An Overview of Data Privacy Laws in India: Key Features to Keep in Mind When Establishing a Business

Information Governance

Technology, Privacy, and eCommerce

volodyar / *Shutterstock.com*

Key Highlights

- With foreign players increasingly entering the Indian market, in-house counsel should understand the key features of India’s existing data protection framework and upcoming changes.
- There is increasing momentum to bolster India’s data privacy and data protection laws.
- In a significant departure from India’s current nascent data protection laws, the Indian government is expected to release dedicated data protection legislation soon.

Overview of India’s data privacy and protection framework

India’s move at making its foreign investment laws less restrictive has paved the way for the entry of foreign players. Global players opening shop in India bring with them superior global standards of data protection and data privacy. However, it is also imperative for them to be mindful of the unique local Indian law requirements. Any failure to follow the Indian legal requirements could trigger civil or criminal liabilities. Further, this could also entail irreparable loss of reputation.

> Global players opening shop in India bring with them superior global standards of data protection and data privacy.

While the concept of “data privacy” is not explicitly mentioned under Indian laws, courts of the country have, over time, entwined the concept of privacy with interpretation of right to life and personal liberty, as provided under Article 21 of the Constitution of India. The Supreme Court of India has upheld the right to privacy as a fundamental right under Article 21 of the Constitution, in the landmark decision of *Justice K.S. Puttaswamy v. Union of India*.

In this regard, though avenues under the law of torts and the Indian Penal Code 1860 always existed, the concepts of data privacy and data protection were given focused attention through provisions of the Indian Information Technology Act, 2000 (IT Act) after its amendments in 2009 (Information Technology (Amendment) Act 2008).

The Information Technology (Amendment) Act 2008, brought into existence provisions such as Section 43-A and Section 72-A.

- Section 43-A of the IT Act primarily focuses on the compensation for negligence in implementing and maintaining “reasonable security practices and procedures” in relation to “sensitive personal data or information."
- Section 72-A of the IT Act mandates punishment for disclosure of “personal information” in breach of lawful contract or without the consent of the information provider.

On 13 April 2011, the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 (Rules) were promulgated. Though the Rules attempted to elaborate further on the requirements of Section 43-A of the IT Act, their adoption gave rise to considerable amount of confusion, primarily because of certain drafting ambiguities. In order to remedy the situation, a press note was released by the Ministry of Communications and Information Technology on 24 August 2011. This press note clarified several provisions of the Rules.

Apart from the IT Act and the Rules, there are certain sectoral regulations and guidelines which also address various aspects of data privacy and data protection in India. For example, the financial regulator (Reserve Bank of India), the securities market regulator (Securities and Exchange Board of India), and the insurance sector regulator (Insurance Regulatory and Development Authority of India), all have prescribed various requirements in this regard, from time to time.

India’s proposed new data protection law

Recently, there has been considerable traction to enact a dedicated data protection legislation in India. In 2019, the Government of India presented the Personal Data Protection Bill, 2019 (PDP Bill) in the Parliament which was later referred to a Joint Parliamentary Committee (JPC) for detailed review. However, on 3 August 2022, the Ministry of Electronics and Information Technology (MeitY) withdrew the PDP Bill, as revised by the JPC. MeitY has stated its intention to release a fresh draft of the legislation by the next budget session of the Parliament in 2023.

For foreign entities, it may be relevant to note that the contours of this proposed legislation could provide for stricter compliance and granular obligations, as compared to India’s current data protection regime.

Thus, with the increasing sensitivity of the Indian legal system towards data protection and privacy, corporate houses seeking to establish business in India must adhere to the local data privacy and data protection laws.

Specifications for dealing with Sensitive Personal Data or Information (SPDI) in India

The following sections provide an overview of the data privacy and data protection requirements in relation to SPDI, as prescribed under Section 43-A of the IT Act and the Rules. They also cover the new cybersecurity incident reporting related requirements in India.

