A GLOBAL ROADMAP TO PERSONAL DATA PROTECTION

Asia Pacific, Europe & USA

Second Edition

MERITAS®

LAW FIRMS WORLDWIDE

MERITAS®
LAW FIRMS WORLDWIDE

INDIA

FIRM PROFILE:

KHAITAN &CO
Advocates since 1911

Khaitan & Co is a heritage firm of lawyers advising leading business houses, multinational corporations, global investors, financial institutions and the government since 1911.

Service Philosophy
Our ambition is to be a respectable law firm providing efficient and courteous service, to act with fairness, integrity and diligence, to be socially responsible and to enjoy life.

Main Areas of Practice
- Banking and Finance
- Capital Markets
- Competition/Antitrust
- Corporate/Commercial advisory
- Data Privacy
- Dispute Resolution
- Energy, Infrastructure and Resources
- Employment, Labour & Benefits
- Environment Law
- Funds
- Intellectual Property
- Private Client and Trusts
- Real Estate
- Tax
- Technology, Media & Telecom
- White Collar Crime

Data Privacy: The firm has a robust data privacy practice ranging from advice on legal requirements, review and drafting of documentation (contracts, notices and disclaimers) and processes, compliance assessment, and dispute resolution.

Local and International Experience
Khaitan & Co has widespread domestic and foreign clientele serviced from across locations – Mumbai, Delhi, Bengaluru and Kolkata.

CONTACT:

HARSH WALIA
harsh.walia@khaitanco.com

+91 22 6636 5000
www.Khaitanco.com

Introduction

At present, India does not have an exclusive and comprehensive data protection legislation. Certain provisions pertaining to data protection are incorporated in the Information Technology Act, 2000 (IT Act) and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (SPDI Rules) framed under the IT Act. Additionally, there are sector specific regulations, e.g. in relation to payment systems, telecom, healthcare etc. that stipulate certain obligations in relation to protection of personal data and information.

In recent times, the Government has laid considerable emphasis on the formulation of a comprehensive data protection legislation, which in many ways is a necessity in the present-day scenario and a key indicator for a country from the perspective of foreign investment and cross-border trade. This sentiment led to the formation of an expert committee for devising a data protection framework for India (Expert Committee), which was spearheaded by Justice (Retd.) B.N. Srikrishna. The Expert Committee released a draft of the Personal Data Protection Bill 2018 (Draft PDP Bill), which is being considered by the Indian Government at present. Earlier, in 2017, the 'right to privacy' was also declared by the Supreme Court of India as a fundamental right guaranteed by the Constitution of India, which has provided much needed impetus to this initiative.

1. What are the major personal information protection laws or regulations in your jurisdiction?

India currently does not have an exclusive legislation governing protection of personal data or information. Currently, the data protection framework is encapsulated under the provisions of the IT Act and SPDI Rules. Data protection related obligations are also incorporated in sector specific regulations, e.g. in relation to payment systems, telecom and healthcare etc.

It is important to point out that the IT Act and SPDI Rules broadly classify personal information under two categories, viz. 'personal information' (PI) and 'sensitive personal data or information' (SPDI) and afford different degrees of protection to each kind of personal information. The SPDI Rules primarily grant protection to the provider of SPDI and therefore we have provided our responses to all questions raised below from the perspective of SPDI only.

2. How is personal information defined?

Under the SPDI Rules, PI is defined as any information that relates to a natural person, which either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person.

Please note that the SPDI Rules primarily afford protection to SPDI and therefore, it is important to consider the definition of SPDI. SPDI is a subset of PI and means such "personal information which consists of information relating to (i) password (ii) financial information (iii) physical, physiological and mental health condition (iv) sexual orientation (v) medical records (vi) biometric information (vii) any detail relating to above as provided to a body corporate for providing services (viii) any of the information received under above clauses for processing, stored or processed under lawful contract or otherwise". The definition of SPDI excludes any information that is freely available or accessible in the public domain or furnished under the Right to Information Act, 2005 or any other law.

3. What are the key principles relating to personal information protection?

The provisions of the IT Act and SPDI Rules do not formally lay down principles relating to protection of PI and SPDI. However, certain conditions and requirements have been prescribed in cases where an entity collects, receives, possesses, stores, deals with, handles, discloses or transfers SPDI. We have touched upon these conditions and requirements in our responses to the questions raised below.

4. What are the compliance requirements for the collection of personal information?

The following sets out the mandatory compliance requirements for the collection of SPDI under the SPDI Rules:

- Conditions for collection: An entity or any person collecting SPDI on its behalf is required to obtain consent in writing (through letter, fax or email) from the provider of the SPDI regarding the purpose of usage before the collection of such information. Further, SPDI shall not be collected unless it is collected for a lawful purpose connected with the function or activity of the body corporate, and the collection of SPDI is considered necessary for that purpose.
- Safeguards for collection: At the time of collecting SPDI, the collector of SPDI must take reasonable steps to ensure that the provider of SPDI has knowledge of the fact that SPDI is being collected, the purpose for which it is being collected, who are the intended recipients of their SPDI and the name and address of the agency collecting and retaining their SPDI.

