



LAW & POLICY UPDATE

September 25, 2023



 www.hsalegal.com

 mail@hsalegal.com

 HSA Advocates

Compliances of key stakeholders under the Digital Personal Data Protection Act, 2023

Amidst the evolving landscape of data protection laws in India, the Digital Personal Data Protection Act, 2023 (**DPDP Act/Act**) stands as a landmark development. This Act was passed by both houses of parliament and received Presidential assent on August 11, 2023.

While the DPDP Act has been enacted, the provisions have not yet been notified in the Official Gazette. Till the provisions of the DPDP Act are brought into effect, the relevant provisions of Information Technology Act, 2000 and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, continue to regulate the collection, use, processing, and transfer of sensitive personal data or information.

This Act defines 3 key stakeholders (**Data Fiduciary**, **Data Processor** and **Data Principal**) and this note attempts to highlight the various compliance related obligations imposed on such stakeholders, and the penalties provided under the legislation.

Compliance by Data Fiduciary

- **Definition:** An entity or individual that either independently or in collaboration with others, collects, stores, processes, or manages and determines the purpose and means of processing digital personal data of Data Principals whether originally in digital form or subsequently digitized from non-digital form.
- **Compliances:** To ensure a seamless transition from the existing statutory framework to newly enacted DPDP Act, a phased implementation approach should be followed. This interim period presents a unique opportunity for Data Fiduciaries to diligently prepare themselves and align their practices with the DPDP Act before it comes into full effect. Following are the compliance obligations of Data Fiduciaries:
 - Identify and prepare a list of Data Processors. Once the list is prepared, ensure that contractual agreements are executed with Data Processors, which explicitly obligates the Data Processors to be compliant with the provisions of the DPDP Act.
 - Conduct a comprehensive review of present data privacy policies and processes, including purpose of data collection and data retention periods.
 - Adopt a novel consent management mechanism, offering an accessible, transparent, and interoperable platform to the Data Principals, managed by a registered Consent Manager. Data Fiduciaries should also ensure that such consent mechanism facilitates seamless withdrawal of consent as well.
 - Prepare notice for consent required to be given to each Data Principal, including *inter alia* the purpose for which personal data is proposed to be processed; various rights with respect to withdrawal of consent and grievance redressal mechanism; and the manner in which one can make a complaint to the Data Protection Board of India. Since, DPDP Act's applicability is retrospective with respect to notice for consent, Data Fiduciaries should, as soon as reasonably practicable, give through email, in-app notification, or other effective method information to all existing

Team HSA



Soumya De Mallik
Partner



Prithviraj Chauhan
Principal Associate



Unnati Goel
Associate

Data Principals, about the personal data already processed before the date of commencement of the DPDP Act.

- Establish a robust mechanism to address the various grievances of Data Principals. Proactively establish systems and procedures for handling requests for accessing, correcting, and erasing personal data.
 - Strengthen data security measures to protect personal data from breaches by including encryption, access controls, employee training on security practices, and regular security audits. Develop and formalize procedures for managing data privacy breaches effectively and in compliance with legal requirements.
 - Implement stringent data access controls within the organization and actively engage employees in data management practices.
 - Conduct internal assessments to determine whether Data Fiduciaries might qualify as significant data fiduciaries. If a business qualifies as a '**Significant Data Fiduciary**' based on the volume of personal data being processed, risk of harm to the consumers, public order, etc., such a business must undertake additional obligations like data impact assessments, appointment of Data Protection Officer based in India to represent the significant Data Fiduciary, appointment of an independent data auditor to carry out data audit. Starting this process early will streamline compliance once it becomes a mandate.
 - Develop technical capabilities to give option to the Data Principals to access the contents of the notice in English or any constitutionally recognized Indian language they are comfortable with and maintain records of these notices.
 - Adhere to purpose limitation and data minimization principles as fundamental aspects of data processing. Only required personal data should be collected, and it should only be collected and processed for specified, explicit, and legitimate purposes and not for any other purpose.
 - Adhere to the storage limitation principle, which will require Data Fiduciaries to regularly review data in their possession and methodically cleanse their databases, once the purpose for which it was collected is served.
- **Cross-border processing related compliance by Data Fiduciaries:** The DPDP Act provides for blacklisting of countries wherein the Central Government shall notify the list of countries where transfer of personal data for processing purposes by a Data Fiduciary shall be restricted. Following are few compliances which Data Fiduciaries operating in India will have to consider, in the context of the DPDP Act:
- Ensure that their data handling practices align with sector-specific data localization and processing requirements imposed by regulators such as Reserve Bank of India (**RBI**), Securities and Exchange Board of India (**SEBI**) and others.
 - Anticipate potential requirements related to data adequacy under the DPDP Act. Accordingly, prepare to assess the adequacy of data protection in the destination country and implement measures to meet the standards.
 - Explore the possibility of implementing private data protection measures such as standard contractual clauses or binding corporate rules, to ensure the security and privacy of data transferred to countries with less secure regulatory environments.
 - Evaluate the feasibility of data localization within India to minimize cross-border data transfers.
 - Familiarize organization with the principles and requirements of the EU's GDPR and align the data handling practices with GDPR standards, especially in areas such as Data Principal rights and consent mechanisms.