Sensitive Personal Data or Information (SPDI)

The Rules identify the following personal information as SPDI:

- Passwords;
- Financial information, such as bank account or credit card or debit card, or other payment instrument details;
- Physical, physiological, and mental health condition;
- Sexual orientation;
- Medical records and history;
- Biometric information;
- Any detail relating to the above as provided to corporate entity for providing service; and
- Any information received under the above by corporate entity for processing, or which is stored or processed under lawful contract or otherwise

Information that is freely available, accessible in the public domain, or available under the Right to Information Act 2005, is excluded from the definition of SPDI.

Reasonable security practices and procedures

Section 43-A of India's IT Act and the Rules compel business houses handling SPDI to review their contractual arrangements in order to ensure that their data security practices and procedures are on par with those that are stipulated under the law.

Section 43-A of the IT Act mandates following "reasonable security practices and procedures" in relation to SPDI. The International Standard IS/ISO/IEC 27001 relating to Information Technology-Security Techniques-Information Security Management System Requirements is one of the standards "Stipulated Standard") specified under the Rules that may be implemented by a corporate entity while handling SPDI.

If any industry association or entity follows any standard apart from the Stipulated Standard for data protection, they are required to get their codes (Codes) approved and notified (i.e., published) by the Government of India. Such corporate entities which have implemented the Stipulated Standard or Codes need to get the same certified or audited by an independent auditor approved by the Central Government. Further, an audit has to be carried out by such an auditor at least once a year or as and when there is a significant upgradation of processes and computer resources.

Collection of SPDI

Under the Rules, a corporate entity is required to obtain prior consent from the information provider regarding the purpose of usage of the SPDI. Such information should be collected only if it is essential and required for a lawful purpose connected with the functioning of the corporate entity.

The corporate entity is also required to take reasonable steps to ensure that the information provider has knowledge about the collection of information, the purpose of the collection of such information, the intended recipients and the name and address of the agency collecting and retaining the information. The information should be used only for the purpose for which it is collected and should not be retained for a period longer than what is required.

The corporate entity must allow the information provider the right to review or amend its SPDI and give the information provider an option to retract consent at any point of time, in relation to the information that has been so provided. In case of withdrawal of consent, the corporate entity has the option to not provide the goods or services for which the concerned information was sought.

Transfer of SPDI

A corporate entity may transfer SPDI to other corporate entities, located anywhere across the globe, provided that the transferee ensures the same or equal level of data protection that is adhered to by the corporate entity as per the Rules.

> A corporate entity may transfer SPDI to other corporate entities, located anywhere across the globe, provided that the transferee ensures the same or equal level of data protection that is adhered to by the corporate entity as per the Rules.

However, the transfer may be permitted only if it is necessary for the performance of a lawful contract between the corporate entity and information provider, or if such information provider has consented to such transfer. Additionally, there could be restrictions on the transfer of personal data to other jurisdictions under sectoral laws, regulations, or directives issued by sectoral regulators.

Disclosure to third party

The Rules specify that apart from the information sought by governmental agencies or under applicable legal provisions, a corporate entity is required to obtain permission from the information provider, prior to disclosure of such information to a third party, unless the disclosure has been agreed to in an agreement between the parties.

Privacy policy

The Rules mandate that a corporate entity handling SPDI shall provide a comprehensive privacy policy containing details such as the type of information collected, the purpose for the data collection, the disclosure policy, the security practices and procedures followed, etc. The privacy policy must be clearly published on the website of the corporate entity and must be made readily available to the information providers.

Grievance officer

The Rules provide that a corporate entity must address grievances of the information provider within a specified time. For this, a corporate entity must appoint a grievance officer to address such grievance within one month from receipt of the grievance.

India’s new cybersecurity and incident reporting regime

India's Computer Emergency Response Team (CERT-In) serves as the national agency for collection, analysis, and dissemination of information on cyber incidents, coordination of cyber incident response activities, providing emergency measures for handling cybersecurity incidents, etc. In an effort to strengthen cyber incident reporting and internet security, CERT-In has issued a direction on 28 April 2022 (Direction) under Section 70-B(6) of the IT Act.

