Data. Protection. Adding Value.

Data Protection Laws - India

Legislation

The Digital Personal Data Protection Act, 2023 ("**DPDPA**") has been enacted by the Government and published in the Official Gazette on August 11, 2023 - *CG-DL-E-12082023-248045*. This enactment is dedicated towards protecting the digital personal data of its citizens which highlights the significance of the Data Protection Board of India ("**DPBI**"), outlines essential provisions such as the rights and responsibilities of organizations that are handling the data and individuals whose data is being handled.

Risk Level: High

Scope: This Act applies to

- **Within the Indian Territory***:* Processing of digital personal data where the personal data is collected in digital form or in non-digital form which can be digitized subsequently; and
- **Outside the Indian Territory***:* Processing of digital personal data is in connection with any activity related to offering of goods or services to Data Principals ("**DP**") within the territory of India.

Exemptions: The DPDPA does not apply to

- Personal data processed by an individual for any personal or domestic purpose; and personal data that is made or caused to be made publicly available by the DP; and
- Any person who is under an obligation under any law to make such personal data publicly available.

Supervisory Authority & Enforcement

Supervisory Authority: The DPDPA provides for the establishment of a Data Protection Board of India ("**DPBI**") to be set up by the Government of India. Central Government will notify of the establishment of the DPBI. The DPBI will consist of a chairperson and other members as determined by Central Government. Its responsibility will be to direct any urgent remedial/mitigation measures or impose penalties on occurrence of a personal data breach.

The DPDPA has been approved by the Parliament and is an enacted legislation today. The rules for the DPBI are anticipated to be released for public consultations. It is expected that thereafter the DPBI will be established. The Government will notify of the enforcement date.

Registration/Approval Requirements: No registration requirements have been prescribed by the DPDPA, yet.

Data Principal's Right and Duties

Data Principals have the following rights under the DPDPA in relation to the processing of their personal data:

- **Right to access information about personal data**
- **Right to correction and erasure of personal data**
- **Right of grievance redressal**
- **Right to nominate**
- **Right to deletion/be forgotten**

The DPDPA further introduces specific **duties** that the DP needs to fulfill. Based on this, the DP is required to ensure that it has **not suppressed** any material **information**, **impersonated** as another person, or registered a **false grievance** or complaint.

DPs are also required to furnish authentic information while providing their personal data.

Penalties

The DPDPA allows for the following fines to be issued:

Breach by Data Fiduciary ("**DF**") to take reasonable security safeguards to prevent personal data breach	Up to **USD 31.25 m**
Breach in observing the obligations to give the Board and affected DP when a personal data breach has occurred	Up to **USD 25 m**
Non-fulfilment of additional obligations in relation to childeren	Up to **USD 25 m**
Non-fulfilment of additional obligations of Significant Data Fiduciary ("**SDF**"):	Up to **USD 18.75 m**
Non-compliance with duties of DPs	Up to **USD 100**
Breach of any term of voluntary undertaking accepted by DPBI	Up to the extent applicable for the Breach for which DPBI was instituted
Any other non-compliance, not specifically listed above	Up to **USD 6.25 m**

Processing of Personal Data

Personal data can be processed for a **lawful purpose** for which **consent has been obtained** and for certain legitimate uses, as listed below:

- For a specific purpose for which the Data Principal voluntarily provides its data to the Data Fiduciary;
- To provide or issue a subsidy, benefit, service, certificate, license or permit by the State and the performance of any other legal functions of the state;
- To fulfill any legal obligation to disclose to the State;
- To comply with a judgement or order relating to claims of contractual or civil nature (e.g., recovery of debts etc.);
- In case of medical emergencies, for providing health treatments or services during any threat to public health, including epidemics and other outbreaks of disease;
- In case of disasters, breakdowns of public law order, in particular to provide assistance or services;
- For employment purposes (e.g., performance of the employment, feedbacks etc.), including safeguarding employers from loss or liability.

pwc

Obligations of the Data Fiduciary

Data Fiduciaries are required to:

- Ensure effective implementation of **appropriate technical and organizational measures**;
- Ensure **completeness, accuracy and consistency** of the personal data processed;
- **Prevent and report data breaches** to the DPBI and the affected DPs;
- Comply with the principle of **data minimization**;
- **Publish** business **contact information** of a Data Protection Officer or Grievance Officer on all relevant touchpoints;
- Establish an effective **grievance redressal mechanism**;
- Issue **privacy notices** to the relevant DPs;
- Ensure that it has **obtained consents** in clear and plain language for the purposes for which personal data is collected, where required.

Obligations of Significant Data Fiduciaries

The Central Government may classify any Data Fiduciary or class of Data Fiduciary as a Significant Data Fiduciary ("**SDF**") on the basis of the following parameters:

- Volume and sensitivity of personal data processed;
- Risk to the rights to the Data Principal and potential harm;
- Potential impact on the sovereignty and integrity of India;
- Risk to electoral democracy;
- Security of the State;
- Public order; and
- Such other factors, as it may consider necessary.

If a DF or class of DFs are identified as SDF's then certain mandatory obligations apply to such SDFs, namely, SDFs are require to appoint a **Data Protection Officer** and an independent **Data Auditor** for carrying out periodic data audits.

Security & Data Breaches

A **personal data breach** means under the DPDPA any unauthorized processing of personal data which includes any accidental disclosure, acquisition, sharing, use, alteration, destruction or loss of access to personal data. It essentially compromises the confidentiality, integrity or availability of personal data.

The DPBI has the power to inquire about the breach and direct any urgent remedial or mitigation measures and/ or impose penalties.

Service Provider & Cross-Border Transfers for processing

Processing of personal data outside India: Sector specific restrictions will continue to apply for cross border processing of personal data, if the sectoral law provides a higher degree of protection. Central Government may notify certain countries as blacklisted where processing of personal data will be restricted.

Localisation Requirements: There are no localization restrictions under the DPDPA.

To Watch

The enforcement of DPDPA will repeal section 43A and section 87 related to personal data under the Information Technology Act and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data of Information) Rules, 2011. The procedural rules to the enacted legislations are anticipated in the upcoming months. It is anticipated that the Central Government may open such rules for public consultations, prior to enforcing the legislation.

Let's connect to discuss how we can help:

Anshul Jain

Regulatory Services India, Partner

+91 9810306217

jain.anshul@pwc.com