scriboard®
Advocates & Legal Consultants

the
IP-TECH
law series
2018

Guide to

Data Transfer

Indian Regulations

LAW WIRE®
COMMUNICATING THE LAW™

Data Transfer
Indian Regulations

In India, we do not have adequate and comprehensive Data Privacy / Protection legislation. In the absence of blanket legislation, Information Technology Act provides for data protection and acts as a guiding rulebook.

The Rules under Section 43A [Compensation for Failure to Protect Data] of the Information Technology Act, 2000 [Amended 2008] are largely [not wholly] applicable to Sensitive Personal Information. In the event of information security breach [non-compliance with the rules and the act], the body corporate [Data Controller] shall be required to demonstrate that they have implemented security control measures as per their documented information security programme and information security policies.

Furthermore, Section 72 and Section 72A of the Information Technology Act provides for "Penalty for Breach of Confidentiality and Privacy" and "Punishment for Disclosure of information in breach of lawful contract" respectively.

Fair dealing with Data
The data / information should be dealt in a fair, reasonable and ethical manner. Over the years, the technology has advanced but the basic rules / principles that are followed while dealing with data / information remains the same, as listed below:

1. Processing of data must be fair, lawful and in conformity with special rules for sensitive data
2. Data should be obtained / collected for specific & lawful purpose[s] and must not be subjected to any further incompatible processing
3. Data sought should be adequate, relevant and not excessive
4. Data obtained / collected should be kept accurate and up-to-date
5. Data obtained / collected should not be kept for longer than is required / necessary
6. Rights and Requisitions
    - Rights of Data Subjects to be addressed
    - Providing / securing information as per the Law
    - Requisitions form the Government
7. Technical, Managerial and Organizational measures
    - Against Unauthorized / Unlawful processing of Personal Data
    - Against accidental loss and destruction of Personal Data
    - Against damage to Personal Data
8. Cross border data flow
    - Data transfer laws of receiving state to be adhered to
    - Similar or higher level of data projection is a must

Data Protection under the Information Technology Law
Under the Information Technology Act [and Rules], the highest level of security has been demanded for safeguarding "Sensitive Personal Data and

Information" under Section 43A [and rules therein] which talks about "Failure to Protect Data".

As per the "Rules" Sensitive personal data or information [SPDI] of a person means 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. Freely available or accessible information or information furnished under the Right to Information Act, 2005 or any other law for the time being in force has been expressly excluded from the definition.

The "Rules" further define "Personal information" [PDI] 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 that person.

The IT Act requires the data controller to maintain "reasonable security procedures." The data controller may maintain security measures if the data controller (1) implemented security practices and standards [Comprehensive documented information security programme and information security policies], such as IS/ISO/IEC 27001, or (2) adopted a code developed by an industry association that the government has approved and notified.

An independent auditor that the Government of India approved must audit the security procedure of the data controller on a regular basis. The data controller must conduct an audit each year or when the data controller has significantly upgraded its computer resource.

For ease and clarity please find below a complete compliance list under "The Information Technology [Reasonable Security Practices and Procedures and Sensitive Personal Data or Information] Rules, 2011 and in our opinion, the following safeguards must be incorporated:

1. Rule 4 - Mandatory 'Privacy Policy' for handling of or dealing in personal information including sensitive personal data or information [PDI; SPDI]
2. Rule 5 – Collection of information [PDI; SPDI]
    - Mandatory consent from provider of information while collecting information [SPDI]
    - Disclosure of purpose and intended recipients [SPDI]
    - Not to retain Information for longer than is required [SPDI]
    - Review of Information by the provider [PDI; SPDI]
    - Option for the provider of information to pull out [PDI; SPDI]
    - Duty to keep the information secure [PDI; SPDI]
    - Mandatory appointment of Grievance Officer to address complaints [PDI; SPDI]

3. Rule 6 – Disclosure of Information [SPDI]
    - Disclosure to third parties require prior consent; Third parties should not disclose it further [SPDI]
    - Disclosure to certain Government Agencies mandated under law without prior permission [SPDI]
    - Body corporate should not publish Sensitive Personal Information / Data [SPDI]
4. Rule 7 – Transfer of Information [PDI; SPDI]
    - Requires prior consent of provider of information [PDI; SPDI]
    - Allowed only if its an obligation under a contract [PDI; SPDI]
    - Same level of data protection should be ensured [PDI; SPDI]
5. Rule 8 - Reasonable security practices and procedures while dealing with Sensitive Personal Information [PDI; SPDI]
    - Comprehensive documented information security programme and information security policies [PDI; SPDI]
    - International Standard IS/ISO/IEC 27001 on "Information Technology / Security Techniques / Information Security Management System" approved as compliant [PDI; SPDI]
    - Other codes must be duly approved by the Central Government [PDI; SPDI]
    - Audit 'reasonable security practices and procedures' by an auditor at least once a year or after every significant upgradation [PDI; SPDI]

