Data Protection and Cross-Border Data Transfer: Navigating Legal Compliance

Majmudar & Partners
INTERNATIONAL LAWYERS

96, Free Press House, Free Press Journal Road, Nariman Point, Mumbai 400 021, India
Other office in Bangalore
Integrated network offices in Chennai, Hyderabad and New Delhi

Introduction: Current Data Privacy Regime in India

- The Information Technology Act, 2000 and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 (**SPDI Rules**) regulate collection, storage, use, and handling of personal information and sensitive personal data or information (**SPDI**).

- Statutory requirements apply to entities in or outside India that process personal data either in India or use a computer, computer system, or computer network located in India.

- Statutory requirements include requirements to obtain prior consent of the data subject for use or transfer of SPDI, to publish a privacy policy, to designate a grievance officer, and to implement security practices.

- SPDI must be collected lawfully, only if necessary, and must be backed by prior consent of the provider. It must not be retained longer than necessary for its lawful purpose.

- SPDI can only be transferred or disclosed to third-parties if the third party has equivalent data protection standards and if such transfer/ disclosure has been consented to by the data subject or is necessary to perform a lawful contract between the recipient entity and the data subject.

DPDP Act: A New Era of Data Privacy in India

- The Digital Personal Data Protection Act, 2023 (**DPDP Act**) was enacted in 2023 to overhaul the data privacy regime in India. However, it has yet to be implemented.

- The draft Digital Personal Data Protection Rules, 2025 (**Draft DPDP Rules**) have been released for public comments and are expected to be notified shortly.

- Once implemented, the DPDP Act and the Draft DPDP Rules will replace the existing data protection framework.

- The DPDP Act and Draft DPDP Rules apply to the processing of digital personal data (whether collected online or offline and digitized subsequently) within the territory of India, and outside India if such processing is in connection with any activity related to the offering of goods or services to data principals in India.

- Extraterritorial reach impacts multinational companies and cloud service providers.

- Businesses dealing with Indian consumers are in scope, regardless of their physical location.

Obligations of Data Fiduciaries: Consent and Notice

- The DPDP Act permits data processing only after obtaining the consent of the data principal, or for certain legitimate uses. Data fiduciaries should provide notice to data fiduciaries when a request is made for obtaining their consent. Data fiduciaries should limit data collection to what is necessary and process data for the specified purpose in the notice.

- Consent should be free, specific, informed, unconditional and unambiguous with a clear affirmative action.

- Notices to data principals should be clear, in plain language, and available in English or any language listed in the Eighth Schedule of the Constitution of India.

- Notices must include:

    (i) itemized description of the personal data collected;
    (ii) specific purpose for processing;
    (iii) communication link for exercising rights; and
    (iv) details on withdrawing consent.

- Withdrawing consent should be as easy as giving it.

Obligations of Data Fiduciaries: Security Safeguards, Grievance Redressal, etc.

- Data fiduciaries should adopt reasonable data security safeguards to secure such personal data through encryption, obfuscation, masking, data backups, and monitoring.

- Data fiduciaries should intimate the data principal and the Data Protection Board of India (**Board**) in case of breach of personal data. Detailed breach report should also be provided to the Board within 72 hours.

- Data fiduciaries should cease and ensure within a reasonable time that any third parties/ data processors cease processing the personal data of a data principal, in case the data principal withdraws his/ her consent, except when required by law.

- Data fiduciaries should prominently publish on their website or app, and mention in every response to a communication for the exercise of data principal's rights under the DPDP Act, the business contact information of a person who can respond to queries of data principals.

- Data fiduciaries should establish an effective mechanism to redress the grievances of data principals.

Obligations of Data Fiduciaries: Data Erasure and Special Protections

- Data fiduciaries should provide for data erasure upon withdrawal of consent by provider, or when specified purpose of processing data is no longer served, unless retention is required by law.

- E-commerce, online gaming, and social media intermediaries must erase personal data after a specified period if the data principal does not interact or exercise their rights.

- Data principals should be notified 48 hours before erasure, allowing them to retain their data by logging in or exercising their rights.

