ANA LAW GROUP
ANOOP NARAYANAN & ASSOCIATES

INDIA TO ADOPT A NEW DATA PROTECTION REGIME

Introduction

The Supreme Court of India's recent landmark judgment has declared the right to data privacy as a fundamental right under the Indian Constitution. This judgment has also directed the Central (Federal) Government to create an exclusive stringent data protection regime, as the existing law is unable to keep up with the increasing digitization and e-commerce activities in India.

Please find below a complete overview of the existing data protection law in India and the anticipated positive effects of the Supreme Court's decision:

1. What is the legislative framework for data protection in India?

India has an omnibus data privacy law that is similar in many respects to the existing European Union (EU) data protection law. The obligations under the Indian data privacy regime which require the companies to provide privacy policies, restrict the processing of sensitive personal data, restrict international data transfers and require additional security measures, create some fundamental challenges for India's numerous information technology and other data processing vendors and their customers.

In India, personal and confidential information is protected under the Information Technology Act, 2000 (the "IT Act") and the IT Rules. The IT Act is based on the United Nations' resolution recommending all members to adopt the Model Law on Electronic Commerce adopted by the UNCITRAL. The IT Act, *inter alia*, addresses the data security concerns and provides for civil and criminal liability for breach or unlawful disclosure of sensitive personal data, information, computer database theft, privacy violation, etc.

India's Central (Federal) Government has, in April 2011, notified the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 (the "Data Protection Rules") under the IT Act, governing the entities which collect and process the sensitive personal information in India.

2. What constitutes sensitive personal data under the Indian regime?

The Data Protection Rules define "Sensitive Personal Data or Information" of a person as such personal information which consists of information relating to:

- password;
- 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 body corporate for providing service; and
- any of the information received under the above heads by body corporate for processing, stored or processed under lawful contract or otherwise.

Provided that, any information that is freely available or accessible in public domain or furnished under any law for the time being in force shall not be regarded as sensitive personal data or information.

3. Are there any sector-specific laws relating to data protection in India?

Yes, there are certain sector-specific regulations which govern data privacy and protection in India, in addition to the IT Act and the Data Protection Rules. Some of the regulations are discussed below:

Banking sector: The Indian Government and the Reserve Bank of India (the "RBI") periodically enact laws and issues master circulars, guidelines, rules and regulations, respectively, addressing the data privacy of the client information. Some of the examples are provided below:

a. The Public Financial Institutions (Obligations as to Fidelity and Secrecy) Act, 1983, prohibits the public financial institutions from disclosing the client's information to the third parties, except in accordance with the laws of practice and usage.

b. The RBI Guidelines on Managing Risks and Code of Conduct in Outsourcing of Financial Services by Banks, dated 3 November 2006, prescribe measures maintaining the confidentiality and security of customer data while transferring data to the third party service providers.

c. The RBI Master Circular on Credit Card, Debit Card and Rupee Denominated Cobranded Prepaid Card operations of Banks, 2013, prescribes conditions on the banks and non-banking financial institutions for disclosure of customer information.

d. The Credit Information Company (Regulation) Act, 2005 governs access to data, data collection and its purpose, disclosure norms, data retention, confidentiality, fidelity and secrecy of data, etc.

e. The Banking Codes and Standards Board of India prescribe code of conduct on banking operations including privacy and confidentiality of customer information.

Insurance sector: There are regulations for the insurance companies involved in the outsourcing activities with the assistance of third party service providers. The Insurance Regulatory and Development Authority (the "IRDA") had issued Guidelines on Outsourcing of Activities by Insurance Companies (the "Insurance Outsourcing Guidelines") in 2011 to regulate the outsourcing activities by the insurance companies (the "Insurers") to the third party service providers.
Clause 9 of the Insurance Outsourcing Guidelines provide that the insurers must frame a comprehensive outsourcing policy containing criteria for selection of such activities as well as service providers, delegation of authority and systems to monitor and review such operations. Further, it provides that outsourcing relationships must be governed by written contracts between the insurers and the third party service providers. The insurer must take appropriate steps to require the third party service providers to protect the clients' confidential information.

Telecom sector: The Telecom Regulatory Authority of India (the "TRAI") has released a Consultation Paper on Privacy, Security and Ownership of the Data in the Telecom Sector on 9 August 2017 concerning the issues relating to data protection of the telecom subscribers, for obtaining views from the stakeholders prior to framing a law on data protection in the telecom sector. Following are the major issues identified in the aforesaid consultation paper:

a. The manner of collection of personal data from the telecom subscribers;
b. Sharing of the telecom users' personal data;
c. The rights and responsibilities of telecom service providers towards controlling the users' personal data;
d. Measures for strengthening the safety and security of the users' data;
e. Cross-border flow of information

4. Which are the relevant authorities for governing the data protection laws in India?

India does not have a Data Privacy Authority as yet. Instances of data breach are handled by the Vigilance and Grievances wing of the Department of Electronics and Information Technology.

