DATA PROTECTION LAWS OF THE WORLD

India

DLA PIPER

INDIA

Last modified 24 March 2015

LAW IN INDIA

There is no specific legislation on privacy and data protection in India. However, the Information Technology Act, 2000 (the 'Act') contains specific provisions intended to protect electronic data (including non-electronic records or information that have been, are currently or are intended to be processed electronically).

India's IT Ministry adopted the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules (Privacy Rules). The Privacy Rules, which took effect in 2011, require corporate entities collecting, processing and storing personal data, including sensitive personal information to comply with certain procedures. It distinguishes both 'personal information' and 'sensitive personal information', as defined below.

In August 2011, India's Ministry of Communications and Information issued a 'Press Note' Technology (Clarification on the Privacy Rules), which provided that any Indian outsourcing service provider/organisation providing services relating to collection, storage, dealing or handling of sensitive personal information or personal information under contractual obligation with any legal entity located within or outside India is *not* subject to collection and disclosure of information requirements, including the consent requirements discussed below, provided that they do not have direct contact with the data subjects (providers of information) when providing their services.

DEFINITIONS

Definition of personal data

The Privacy Rules define the term 'personal information' as any information that relates to a natural person, which either directly or indirectly, in combination with other information that is available or likely to be available to a corporate entity, is capable of identifying such person.

Definition of sensitive personal data

The Privacy Rules define 'sensitive personal data or information' to include the following information relating to:

- password
- financial information eg bank account/credit 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 a corporate entity for providing services, and
- any of the information received under the above clauses for storing or processing under lawful contract or otherwise.

Biometrics means the technologies that measure and analyse human body characteristics, such as 'fingerprints', 'eye retinas and irises', 'voice patterns', 'facial patterns', 'hand measurements' and 'DNA' for authentication purposes.

However, any information that is freely available in the public domain is exempt from the above definition.

NATIONAL DATA PROTECTION AUTHORITY

No such authority exists.

REGISTRATION

No requirements.

DATA PROTECTION OFFICERS

Every corporate entity collecting sensitive personal information must appoint a Grievance Officer to address complaints relating to the processing of such information, and to respond to data subject access and correction requests.

COLLECTION & PROCESSING

Under the Act, if a corporate entity that possesses, manages or handles any sensitive personal information in a computer resource that it owns, controls or operates, is negligent in implementing and maintaining compliance with the Privacy Rules, and its negligence causes wrongful loss or wrongful gain to any person, the corporate entity shall be liable for damages to the person(s) affected.

The Privacy Rules state that any corporate entity or any person acting on its behalf, which is collecting sensitive personal information, must obtain written consent (through letter, email or fax) from the providers of that information. However, the August 2011 'Press Note' issued by the IT Ministry clarifies that consent may be given by any mode of electronic communication.

The Privacy Rules also mandate that any corporate entity (or any person, who on behalf of such entity) collects, receives, possess, stores, deals or handles information, shall provide a privacy policy that discloses its practices regarding the handling and disclosure of personal information including sensitive personal information and ensure that the policy is available for view, including on the website of the corporate entity (or the person acting on its behalf). Specifically, the corporate entity must ensure that the person to whom the information relates is notified of the following at the time of collection of sensitive personal information or other personal information:

- the fact that the information is being collected
- the purpose for which the information is being collected
- the intended recipients of the information, and
- the name and address of the agency that is collecting the information and the agency that will retain the information.

Further, sensitive personal information may only be collected for a lawful purpose connected with a function or purpose

of the corporate entity and only if such collection is considered necessary for that purpose. The corporate entity must also ensure that it does not retain the sensitive personal information for longer than it is required, and should also ensure that the same is being used for the purpose for which it was collected.

A corporate entity or any person acting on its behalf is obligated to enable the providers of information to review the information they had so provided and also to ensure that any personal information or sensitive personal information that is found to be inaccurate or deficient is corrected upon request. Further, the provider of information has to be provided a right to opt out (ie he/she will be able to withdraw his/her consent) even after consent has been provided. However, the corporate entity will not be held responsible for the authenticity of the personal information or sensitive personal information given by the provider of information to such corporate entity or any other person acting on its behalf.

TRANSFER

The data collector must obtain the consent of the provider of the information for any transfer of sensitive personal information to any other corporate entity or person in India, or in any other country that ensures the same level of data protection as provided for under the Privacy Rules. However, consent is not necessary for the transfer, if it is required for the performance of a lawful contract between the corporate entity (or any person acting on its behalf) and the provider of information or as otherwise specified in the Act.

