A Roadmap to Personal Data Protection & Privacy in Asia

November 2023

MERITAS®

India

FIRM

Khaitan & Co LLP
www.khaitanco.com

CONTACT

Harsh Walia
Mumbai, India

Tel +91 11 4151 5454
walia@khaitanco.com

Khaitan & Co was founded in 1911 and is among India's oldest and most prestigious full-service law firms. It is also one of the largest, with 1000+ professionals and 230+ partners, counsels, and directors. The firm's teams, comprising a powerful mix of experienced senior lawyers and dynamic rising stars in Indian law, offer customized and pragmatic solutions that are best suited to their clients' specific requirements. The firm acts as a trusted advisor to leading business houses, multinational corporations, financial institutions, governments, and international law firms. From mergers and acquisitions to intellectual property, banking to taxation, capital markets to dispute resolution, and emerging areas like white-collar crime, data privacy, and competition law, the firm has strong capabilities and deep industry knowledge across practices. With offices in New Delhi, Noida, Mumbai, Bengaluru, Chennai, and Kolkata, the firm also has capabilities in overseas markets via its country-specific desks and robust working relationships with top international law firms across jurisdictions. The firm opened its first international office in Singapore in 2021.

1. What are the major personal data protection laws or regulations in your jurisdiction? Is there any cross-sector legislation, and does it prevail over sector-specific legislation or vice versa?

Presently, India does not have comprehensive data protection legislation. Such provisions are encapsulated in the Information Technology Act 2000 ("IT Act") and rules framed under it ("SPDI Rules") alongside sector-specific legislations that coexist and complement the IT Act.

Generally, sector-specific laws take precedence over broader general laws. However, they may be limited. Hence, the IT Act fills the gaps and ensures comprehensive data protection.

On August 11, 2023, the Digital Personal Data Protection Act, 2023 ("DPDP Act") was enacted. It will replace the framework under the IT Act and SPDI Rules once it formally comes into effect and prevails when in conflict with other data protection legislation.

2. Which regulatory authorities are responsible for the implementation and enforcement of personal information protection laws?

While there is currently no such overarching regulatory authority, the DPDP Act envisages the constitution of a Data Protection Board for such purposes.

3. How is "personal information"/"personal data" defined, and are there any categories of personal data that receive special or different protection (e.g., employees, minors, "sensitive" personal information, etc.)? If so, what are these categories, and can you summarize what special rules apply to these categories?

According to SPDI Rules, "personal information" ("PI") is any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available to a body corporate, is capable of identifying a person.

The SPDI Rules predominantly affords protection to "sensitive personal data or information" ("SPDI"), defined as PI relating to:

(i) password;

(ii) financial information such as bank account, credit card, debit card, or other payment instrument details;

(iii) physical, physiological, and mental health conditions;

(iv) sexual orientation;

(v) medical records and history;

(vi) biometric information; etc.

Information that is freely available or accessible in public domain or furnished under the Right to Information Act, 2005 or any other laws is excluded from the purview of SPDI.

Once effective, the DPDP Act will afford protection to all "personal data" in a digital form, except 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.

4. What are the key principles under the major personal data protection laws or regulations relating to personal data?

While the IT Act and the SPDI Rules do not expressly set out key principles for data protection, the following may be noted:

(a) Consent is the only lawful basis for collection of PI: Written consent (including by way of electronic means) is the only grounds for collection of SPDI.

(b) Transparency: Entities collecting SPDI must ensure that the provider of SPDI knows (i) that information is collected, (ii) the purpose for collection, (iii) the intended recipients of the information, and (iv) the name and address of the agency that is collecting the information and that the agency will retain such information.

(c) Purpose limitation: SPDI should not be collected unless for a lawful purpose connected with the function of the entity.

(d) Data minimization: SPDI should not be collected unless such collection is considered necessary for that purpose.

(e) Storage limitation: Entities holding the SPDI should not retain it for longer than is required for the purposes for which the information may lawfully be used or otherwise required under any other law.

The DPDP Act is also based on other principles such as usage of personal data in a lawful manner, using data only for the purpose it was collected for, accuracy of personal data, implementation of reasonable safeguards, and accountability of data fiduciaries.

5. Are there any formal registration compliance requirements that apply to all businesses (e.g., the appointment of data protection officers, registration of databases, etc.)?

There are no specific registration compliance requirements currently. However, general obligations for entities collecting or processing SPDI include designating a grievance officer and publishing their contact details, implementing reasonable security practices and procedures ("RSPP"), and conducting periodic audits. The DPDP Act also envisages the appointment of a Data Protection Officer and independent auditor for "significant data fiduciaries" (which are yet to be classified).

6. What obligations are there for organizations to establish compliance programs (e.g., legal and operational policies, contracts, etc.) relating to the processing, use, and disclosure of personal data?

Entities collecting and processing SPDI must provide a privacy policy to the data subjects and ensure that it is "available for view." The SPDI Rules prescribes that the privacy policy should be published on the entity's website and inform the provider of:

(a) information regarding type of personal information and SPDI collected;

(b) its practices and policies;

(c) any disclosure to third parties; and

(d) RSPP adopted by the entity.

For RSPP, the SPDI Rules recognize the international standard IS/ISO/IEC 27001 on "Information Technology – Security Techniques – Information Security Management System – Requirements" for implementation. Under the SPDI Rules, a comprehensive and documented information security program and policies containing managerial, technical, operational, and physical security control measures that are commensurate with the information assets being protected, must be prepared and implemented. These measures should be audited through an independent auditor at least once a year or when the entity undertakes significant upgradation of its process and infrastructure.

