ANA LAW GROUP
ANOOP NARAYANAN & ASSOCIATES

A BRIEF OVERVIEW

OF

DATA SECURITY LAW IN INDIA

2016

INTRODUCTION

India has an omnibus privacy law that is similar in many respects to the existing EU data protection law. The obligations under the Indian data privacy regime that require the companies to provide privacy policies, restrict the processing of sensitive personal data, restrict international data transfers and require additional security measures, creates 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 of 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 ("Data Protection Rules") under the IT Act, governing the collection and processing of personal information in India.

DEFINITION - SENSITIVE PERSONAL DATA

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 clauses as provided to body corporate for providing service; and
- any of the information received under above clauses 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.

KEY PROVISIONS

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 should be accessible to the data providers.

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 to the data providers does not amount to "consent" for the purposes of the Data Protection Rules.

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.

Notice of Collection of Information - The company should 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 should be given an option not to provide the information, or revise / withdraw the information.

Disclosure - The company must not disclose the sensitive personal information to a third party without the data provider's consent. Further, the third party should not further disclose the information.

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

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.

Grievances – All discrepancies or grievances reported to companies must be addressed in a timely manner. 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.

RESTRICTIONS ON DATA TRANSFER OUTSIDE INDIA

- the recipient entity ensures adherence to the same level of data protection (reasonable security practices are prescribed under the Rules), and
- only if the transfer of information is necessary to comply with a lawful contract, or
- with the prior consent of the data provider.

Besides the Data Protection Rules, there is no other law that governs overseas data transfer. Further, the data transfer restrictions / requirements are applicable to any personal information transferred outside India irrespective of the countries to which the data is transferred.

PENALTIES

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 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 offences such breach of confidentiality and privacy and disclosure of information in breach of lawful contract.

DATA PRIVACY AUTHORITY

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.

CYBER-ATTACK AND REPORTING

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 prescribes 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".

All individuals, organizations or corporate entities have the option to report the cyber 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. These 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.

For critical infrastructure, the Central Government has set up a National Critical Information Infrastructure Protection Centre (NCIIPC) under the National Technical Research Organisation as a nodal agency, primarily to protect critical information infrastructure in India.

The Government has also enacted the Information Technology (National Critical Information Infrastructure Protection Centre and Manner of Performing Functions and Duties) Rules, 2013 (the "NCIIPC Rules") which prescribes the functions and responsibilities of NCIIPC and the procedures.

Critical Information Infrastructure is defined as computer resource, the incapacitation or destruction of which, shall have debilitating impact on national security, economy, public health or safety.

The nodal officers of each critical sector must report the breach incident to NCIIPC without any delay. NCIIPC has the power to initiate measures such as interception, monitoring, decrypting or blocking of cyber information to protect critical information infrastructure. The NCIIPC Rules do not specify any timeline for notifying the breach.

However, as of now, there is no publicly available information on the practical enforceability of these provisions and any penalties imposed by CERT-In or NCIIPC for contravention.

DATA LEAKAGE AND TOOLS

Many large international corporates and banking and financial institutions are in the process of deploying data leakage prevention tools to secure their sensitive business information from leaking outside through the information technology systems via copying, uploading or e-mails. The deployment of tools involve monitoring the data and system files, scanning the data, intercepting it, encrypting and decrypting the data, transfer of data for investigation purposes to an affiliate or a third party investigator, etc. The companies' are concerned whether the use of each of the tools is permitted by and in compliance with the applicable data protection and privacy laws for the end-point operations and network operations, applicable communications law, employment law, etc.; whether the location of servers matter; whether the levels of data protection and compliances are stronger for banking and financial information, information of national importance, etc.; whether there are any potential criminal penalties for non-compliances; whether the third parties such as forensic specialists can be held liable for any data breach, and so on.

India's data specific and other laws and their applicability on these issues must be assessed before deploying the tools and dealing with sensitive personal information.

EXPECTED FUTURE DEVELOPMENTS IN LEGAL FRAMEWORK

One of the expected legal developments is the notification of the Personal Data Protection Bill, 2006 (the "Proposed Bill"), which has not as yet become a law. The Proposed Bill is intended to apply to both government and private organizations and to provide for protection of personal data and information of an individual collected for a particular purpose by an organization, and to prevent its usage by another organization

for commercial or other purposes. The Proposed Bill also provides for compensation or damages resulting from disclosure of personal data or information of any individual without his / her consent.

OUR DATA PRIVACY PRACTICE

We have significant experience in counselling international clients on issues related to data protection and privacy in India. Our attorneys have acted for a variety of businesses on a number of complicated transactions, thereby attaining in-depth knowledge about how different industries operate, the specific concerns with respect to data and information management, and the practical aspects.

We regularly represent clients from industries such as banking and insurance, financial institutions, luxury goods, consumer goods, health care, payroll processing companies, pharmaceuticals, telecommunications and Internet service providers, credit research agencies, employee screening companies, etc.

Our data protection and privacy practice has grown as one of the best practices in India, based on the quality of deliverables, practical, clear and timely advice, and the ability to provide comprehensive business solutions in a legally compliant manner.

In addition to providing regular legal advice on issues involving data protection and privacy, we also assist a number of international companies on global privacy law that involve Indian projects, drafting and negotiating contracts with Indian counterparts, preparation of data protection and privacy policies for international companies' Indian subsidiaries, compliant with the major international privacy laws.

We provide extensive support to our clients in the following areas:

- Advising on processing data domestically, complying with the regulatory requirements and the disclosure of processing to data subjects;
- Advising on transfers of sensitive personal data within and outside India;
- Advising on security breaches and drafting security breach policies;
- International compliance projects including implementing corporate rules and handling cross-border data flows;
- Advising on prosecutions and offences, and on actions by the regulators;
- Conducting audits; and
- Drafting legally compliant agreements, consent forms, etc.