5. What are the compliance requirements for the processing, use and disclosure of personal information?

Please note that the IT Act and SPDI Rules do not define the term 'processing'. Generally speaking, the applicability of SPDI Rules is triggered when an entity or any person/ entity on behalf of such entity "collects, receives, possesses, stores, deals with or handles" SPDI. Bearing this in mind, please note the following compliance requirements under the SPDI Rules relating to "processing" and use of SPDI:

- Privacy Policy: According to the SPDI Rules, in case a body corporate (which means any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities) deals with or handles SPDI of any other person, then it must provide a privacy policy to providers of SPDI and ensure that the same is "available for view". The privacy policy must provide for the type of PI or SPDI collected by the entity, the purpose of collection and usage of such information, disclosure of information (including SPDI) and reasonable security practices and procedures implemented by the entity.
- Purpose limitation: Upon collection, a body corporate has to ensure that SPDI is used for the purpose for which it has been collected.
- Storage limitation: Further, SPDI should be retained by the body corporate only so long as it is necessary for the fulfilment of the specified purpose(s), unless the law requires retention of such information for a longer duration.

As far as disclosure of SPDI to third parties is concerned, please note that it is only permitted with the prior permission of the provider of SPDI, unless such disclosure has already been agreed to by the provider in the contract pursuant to which she/ he provides her/ his SPDI or where such disclosure is necessary for compliance of a legal obligation. The third party receiving the SPDI is not entitled to further disclose such information. Further, SPDI can be shared with government agencies (pursuant to a request made in writing) without prior consent from the provider of SPDI, for the purpose of verification of identity, or for prevention, detection, investigation including cyber incidents, prosecution and punishment of offences. As a part of the written request, the government agency shall also state that the information so obtained shall not be published or shared with any other person.

6. Are there any restrictions on personal information being transferred to other jurisdictions?

According to SPDI Rules, SPDI may be transferred by the body corporate collecting SPDI to any body corporate or person within India or any other country that ensures the same level of data protection that is adhered to by the former as provided in the SPDI Rules. Further, the transfer is allowed only if it is necessary for the performance of a lawful contract or where the provider of SPDI has consented to such data transfer.

Separately, please note that there are restrictions on transfer of certain types of data outside India under some sectoral regulations (which are applicable on payment system providers and telecom service providers). Therefore, to the extent such types of data comprise of PI and SPDI, it is possible that the transfer of PI and SPDI to other jurisdictions can be impacted.

7. What are the rights of an individual whose personal information is collected? Can he/she withdraw the consent to the retention of his/her personal information by a third party, and if so, how?

The provider of SPDI have the following rights under SPDI Rules:

- The right to be informed about (a) the fact that SPDI is being collected, (b) purpose for which it is being collected, (c) who are the intended recipients of their SPDI and (d) the name and address of the agency collecting and retaining their SPDI
- The right to review the information provided to collecting entities and the right to request for correction of any SPDI, found to be inaccurate or deficient
- The right to not provide any SPDI that is sought to be collected
- The right to withdraw her/ his consent that was provided earlier for use or retention of her/ his SPDI any time while availing the relevant services
- The right of redress of grievances in connection with the processing of her/ his SPDI

As noted above, the SPDI Rules do enable the provider of SPDI to withdraw her/his consent, which has been provided earlier. The notice of withdrawal must be in writing and can be sent at any time while availing the services. It is important to note that as a corollary, the body corporate will have an option to not provide goods and services for which the SPDI was sought after the provider has withdrawn her/ his consent.

8. Is an employee's personal information protected differently? If so, what's the difference? Apart from the personal information of employees, are there any other types of personal information that receive special protection?

No, there is no special provision for the protection of an employee's PI or SPDI. We have not come across any other types of personal information that receive special protection. However, it is possible that certain types of PI and SPDI are also regulated by sector specific regulations, to the extent that they form part of the data or information that is sought to be protected or covered by such sector specific regulation.

9. Which regulatory authorities are responsible for implementation and enforcement of personal information protection laws in your jurisdiction?

At present, there is no specifically constituted regulatory authority that is responsible for implementation and enforcement of laws relating to protection of personal information in India.