In comparison, the DPDP Act sets out more robust obligations for organizations depending on the role it undertakes. However, many aspects are yet to crystallize and the Government is expected to issue further rules/notification.

7. What restrictions, if any, are there on personal data being transferred to other jurisdictions? How would organizations generally address these restrictions?

Under the SPDI Rules, disclosure and transfer (including cross-border transfer) of SPDI is permitted where:

(a) SPDI is collected under a lawful contract and the provider of SPDI has given permission for disclosure to any third party; or

(b) disclosure is necessary for compliance with a legal obligation.

Third parties to whom SPDI is disclosed must not disclose it further.

Additionally, transfer (including cross-border transfer) of SPDI is allowed where:

(a) necessary for performance of a lawful contract between the entity and provider of SPDI or where the provider of SPDI has consented to such transfer; and

(b) the transferee/recipient entity ensures the same level of data protection as prescribed under SPDI Rules.

For the avoidance of doubt, there are no blanket restrictions under the IT Act, but certain sectoral laws may have data localization requirements.

Practically speaking, organizations should ensure that prior permission of the user is obtained for sharing their SPDI and suitable protective measures are undertaken before disclosure/transfer. Organizations may also contractually ensure that any entities/persons to whom any information is transferred afford the same level of data protection as prescribed under the SPDI Rules.

The DPDP Act currently permits processing of personal data outside India (unless restricted by the Government by notification), subject to general obligations under the DPDP Act.

8. What restrictions, if any, are there on using or re-using personal data for data analytics/innovation or in adopting new business solutions such as artificial intelligence or data analytics? How would organizations generally address these restrictions?

There are no specific restrictions on re-using personal data for data analytics or other similar purposes. However, the SPDI Rules require that SPDI be collected for a lawful purpose connected with the function or activity of the company, and collection is necessary for that purpose. Further, entities collecting SPDI are required to inform the provider of SPDI about the purpose for collection. The DPDP Act also sets out similar principles for the processing of personal data.

Hence, organizations intending to re-use personal data should inform the providers of information about the different purposes the data may be used for and seek appropriate consent.

9. What are the rights of an individual whose personal data is collected? Can they withdraw their consent, object to (and/or request deletion of) the retention of their personal data? If so, how?

The SPDI Rules sets out the rights of providers of SPDI. Notably, any entity collecting/processing SPDI (or other entities on its behalf) is required to inter alia provide an option to the provider of the information to:

(a) not provide the information sought to be collected; and

(b) withdraw consent (in writing) given previously.

Per the SPDI Rules, providers of information, upon request, must be permitted to review the information they provided, and personal information or SPDI found to be inaccurate or deficient shall be corrected or amended as feasible.

Although the SPDI Rules do not prescribe formal mechanisms for providers of SPDI to exercise their rights, they may typically be exercised by writing to the grievance officer designated by the entity.

While the SPDI Rules do not expressly envisage the right to erasure/right to be forgotten, the High Courts of various states in India have adopted contradicting views on the same. Several have recognized the right to be forgotten as a part of right to privacy of an individual, but some have also refused to enforce this right except in certain cases. Hence, the position on right to erasure/right to be forgotten remains unsettled.

Separately, the DPDP Act sets out extensive rights for data principals, including right to access information about personal data, right to correction and erasure of personal data, right to grievance redressal, and right to nominate. Where consent is the basis for processing of personal data, the data principals have the right to withdraw their consent at any time.

10. Are there any penalties, liabilities, or remedies if any of the personal information protection laws are violated?

Per the IT Act, an entity possessing, dealing, or handling any SPDI, who is negligent in implementing and maintaining RSPP and, as a result, causes wrongful loss or wrongful gain to any person will be liable to pay damages by way of compensation to the affected person.

Further, the IT Act prescribes imprisonment and imposition of fines for unauthorized disclosure of personal information with the intent to cause or knowing that it is likely to cause wrongful loss or wrongful gain.

However, the on-ground enforcement of these provisions has been rather bleak.

In contrast, the DPDP Act sets out hefty penalties depending on the nature of breach/non-compliance, and a more comprehensive dispute resolution and enforcement mechanism.

11. Is there mandatory data breach reporting in your jurisdiction? If so, could you summarize the thresholds that trigger reporting, what should be reported and to whom, and what timelines are required/expected?

The IT Act and SPDI Rules do not set out data breach reporting requirements.

However, there are such requirements under directions issued by the Indian Computer Emergency Response Team, pursuant to the IT Act. All entities are required to mandatorily report certain types of cyber incidents and cyber security incidents to Indian Computer Emergency Response Team within six hours of noticing such incident or being notified about such incident, in the prescribed manner. Additionally, there are breach reporting requirements under sectoral laws such as finance and insurance which prescribe different timelines and thresholds for breach reporting.

Further, under the DPDP Act, any "personal data breach" needs to be intimated to the Data Protection Board and each affected data principal in the manner as may be prescribed by the Government.

12. Are there any recent notable developments in your country or cases that you think are likely to affect data privacy/data protection in the future? Is there anything else you would like to highlight?

As noted above, the DPDP Act has been enacted, but has yet to take effect. The Government will likely prescribe a phase-wise rollout of the provisions of the DPDP Act over a period of time. Once effective, the DPDP Act will serve as a comprehensive framework for data protection in India and envisages more robust requirements for the processing of personal data.