As per the Direction, certain specified types of cyber incidents (such as targeted scanning/probing of critical networks/systems, compromise of critical systems/information, unauthorized access of IT systems/data etc.), must be reported to the CERT-In within six hours of noticing such incidents or being notified of such incidents. Further, the Direction provides for certain other obligations for entities, as described below:

- Mandatory synchronization of information and communications technology (ICT) system clocks;
- Appointment of a point of contact for liaising with CERT-In;
- Maintenance of ICT system logs within servers in India;
- Retention of specific customer details by data centers, virtual private server providers, cloud service providers, and virtual private network service providers; and
- Maintenance of Know-Your-Customer (KYC) records of customers and records of financial transactions by virtual asset service providers, virtual asset exchange providers, and custodian wallet providers.

The Direction took effect on 27 June 2022 and was extended until 25 September 2022 only for certain categories of entities, such as micro, medium, and small enterprises.

Conclusion

As India is increasingly becoming a prominent part of the global economy with ever burgeoning foreign investment, there is an unprecedented thrust now to upgrade the country's data privacy and data protection standards.

> As India is increasingly becoming a prominent part of the global economy with ever burgeoning foreign investment, there is an unprecedented thrust now to upgrade the country's data privacy and data protection standards.

The upcoming data protection law is expected to answer the long-pending demand in this regard and strengthen India's data protection regime. Further, sectoral regulations and India's new cybersecurity related directions have already brought to the forefront the changing legal paradigm in India. This is the right time for businesses, whether domestic or operating on a cross-border basis, to re-calibrate their legal and compliance approach in relation to data privacy and data protection in India.

Disclaimer: The information in any resource in this website should not be construed as legal advice or as a legal opinion on specific facts, and should not be considered representing the views of its authors, its authors' employers, its sponsors, and/or ACC. These resources are not intended as a definitive statement on the subject addressed. Rather, they are intended to serve as a tool providing practical guidance and references for the busy in-house practitioner and other readers.

Supratim Chakraborty

Partner, Corporate and Commercial Practice Group

Khaitan & Co

Chakraborty is a partner in the corporate and commercial practice group of Khaitan & Co. He specializes in corporate and commercial transactions such as mergers, acquisitions, joint ventures, and general corporate law advisory. Chakraborty has advised eminent clients in relation to information technology laws in India including data privacy and cybersecurity-related issues. He has been recognized as a Notable Practitioner in the IFLR 1000 2020, 2021, and 2022 Rankings. And he has been categorized as a Recommended Lawyer in the prestigious RSG India Report 2019. Chakraborty has also been recognized as Leading Individual in Legal 500 2021 and 2022 Rankings.?

Chakraborty is a member of ASSOCHAM’s National Council for FinTech, Digital Assets and Blockchain Technology. He has spearheaded some of the important stakeholder consultation meets / feedback sessions organized by industry associations on the draft Personal Data Protection Bill. Supratim holds a GDPR FAS Certification and DPO Certification.

Sumantra Bose

Principal Associate, Corporate and Data Privacy

Khaitan & Co.

Sumantra Bose is a principal associate in the Corporate and Data Privacy practice of Khaitan & Co. He has experience in advising domestic and international clients on data protection and cybersecurity laws in India. He has been extensively involved in advising in matters concerning core privacy aspects for major conglomerates having diverse businesses. Bose has been extensively involved in corporate acquisitions and investments in technology platforms and digital businesses. He has been named as a recommended lawyer in the 2021 and 2022 Legal 500 editions for Data Protection in India. ?

Bose has authored several articles on data privacy, protection for data guidance, practical law, in the American Bar Association section on international laws and prominent newspapers in India. He has also played an active part in the policy space and has been a part of the team involved in providing inputs to Vidhi Centre for Legal Policy regarding a concept note on reforming of the Indian Information Technology Act.