Compliance by Data Processor

- **Definition:** Person or third-party entity who process digital personal data on behalf of the Data Fiduciaries. It assumes a crucial role in the data processing ecosystem, as it carries out data-related activities delegated to it by the Data Fiduciary.
- **Compliances:** Though, DPDP Act does not specifically impose any obligations on the Data Processors, Data Fiduciaries might contractually delegate some of their obligations to the Data Processor through contractual agreements with Data Processors.

Compliance by Data Principal

- **Definition:** Individual to whom personal data relates to and includes a child 'along with the parents or lawful guardian of such a child' and a person with disability 'along with a lawful guardian acting on her behalf'.

- **Compliances:** Unlike privacy laws of other countries, while DPDP Act provides Data Principals rights such as the right to access information, right to correction and erasure of personal data, right to grievance redressal, right to nominate, etc., it also imposes few duties and obligations on them and if these obligations are not complied with, they can even be penalized. Following are the few compliance obligations of Data Principals:
 - Ensure not to impersonate another person while providing personal data for a specified purpose.
 - Ensure not to suppress any material information while providing personal data for any document, unique identifier, proof of identity or proof of address issued by the state or any of its instrumentalities.
 - Ensure not to register a false or frivolous grievance or complaint with a Data Fiduciary or the Data Protection Board of India.
 - Furnish only such information as is verifiably authentic while exercising the right to correction or erasure under the provisions of DPDP Act or the Rules made thereunder.

Penalties

Non-compliance with the provisions of the DPDP Act can have significant implications on the stakeholders. DPDP Act prescribes penalties in accordance with the subject matter of the breach including the nature, gravity and duration of the breach, the nature of affected personal data, the repetitiveness of the breach etc. The Data Protection Board of India, on receipt of an intimation of personal data breach shall conduct an inquiry and after being satisfied that the provisions of the DPDP Act or its Rules has been significantly breached, has the authority to impose monetary penalty as specified in the Schedule. For instance:

- The breach in obligation of a Data Fiduciary to take reasonable security safeguards to prevent personal data breach - up to INR 250 crore
- The breach in obligation of a Data Fiduciary to notify the Data Protection Board of India and affected Data Principals of a personal data breach - up to INR 200 crore
- The breach of additional obligations in relation to processing data of children - up to INR 200 crore
- Breach of additional obligations of significant Data Fiduciary - up to INR 150 crore
- The breach of an undertaking accepted by the Data Protection Board of India and given by a person against whom a proceeding has been initiated and for the breach of any other provisions of the DPDP Act - up to INR 50 crore

Even the Data Principals are subjected to penalty for breach in observance of their duties under the DPDP Act 'up to INR 10,000'. It is interesting to note that all sums realized by way of penalties under the DPDP Act, shall be credited to the Consolidated Fund of India.

HSA Viewpoint

In the digital age, embracing data protection is not just a legal requirement, it's a commitment to a secure digital future. The DPDP Act ushers in the first comprehensive law for the protection of digital personal data in India. All key stakeholders under this newly enacted law will have to adapt to the new set of requirements to meet their compliance thresholds.

By creating exclusions to its applicability (such as placing non-digital data or non-personal data outside its scope), exemptions in specific circumstances and leaving room for anticipation of the Rules framed thereunder, the DPDP Act provides scope for some deliberations. As recently as on September 20, 2023, the Union Minister of State for Skill Development & Entrepreneurship and Electronics & IT, Shri Rajeev Chandrasekhar, led the first digital India dialogue discussions with key industry stakeholders on the transition time needed for specific clauses of the law, inputs on the implementation of the compliance obligations and rule structures of the DPDP Act. It is anticipated that over the next 30 days, Draft Rules will be brought out under the DPDP Act, and the Data Protection Board of India will be formed.

Since it seems likely that the Ministry of Electronics & IT intends to move at a swift pace with the formation of the Data Protection Board of India, the rule making process and implementation process, stakeholders should accordingly be fleet-footed with their preparations to be compliant with the DPDP Act.