and their operations. With respect to notice and consent requirements, they should be prepared to go back to individuals once the Act becomes effective. Organizations that collect, process and monetize personal data need to ascertain where, how and whose personal information is lodged within their systems. Although the provisions of the DPDP Act are not effective as yet, organizations also need to consider improving their information technology and cybersecurity systems to meet the new compliance requirements, including in respect of a breach. Relatedly, organizations will need to monitor entities in their supply chains, such as suppliers, about data processing obligations, and review existing contractual arrangements.

---

*This insight has been authored by **Sandip Bhagat** (Partner) and **Deborshi Barat** (Counsel). They can be reached at [sbhagat@snrlaw.in](mailto:sbhagat@snrlaw.in) and [d Barat@snrlaw.in](mailto:d Barat@snrlaw.in), respectively, for any questions. This insight is intended only as a general discussion of issues and is not intended for any solicitation of work. It should not be regarded as legal advice and no legal or business decision should be based on its content.*

© 2023 S&R Associates

**S&R**  
**ASSOCIATES**  
ADVOCATES



### NEW DELHI

64 Okhla Industrial Estate  
Phase III  
New Delhi 110 020  
Tel: +91 11 4069 8000

### MUMBAI

One World Center, 1403 Tower 2 B  
841 Senapati Bapat Marg, Lower Parel  
Mumbai 400 013  
Tel: +91 22 4302 8000