Further, the IT Act mandates the Central Government to appoint an adjudicating officer to conduct an inquiry for injury or damage claim of maximum INR 50,000,000 (USD 767,930 approx.). The claims exceeding this amount would be dealt by the competent civil court.

Additionally, data privacy issues under the sector-specific regulations are governed by the respective sectoral regulators.

5. What are the criteria for collecting data under the Indian laws? Are there any restrictions?

Following are the conditions and restrictions for collection of the sensitive personal data or information under the Data Protection Rules:

a. Privacy - A company that collects, receives, stores, processes or handles personal or sensitive personal information must provide a privacy policy on the company's website which must be accessible to the data providers.

b. Consent - The Data Protection Rules mandate companies to obtain express consent from the data providers regarding the purpose and use of the information. The consent can be obtained through any electronic media. Mere information provided by the data providers does not amount to "consent" for the purposes of the Data Protection Rules.

c. Lawful Purpose - A company can collect the sensitive personal information only if the information is collected for a lawful purpose connected with the company's business and collection of the information is necessary for the purpose.

d. Notice of Collection of Information - The company must ensure that the data providers are made aware of the purpose for which the information is collected, the intended recipients of the information, the agency collecting the information, the agency retaining the information, etc. Further, the data provider must be given an option not to provide the information, or revise / withdraw the information as well.

e. Data Retention - The entities holding sensitive personal data should not retain the information longer than required for the purpose for which it was collected or used lawfully.

f. Security – The companies must have "reasonable security practices and procedures". The companies are deemed in compliance if they have a documented security program with managerial, technical, organizational and physical controls. ISO 27001 is provided as a reference standard.

g. Grievances – All discrepancies or grievances reported to the companies must be addressed in a timely manner. The companies must appoint a grievance officer and publish his / her name and contact details on the company's website. The

grievance officer must redress all the data subjects' grievances within one (1) month of receiving the grievance.

6. Can the data controllers and processors disclose the data without the data provider's prior consent?

The data controllers and processors must not disclose the sensitive personal information to a third party without the data provider's consent, except when such information is required by the government agencies for the time being in force or by the third parties under the law. Further, the third party, receiving such information, must not further disclose the information.

7. Is it mandatory for the data controllers and processors to get registered under the Indian laws?

There are no prevalent statutory requirements for registration of data controllers/processors.

8. What are the restrictions on the cross-border transfer of data under the Indian laws?

Following are the restrictions imposed on the cross-border transfer for the sensitive personal data or information under the Data Protection Rules:

a. The recipient entity must ensure adherence to the same level of data protection (reasonable security practices as prescribed under the Data Protection Rules); and
b. Such transfer of information must be necessary to comply with a lawful contract, or with the prior consent of the data provider.

9. Is it mandatory to report the data breach? Is there a time limitation for reporting such breaches?

The IT Act provides legal framework to address the issues related to hacking and security breaches of information technology infrastructure. Under the IT Act, the Indian government has constituted "Indian Computer Emergency Response Team" (the "CERT-IN") as the national nodal agency for cyber security.

Further, in January 2014, the Government has enacted The Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013 (the "CERT-IN Rules") which prescribe the functions and responsibilities of CERT-IN, procedure for incident reporting, response and information dissemination, etc. There are sectoral CERTs established for various sectors including defence and finance.

The CERT-IN Rules impose mandatory notification requirements for service providers, intermediaries, data centres and body corporates (handling sensitive personal information) to report all cyber security incidents to CERT-IN "as early as possible".

The RBI notification on the Cyber Security Framework in Banks, dated 2 June 2016, prescribes a format for cyber incident reporting and mandates the reporting of the cyber security incident within 2-6 hours.

All individuals, organizations or corporate entities have the option to report the cyber security breach incidents to CERT-IN.

Notwithstanding the foregoing, all entities must mandatorily report the cyber security incidents specified in the CERT-IN Rules to CERT-IN at the earliest. Some of the cyber security incidents are:

- targeted scanning/probing of critical networks/system;
- compromise of critical systems/information;
- unauthorized access of IT systems/data;
- defacement of website or intrusion into a website and unauthorized changes such as inserting malicious code, links to external websites, etc.;
- malicious code attacks such as spreading of virus/worm/trojan/botnets/spyware;
- attacks on servers such as database, mail and DNS and network devices such as routers;
- identity theft, spoofing and phishing attacks;
- denial of service (DoS) and Distributed Denial of Service (DDoS) attacks;
- attacks on critical infrastructure, SCADA Systems and wireless networks;
- attacks on application such as e-governance, e-commerce, etc.