A corporate entity may not transfer any sensitive personal information to another person or entity that does not maintain the same level of data protection as required in the Act.

The contract regulating the data transfer should contain adequate indemnity provisions for a third party breach, should clearly specify the end purposes of the data processing (including who has access to such data) and should specify a mode of transfer that is adequately secured and safe.

Further, under the Act, it is an offence for any person who has pursuant to a contract gained access to any material containing personal information to disclose that information without the consent of the person concerned, and with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain.

Thus, contracts should also specifically include provisions:

- entitling the data collector to distinguish between ‘personal information’ and ‘sensitive personal information’ that it wishes to collect/process
- representing that the consent of the person(s) concerned has been obtained for collection and disclosure of personal information or sensitive personal information, and
- outlining the liability of the third party.

SECURITY

A corporate entity possessing, dealing or handling any sensitive personal information in a computer resource which it owns, controls or operates is required to implement and maintain reasonable security practices and procedures to secure the sensitive personal information. The reasonable security practices and procedures may be specified in an agreement between the parties.

Further, the Privacy Rules provide that in the absence of such agreement ‘reasonable security practices and procedures’ to be adopted by any corporate entity to secure sensitive personal information are procedures that comply with the IS/ISO/IEC 27001 standard or with the codes of best practices for data protection as approved by the Federal Government.

BREACH NOTIFICATION

The Government of India, has established and authorised the Computer Emergency Response Team (Cert-In), to

collect, analyse and disseminate information on cyber incidents, provide forecast and alerts of cyber security incidents, provide emergency measures for handling cyber security incidents and coordinate cyber incident response activities.

The Information Technology (the Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013 (Cert-In Rules) impose mandatory notification requirements on service providers, intermediaries, data centres and corporate entities, upon the occurrence of certain 'cyber security incidents'.

Cyber security incidents have been defined to mean any real or suspected adverse events, in relation to cyber security, that violate any explicitly or implicitly applicable security policy, resulting in:

- unauthorised access, denial or disruption of service
- unauhorised use of a computer resource for processing or storage of information
- changes to data, information without authorisation.

The occurrence of the following types of cyber security incidents, trigger the notification requirements under the Cert-In Rules:

- Targeted scanning/ probing of critical networks/ systems
- Compromise of critical information/ system
- Unauthorized access of IT system/ data
- Defacement of websites or intrusion into website & unauthorized changes such as inserting malicious codes, links to external websites
- Malicious code attacks such as spreading virus, worm/ Trojan/ Botnets/ Spyware
- Attacks on servers such as Database, Mail and DNS & Network devises such as Routers
- Identity theft, Spoofing and phishing attacks
- Denial of service (DoS) & Distributed Denial of service (DDoS) attacks
- Attacks on critical infrastructure , SCADA systems and wireless networks
- Attacks on Application such as E-governance and E-commerce etc.

Upon the occurrence of any of the aforementioned events, companies are required to notify the Cert-In within reasonable time, so as to leave scope for appropriate action by the authorities. The format and procedure for reporting of cyber security incidents have been provided by Cert-In on its official website.

ENFORCEMENT

Civil penalties of up to EUR 694,450 for failure to protect data including sensitive personal information may be imposed by an Adjudicating Officer; damages in a civil suit may exceed this amount.

Criminal penalties of up to 3 years imprisonment or a fine up to EUR 6,950, or both for unlawful disclosure of information.

ELECTRONIC MARKETING

The Act does not refer to electronic marketing directly. However, sending false information (emails, SMS, MMS, etc.) persistently by means of a computer resource or a communication device for the purpose of causing annoyance, inconvenience, etc. is punishable under Indian law. Further, such emails, SMS, MMS etc. must not disguise or conceal the identity of the sender.

The Privacy Rules also provide the right to 'opt out' of email marketing, and the company's privacy policy must address marketing and information collection practices.

ONLINE PRIVACY

There is no regulation of cookies, behavioural advertising or location data.

However, the IT Act contains both civil and a criminal offences for a variety of computer crimes:

- any person who introduces or causes to be introduced any computer contaminant into any computer, computer system or computer network may be fined up to EUR 694,450 (by an Adjudicating Officer); damages in a civil suit may exceed this amount. Under the IT Act, 'computer contaminant' is defined as any set of computer instructions that are designed:
    - to modify, destroy, record, or transmit data or programmes residing within a computer, computer system or computer network, or
    - by any means to usurp the normal operation of the computer, computer system or computer network, and
- any person, who fraudulently or dishonestly makes use of the electronic signature, password or any other unique identification feature of any other person, is subject to a prison term of up to 3 years and fine up to EUR 1,390.