- Children: Parental consent is required for processing data of anyone under 18. Verification of parent should be done through reliable details or digital tokens. Behavioural monitoring of children and targeted advertising directed at children is prohibited.

- Persons with disabilities: Lawful guardian's verifiable consent is required for processing data of persons with disabilities. Verification of guardian's appointment should be done by court or designated authority.

Obligations of Significant Data Fiduciaries

- Any data fiduciary or class of data fiduciaries may be designated as a SDF by the Central Government based on factors such as volume and sensitivity of data processed, risks to data principal's rights, potential impact on India's sovereignty, state security, and public order.

- SDFs have additional compliance obligations such as:

  (i) appoint a data protection officer in India;
  (ii) appoint an independent data auditor to carry out data audit to evaluate compliance of the SDF;
  (iii) conduct data protection impact assessments and periodic audits annually;
  (iv) submit a report to the Board containing the significant observations in the data protection impact assessments and the audit; and
  (v) verify that the algorithmic software used for processing personal data is not impairing data principal's rights.

Rights and Duties of Data Principals

- Data principals have the right to:

  (i) access information about their personal data;
  (ii) correct and erase their personal data. Data fiduciary should publish on its website or application, or both, the details of how a data principal may make a request for exercise of their rights;
  (iii) implement appropriate technical and organizational measures to process requests effectively;
  (iv) have readily available means of grievance redressal (websites/ applications should have grievance redressal timelines); and
  (v) nominate someone in case of their incapacity/death.

- Data principals have the duty to:

  (i) comply with applicable laws while exercising rights under the DPDP Act;
  (ii) not impersonate another person when providing personal data;
  (iii) not suppress material information when submitting data for government-issued documents or IDs;
  (iv) not file false or frivolous grievances with a data fiduciary or the Board; and
  (v) provide only verifiably authentic information when requesting correction or erasure of personal data.

Cross-Border Data Transfer

- SPDI Rules allowed for the transfer of sensitive data overseas as long as equivalent protections were in place in the destination country.
- The DPDP Act introduces a “negative list” approach: the Central Government will specify countries where personal data cannot be transferred.
- No blanket ban, but the Draft DPDP Rules propose a more restrictive approach; all classes of data processed by all data fiduciaries may be subject to government-set requirements for overseas transfer.
- The Draft DPDP Rules seem to expand the scope of restriction, rather than expanding the criteria on the basis of which restrictions will be imposed.
- Neither the DPDP Act nor the Draft DPDP Rules clarify the nature or scope of these potential restrictions.
- The DPDP Act operates alongside existing sector-specific regulations on cross-border data transfers that provide stricter data protection requirements. It does not supersede data protection requirements set by regulators such as the Reserve Bank of India and the Securities and Exchange Board of India.

Cross-Border Data Transfer: Challenges for Foreign Players

- Implications for multinational companies and cloud providers: may require local data centres or hybrid models to comply with data localization requirements.
- Businesses using global cloud infrastructure should be ready to comply with evolving restrictions.
- This could lead to increased compliance costs for foreign technology giants to invest in the creation of regional infrastructure in India to process and store data.
- Will confer competitive advantage to domestic players due to increase in compliance costs for foreign players and unequal access to consumer data.

Operational Challenges

- The DPDP Act places a significant compliance and operational burden on businesses, especially smaller firms.
- Focus on consent and individual rights empowers data principals but requires robust compliance frameworks.
- The law is still evolving, with Draft DPDP Rules under public consultation and open questions on implementation.
- Restrictions on cross-border data transfers may have potential for exclusive localization of personal data for SDFs, if so prescribed by the Central Government.

Conclusion

- The DPDP Act and Draft DPDP Rules are a blueprint for a privacy-first digital future in India.
- For businesses: invest in compliance, treat data as a valuable asset, and prioritize individual rights.
- For cloud providers: transfer data within the guardrails of the law.
- Data privacy is the foundation of digital trust, essential for India’s digital growth and global competitiveness.

Thank you

Majmudar & Partners

INTERNATIONAL LAWYERS

96, Free Press House, Free Press Journal Road, Nariman Point, Mumbai 400 021, India
Other office in Bangalore
Integrated network offices in Chennai, Hyderabad and New Delhi