Notice & consent

1. When collecting personal data, the data controller must inform the data subject [referred to as the provider of information under Indian laws and rules] of (1) the data controller's purpose for collecting the data subject's information, (2) whether the information is to be transferred or disclosed, and (3) the names and addresses of the agency collecting and retaining the information.
2. Every data controller must provide and maintain a privacy policy which states (1) the purpose for collection of information, (2) the type of data being collected, (3) the security measures undertaken to protect the information, (4) details of practices and policies adopted with regard to handling such information and (5) the policy for disclosure of such information to third parties.
3. The data subject's consent is required only when collecting Sensitive Personal Data but it would be prudent to seek consent while dealing with personal data / information as well. The material containing personal information must be obtained while providing services under the terms of a lawful contract.
4. Consent may be obtained online through various means such as electronic mail and also through letter or fax, e.g. a privacy policy which contains an "I Agree" button. Valid consent under the Privacy Rules is granted when the data subject clicks the button.

Consumer rights
The data controller must ensure that every data subject has rights to access and review the information collected. Additionally, the data subject must be able to correct or amend any information that is inaccurate or deficient. The Privacy Rules have not established the procedure for gaining access. The Rules also requires the body corporate to appoint a Grievance Officer to address complaints.

Stated purpose
The data controller can only use personal information for the stated purpose. Additionally, the data controller may not retain information for longer than is necessary for the purpose.

Sharing of data internally
It would be prudent, in the absence of clarity, to apply similar standards of restriction as applied while sharing sensitive personal data / information with third parties, wherever convenient. Internal sharing may be governed by policies, contracts, confidentiality agreements, etc.

Sharing with third parties (business partners and service providers)
The data controller cannot disclose or transfer Sensitive Personal Data or information to third parties unless (1) the data subject provides prior consent or (2) the data controller and the data subject agreed to such disclosure in their contract.

Cross-border data transfer
The data controller can transfer Sensitive Personal Data to a party overseas only if the party ensures the same level of protection of the data controller in India. Additionally, the rules in Restriction/requirements for sharing with third parties apply.

Security checklist for the handlers of data / information

1. Obligation to protect the privacy of the individual who is the provider of the information
2. It is legally permitted to collect and process personal data
3. The processing of such data is in conformity with the local rules
4. A complaint redressal mechanism have been put in place
5. They collaborate and respond to requests and requisitions
6. The provider of information or data has a right to:
    - Know the identity of person collecting data
    - Know the precise details of data held
    - Prevent the data from being used for direct marketing purposes
    - Have inaccurate data corrected or erased
    - Have a government authority assess data controllers processing mechanism
7. The management should notify and inform its employees about the company's policy and standards of data protection / security
8. In the event of an information security breach, the entity is required to demonstrate that it had put in place appropriate measures. These safeguards include:

- A comprehensive Information Security Policy
- Physical Security Measures
- Limited, Restrained and Monitored access to information
- Investigating a security breach without much delay
- Compulsory Staff Training

SCRIBOARD
Advocates and Legal Consultants

www.scriboard.com

Scriboard is a full-service commercial law firm with cutting-edge specialisation in intellectual property, commercial laws, domain name disputes, data privacy / protection, technology including compliance, new media, telecommunications, legal training and allied services. Scriboard regularly advises Fortune 500 and other leading multinational and national companies on a plethora of issues.

LAWWIRE
Communicating The Law

www.lawinfowire.com

Law Wire is a platform, which focuses on providing an in depth coverage on the ever changing Intellectual Property, TMT and New Media Law sector in India and the world. Law Wire bridges the gap between legal knowledge on one hand and the legal policy making on the other. Law Wire is also a platform where readers would get an in depth knowledge of issues pertaining to Intellectual Property and Information Technology Law. This platform endeavours to provide an opportunity to lawyers [including law students] and other professionals in the legal domain to express their views and work in a collective capacity.