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

Yes, the IT Act prescribes certain penalties, liabilities and remedies in case of violation of relevant provisions relating to protection of PI and SPDI. The following may be noted in this regard:

- In case of negligence in implementing and maintaining reasonable security practices and procedures which results in wrongful loss or wrongful gain to any person, such entity shall be liable to pay damages by way of compensation to the person so affected.
- Any person who has secured access to any material containing PI about another person and who discloses such material to another person with the intent to cause or knowing that he/she is likely to cause wrongful loss or wrongful gain and without the consent of the person concerned, or in breach of a lawful contract, may be punished with imprisonment that may extend to three years, or with a fine which may extend to INR 500,000 (Indian Rupees five hundred thousand) or with both.

11. Is there any recent notable development(s) in India or cases which you think is likely to affect data privacy/data protection in the future? E.g. Is your jurisdiction planning to pass any new legislation to protect personal information? How is the area of personal information protection expected to develop in your jurisdiction?

Yes, a new, comprehensive personal data protection legislation is in the pipeline. The Expert Committee formed by the Government of India released the Draft PDP Bill in July 2018 after a process of public consultation. The efforts to create a robust data protection framework for India were catapulted by a landmark decision of the Supreme Court of India in 2017 (Privacy Judgment) where the right to privacy was declared as a fundamental right, guaranteed by the Constitution of India. In the Privacy Judgment, the Supreme Court emphasised on informational privacy and the importance of establishing a robust data protection regime for balancing of privacy interests of individuals with imperatives of the State and information needs of the economy.

The Draft PDP Bill is heavily inspired by the European Union's General Data Protection Regulation (GDPR) and aims to strengthen the data protection framework in India by introducing comparatively stringent requirements with respect to consent, cross-border transfer and disclosure to third parties. Some of the salient features of the Draft PDP Bill are set out below:

- Unlike the SPDI Rules (which primarily afford protection to SPDI), the Draft PDP Bill envisages protection to both 'personal data' (PD) as well as 'sensitive personal data' (SPD).
- The Draft PDP Bill postulates several core data protection principles such as fair and reasonable processing, purpose limitation, collection limitation, data quality, data storage limitation and accountability.

- The Draft PDP Bill provides certain grounds for processing of PD/ SPD, which include (i) consent, (ii) function of the State, (iii) prompt action (e.g. medical emergency or natural disasters), (iv) compliance with law or order/ judgment passed by a court, (v) employment (where obtaining consent is not appropriate or obtaining consent involves disproportionate efforts) and (vi) reasonable purposes that may be specified by the Data Protection Authority of India (DPAI).
- The Draft PDP Bill also grants certain unprecedented rights to data principals (such as right to data portability, right to erasure etc.). It also requires data fiduciaries and data processers to adhere to data transparency and accountability measures (such as implementing privacy by design, appointing data protection officers and conducting data protection impact assessments).
- The Draft PDP Bill prescribes comparatively stricter rules for cross border transfers and also imposes data localisation requirements in respect of certain types of PD and SPD.
- The Draft PDP Bill contemplates the constitution of DPAI for enforcement of the provisions of the Draft PDP Bill.
- The Draft PDP Bill envisages a stringent penalty scheme, which is in line with the provisions of the GDPR and also prescribes criminal penalties in respect of certain offences.

The Draft PDP Bill is likely to be presented in the lower house of the Indian Parliament soon, after undergoing minor modifications. In order to become law, the final version of the Draft PDP Bill will have to be passed by the lower and upper house of Parliament and thereafter receive the assent of the President of India. Further, if the Draft PDP Bill is enacted in its present form, its implementation will be carried out in a phase-wise manner, which will provide a moratorium to entities for re-engineering their practices and procedures to bring them in compliance with the new law. Some of the requirements laid down under the Draft PDP Bill are likely to have a significant impact on the cost of operations of entities.

In a follow up to the Privacy Judgment, the Supreme Court in another significant ruling in 2018 (Aadhaar Judgement) examined various principles of data protection (including data minimisation, purpose limitation, data retention and data security) and applied the same to uphold the legality of a Government sanctioned unique identification scheme, i.e. Aadhaar. Recently, the Telecom Disputes Settlement and Appellate Tribunal, which is also seized with the powers of the Cyber Appellate Tribunal, has also issued some rulings relating to payment of compensation for failure to protect data under the IT Act. Broadly speaking, courts in India have been relatively proactive in adjudicating cases that raise concerns of violation of data privacy and protection in recent times.

Conclusion

The legal framework relating to personal data and information protection in India is currently undergoing a meta-morphosis. The need for an effective data protection framework is imminent in the present day scenario, especially with increasing adoption of digital technologies. The existing legal framework, which is embodied in the IT Act and SPDI Rules, requires a major face-lift to meet the standards set by data protection legislations of other major countries. It is expected that the Draft PDP Bill, if enacted in its present form, will help bridge that gap. Consequently, it will also lead to additional compliances for entities and require them to undertake a thorough re-evaluation of their current data protection practices.