5-Jul-17

INDIA –Data Protection Framework

Indian laws relating to 'data privacy' and 'data protection' are at a nascent stage and are still evolving. The Information Technology Act, 2000 (IT Act) is one of the primary Indian legislations that deals with data privacy and protection'. The IT Act, as it was originally framed did not address these concerns and thus, was amended through the Information Technology (Amendment) Act, 2008, to include some concepts of data privacy and protection. These were introduced primarily through Sections 43-A and 72-A of the IT Act.

Whereas Section 43-A of the IT Act primarily concentrates 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 information provider's consent. In this regard, please note that the term 'personal information' has not been defined under Section 72-A of the IT Act. Therefore, it could be interpreted to mean any 'personal information'.

Further, on 13 April 2011, the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (Indian Privacy Rules) were promulgated. The Indian Privacy Rules attempted to elaborate further on the requirements of Section 43-A of the IT Act. The said Indian Privacy Rules do not require the appointment of a data protection officer or registration. There are limitations on cross-border transfers, but they apply only to sensitive personal data or information. Outsourced providers are subject to a narrower set of obligations. An organization may transfer sensitive personal data or information to any organization or person in India or to another country that ensures the same level of data protection as prescribed under the Indian Privacy Rules**; however,** the government has not issued a permitted list of countries. We strongly recommend keeping partner data in India. Further, the transfer may only be allowed if it is necessary for the performance of the contract between the organization (or its agent) and the individual or where the individual has consented to the transfer.

India does not, yet, have a comprehensive piece of legislation dealing with data privacy or personal data protection. The government recently informed the Supreme Court of India that it expects to put in place a comprehensive data protection framework by October 2017. **The Telecom Regulatory Authority of India will be heading up the initiative.**

General obligations for the collection, transfer, disclosure and use of personal information have been provided for in the IT Act, a nationally applicable piece of legislation which also regulates several other aspects of information technology including e-commerce and cybercrime. As indicated above, in 2011, India issued the Indian Privacy Rules implementing parts of the Information Technology (Amendment) Act, 2008 dealing with protection of personal information. The Indian Privacy Rules prescribe how personal information may be collected and used by virtually all organizations in India, including personal information collected from individuals located outside of India.

The Indian Privacy Rules define "*personal information*" 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."*

"Sensitive personal data or information" (SPDI) is defined as personal information which consists of information relating to passwords, **financial information**, health information, sexual orientation, medical records, biometric information, any detail relating to the afore-mentioned provisions as provided to body

corporate for providing service; and any of the information received under afore-mentioned provisions by body corporate for processing, stored or processed under lawful contract or otherwise. The Indian Privacy Rules set out various obligations in respect of these SPDI, including mandatory consent and disclosure requirements for data collection, usage, processing, storage and transfer, and requirements for appointment of a grievance officer.

In relation to security practices and procedures, the Indian Privacy Rules require every company to have in place such information security practices, standards, programs and policies which are commensurate with the information assets being protected. For this purpose, the Privacy Rules have stipulated, as a benchmark, the International Standard IS/ISO/IEC 27001 on "Information Technology -Security Techniques - Information Security Management System – Requirements" (Stipulated Standard). If a company follows any standard apart from the Stipulated Standard for data protection, they are required to get their codes (Codes) approved and notified by the Government of India. Any such standard, i.e. Stipulated Standard or Codes, implemented by the company needs to be certified or audited by an independent auditor approved by the Central Government. Further, such standard has to be audited by an auditor at least once a year or as and when there is a significant upgradation of processes and computer resources.

Application of the Rules

The Indian Privacy Rules raised significant issues and caused concern among organizations that outsource business functions to Indian service providers. As drafted, the Indian Privacy Rules applied to all organizations that collected and used personal information of natural persons, regardless of where the individuals reside or what role the company that is collecting the information plays in the process of handling the information. The provisions apply to a "body corporate," which is defined as "*any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities*," as well as, in many instances, "any person on its behalf." As a result, industry both within and outside India expressed concern that the Indian Privacy Rules would decimate the outsourcing industry.

In response to these concerns, on August 24, 2011, the Indian Ministry of Communication & Information Technology issued a clarification in relation to the Indian Privacy Rules (Clarification), stating that the Indian Privacy Rules apply only to organizations in India. **Therefore, if an organization in India receives information because of a direct contractual relationship with an individual, all the obligations under the Indian Privacy Rules continue to apply. However, if an organization in India receives information because of a contractual obligation with a legal entity (either inside or outside India), e.g., the organization is acting as a service provider, the substantive obligations of notice, choice, data retention, purpose limitation, access, and correction do not apply, but other obligations such as security obligations and obligations relating to the transfer of information do apply.**

Consent

The consent requirements at set out under the Indian Privacy Rules apply only to SPDI. Prior written consent is required to process SPDI.