10. Are there any penalties imposed for data breach under Indian laws?

The IT Act prescribes civil and criminal penalties for contravention of the provisions of the IT Act. For instance, if a body corporate possessing, dealing or handling the sensitive personal information in a computer resource is negligent in implementing reasonable security practices and thereby causes wrongful loss or wrongful gain to any person, the body corporate will have to compensate the affected person. Further, the IT Act prescribes fine / imprisonment up to three (3) years for the offences of such breach of confidentiality and privacy and disclosure of information in breach of lawful contract.

11. Are there any regulations relating to employee data privacy protection and employee monitoring in India?

India does not have specific laws to deal with the protection of employee data or employee privacy. The IT Act and the Data Protection Rules are the only laws currently applicable on the data protection in India. Nevertheless, the employers in India have all the liabilities that a data controller and processor has under the IT Act and the Data Protection Rules, as stated above will have, while collecting the sensitive personal data or information of their employees for various purposes including recruitment process, employee evaluation process, etc.

In this regard, the body corporates must have employee data protection and privacy policies and reasonable security practices and procedures under the IT Act. They must obtain written consents from their new as well as existing employees prior to the collection, use or transfer (including cross-border transfers in case of multinational companies) of the employees' personal data. The employment contracts may contain clauses relating to the collection, retention or transfer of employee data.

As regards employee monitoring, the current Indian laws do not prohibit or restrict the camera surveillance for the employees, or monitoring of the employees' e-mails, telephone calls, etc. Provided, however, such activities must be reasonable and should not violate the employees' personal privacy.

Although the Supreme Court of India has declared the right to privacy as a fundamental right under the Indian Constitution in its recent landmark judgment of *Justice K.S Puttaswamy (Retd.)* v. *Union of India and Ors* [WP (C) 494 of 2012], it is subjected to reasonable restrictions and is currently enforced only against the State or its instrumentalities. The Supreme Court in the aforesaid decision has directed the Indian government to frame a data protection regime for India to enforce the right to data privacy against the private entities as well, with reasonable restrictions.

12. What is the scope of the right to data privacy (informational privacy) as a fundamental right in India?

The Supreme Court in the aforesaid judgment has recognized the right to informational privacy (i.e., the digital data) as a fundamental right and held that it can be enforced against the State and its instrumentalities. Further, the Supreme Court has raised the following data privacy concerns where a large amount of data is held by the non-state/private entities:

a. The digital entities have control over the Indian citizens' data without any governance; the bank accounts are linked with the electronic mails, which are again linked to the social networking sites, etc.
b. The privacy consent notices of different websites to assess the users' data.

A definite and uniform framework is required to govern data protection in India, especially when the data is held by private or non-state entities. In this regard, the Supreme Court has directed the Justice B.N. Srikrishna Committee, formed by the Ministry of Electronics and Information Technology, to frame a data protection regime in India enforceable against the private or non-state entities.

13. What are the effects and prospective impacts on data privacy regime after the recent declaration of the right to privacy as a fundamental right in India?

Following are the major effects and prospective impacts of the declaration of the right to privacy protection as a fundamental right:

- The Justice B.N. Srikrishna Committee will propose to introduce the Data (Privacy and Protection) Bill, 2017.
- The linking of Indian citizens' biometric data with their bank accounts, SIM cards, PAN cards, etc., by the Indian Government, has been challenged in the Supreme Court. The Supreme Court has decided to form a constitutional bench to decide the validity of such linkage.
- The Supreme Court has issued notices to social networking companies, such as WhatsApp, Facebook, Twitter and Google to respond regarding their privacy policies and manner of collecting and disclosing the users' personal data to third parties, as these websites started linking their users' accounts to facilitate data transfer between each other.

Conclusion

The actual effect and implementation of the Supreme Court's landmark judgment is yet to be witnessed. The roll-out of Digital India Initiative has led to increase in digital payments, linkage of biometrics of citizens and e-commerce activities in the country, which gives exposure to several cybercrimes and breaches. Further, India handles data privacy, analytics and data management for companies all across the globe. The existing data protection regime in India is inadequate to regulate such flow of personal data within or outside India. Therefore, India awaits a robust data protection regime as an outcome of the Supreme Court of India's directive in the near future.

E-mail us at: mailbox@anaassociates.com

Contact: ANA Law Group, Indiabulls Finance Centre, Tower-2, 11th Floor, 1103, Elphinstone Road, Mumbai - 400 013
Phone: +91 22 6112 8484 | Fax: +91 22 6112 8485