Cross-Border Transfers

Under the Indian Privacy Rules, an organization may transfer SPDI to any organization or person in India or to another country that ensures the same level of data protection; however, the government has not issued a list of countries that, in its view, provide such protection. The transfer may only be allowed if it is necessary for the performance of the contract between the organization (or its agent) and the individual or where the individual has consented to the transfer.

In accordance with a recent, little-known company law provision relating to maintenance of accounts, **if a company's books, papers and books of accounts are maintained in electronic form outside India, a backup must be stored on servers physically located in India**. This rule has not been strictly enforced by the regulators. This also runs contrary to the increasingly common practice of multinationals, which use global accounting systems to maintain the accounts of entities worldwide, including Indian entities.

Third Parties: The Indian Privacy Rules regulate the disclosure or transfer of SPDI to a third party. The disclosure of SPDI is permitted if:

- it has been agreed in a contract with the provider;
- it is necessary to comply with a legal obligation; or
- the provider has given its prior consent.

Transfers can be made only to a third party that observes the same level of data protection as provided by the Indian Privacy Rules. Further, transfers are permitted only if they are necessary for the performance of a lawful contract with the provider or where the provider has consented to the transfer.
The Privacy Rules require data processors to disclose the name and address of every agency which will have access to personal information when collecting information from a data subject. Since the transfer of sensitive personal data from a data subject to a data processor is subject to restrictions, these restrictions will also apply to a further transfer from one data processor to another.

Sanctions

Section 43-A of the IT Act prescribes compensation payable to the affected person by way of damages (uncapped) for negligence in implementing and maintaining 'reasonable security practices and procedures' in relation to SPDI. However, Section 72-A of the IT Act provides for criminal sanctions of up to three years in prison and/or a fine of up to INR 500,000 in respect of intentional or negligent disclosure of an individual's personal information, obtained under a contract, where such disclosure is made without the consent of the concerned individual or in breach of the concerned contract.

Section 75 of the IT Act, which gives India jurisdiction in relation to offences or contraventions under the IT Act committed outside India by any person, provided the act constituting the offence or contravention involves a computer or computer network located in India.

Therefore, any collection, processing, storage, use or transfer of personal information or SPDI which takes place through a computer or computer network located in India would have to comply with the IT Act and Indian Privacy Rules as explained above. As such, the penalties and liability prescribed under Sections 43A and 72A of the IT Act, have also been given extra-territorial applicability and would apply to contraventions committed by non-Indian companies, irrespective of the nationality of the data subject whose information is collected, processed or transferred. While the practical enforcement of penalties against a company is unlikely where such company has no presence in India, authorities may resort to other means, including blocking access to servers or networks located in India in the event of repeated

and significant contraventions or failures by a company to comply with obligations under the Indian Privacy Rules.

Ministry of Electronics and Information Technology periodically publishes rules to supplement its provisions for the regulation of data privacy and personal data protection.

Information Technology (the Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013 (Cert-In Rules) - defines "Cyber Security Incidents" as "*any real or suspected adverse event in relation to cyber security that violates any explicitly or implicitly applicable security policy, resulting in unauthorized access, denial of service or disruption, unauthorized use of a computer resource for processing or storage of information or changes to data or information without authorization.*"

The Cert-In Rules stipulate that "*any individual, organization or corporate entity affected by cyber security incidents may report the incident to CERT-In. The type of cyber security incidents as identified in Annexure shall be mandatorily reported to CERT-In as early as possible to leave scope for action. Service providers, intermediaries, data centers and body corporate shall report the cyber security incidents to CERT-In within a reasonable time of occurrence or noticing the incident to have scope for timely action.*"

Further, the Annexure referred above sets out the following cyber security incidents:

- Targeted scanning/probing of critical networks/systems
- Compromise of critical systems/information
- Unauthorised access of IT systems/data
- Defacement of website or intrusion into a website and unauthorised 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 applications such as e-governance, e-commerce etc

Upon the occurrence of any of these events, companies are now required to notify the Computer Emergency Response Team (CERT-In), a government body established to collect, analyze and disseminate information on cyber incidents, provide forecasts and alerts about cyber security incidents, provide emergency measures for handling cyber security incidents and coordinate cyber incident response activities. As indicated above, such notifications are required to be made within a reasonable time, to leave scope for appropriate action by the authorities.

Resources:

- Data Protection in India → available here
- Analysis: Data Protection in India – Getting it Right → available here
- Data Security and Cybercrime in India → available here