scriboard®
Advocates & Legal Consultants

the
IP-TECH
law series
2018

Guide to

Information Technology Law Compliance

Indian Regulations

LAW WIRE®
COMMUNICATING THE LAW™

Information Technology Law Compliance

Indian Regulations

Organisations collect a huge amount of personal data, which in the legal parlance may be known as SPDI [Sensitive Personal Data or Information]. Such organizations are required to comply under the Information Technology Act [2000] and its Rules, which lay down certain procedures to be followed at the time of collection of data, transfer of data, and disposal of data, and to maintain relevant security practices and procedures.

A Techno-legal compliance assessment requires a thorough assessment of the company's data / information flow through its activities and suggesting necessary corrective steps which will minimize the company's liability in the event of an adverse incident. The assessment is carried out keeping in mind the specific legal requirements with respect to the organization.

The following activities are proposed in furtherance of the compliance assessment:

1. Assessing flow of information within an organisation
2. Creating assessment reports
3. Suggesting remedial measures for shortcomings
4. Implementation of remedial measures
5. Post implementation assessment
6. Review of corporate / employee agreements and existing IT policies
7. Formulating / Drafting comprehensive Information Security Management System (ISMS) policies
8. Training and awareness programs

Negligence in implementing and maintaining reasonable security practices and procedures may make a person liable to pay damages. It is interesting to note that under the amended Information Technology Act, compensation claims upto Rs. 5 Crore are handled by Adjudicating Officers while claims above Rs. 5 Crore are handled by the relevant courts. On breach of confidentiality and privacy, the law calls for punishment and / or fine for disclosure of information in breach of a lawful contract.

Data Privacy and Information Security

The Information Technology Act places a duty on the organisation to "… maintain reasonable security practices and procedures" [Section 43A]. The Act under the Section - "Offences by Companies" [Section 85] – makes it clear that "… every person who, at the time the contravention was committed, was in charge of, and was responsible to, the company for the conduct of business of the company as well as the company…" The persons responsible may not just be Directors or members of the senior management, it could be any employee entrusted with the related responsibility under the Act. It is imperative that all facets of the use of organisation's IT resources should be governed by internal IT Use and Security Policies.

A corporate body, being a legal person, can be seen as a perpetrator of cyber crimes if an employee or official of the corporation in the course of his employment commits it.

The section makes corporations and their directors, managers and other officials liable for any contravention of any provisions of the Act. The top management is made liable if it is proved that they had knowledge of the contravention or that the contravention was committed because of their negligence.

Data protection has now been made more explicit through clause 43A. This clause provides for compensation to an aggrieved person whose personal data, including sensitive personal data, may be compromised by a company during the time this data was under processing with the company and as a result of the company's negligent failure to protect such data due to a lack of implementing or maintaining reasonable security practices.

"Reasonable security practices and procedures" will constitute those practices and procedures that protect such information from unauthorized access, damage, use, modification, disclosure, or impairment as may be specified in an agreement between the parties or as may be specified by any law in force. In the absence of such an agreement or any law, the central government will prescribe security practices and procedures in consultation with professional bodies or associations.

Data privacy in India is primarily governed by the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 notified by the Central Government.

Negligence in implementing and maintaining reasonable security practices and procedures may make a person liable to pay damages. It is interesting to note that under the amended Information Technology Act, compensation claims upto Rs. 5 Crore are handled by Adjudicating Officers while claims above Rs. 5 Crore are handled by the relevant courts.

Confidentiality and Privacy

On breach of confidentiality and privacy, the law calls for punishment for disclosure of information in breach of a lawful contract. Any person including an intermediary who discloses personal information, in its possession under a lawful contract, without the consent of the subject person shall be liable. Punishment will consist of imprisonment of up to three years, and/or a fine of 500,000 rupees. This addition to the law improves data protection to some extent and businesses would feel more secure while dealing with personal and sensitive data in India or similar data that might pass through India.

Compliance under "The Information Technology Act, 2000"

1. Retention of electronic records [Section 7]
2. Regular Audit of electronic records [Section 7A]
3. Reasonable measures to ensure that its employees don't inflict damage upon any computer, computer system, etc. Without the

permission of the owner, they also must not do the following acts [Section 43]
    - Securing access to computer or computer system
    - Downloading, copying and extracting data
    - Introducing computer virus or contaminant
    - Damaging or disrupting the computer
    - Denying access to any person authorized to do so
    - Assisting someone in gaining access to the computer
    - Tampering and manipulating any computer
    - Stealing, destroying, deleting or altering any information and assisting someone in doing so
4. Compensation for failure to protect data [Section 43A]
5. Furnish information, record, document or report including books of accounts to the concerned authorities [Section 44]
6. Reasonable steps to ensure that its employees don't tamper with computer source documents [Section 65]
7. Computer related offences [Section 66 (A-F)]
    - Offensive messaging
    - Receiving stolen computer source and Data
    - Identity Theft
    - Cheating by personating using computer source
    - Violation of privacy
    - Cyber Terrorism
8. Publishing obscene material [Section 67]
9. Preservation and retention of information by intermediaries [Section 67 C]
10. To comply with the directions to monitor and collect traffic data or information through any computer resource for cyber security [Section 69B]
11. To comply with the direction of the Indian Computer Emergency Response Team (CERT-IN) in the area of cyber security [Section 70B]
12. Organizations must also take serious note of the following offences:
    - Misrepresentation [Section 71]
    - Breach of Confidentiality [Section 72]
    - Disclosure of information in breach of contract [Section 72A]
    - Publishing false particulars in Electronic Signature Certificate [Section 73]
    - Using Electronic Signature Certificate for fraudulent purposes [Section 74]
13. Offences committed by Companies [Section 85]

Compliance under "The Information Technology [Reasonable Security Practices and Procedures and Sensitive Personal Data or Information] Rules, 2011

1. Rule 4 - Mandatory 'Privacy Policy' for handling of or dealing in personal information including sensitive personal data or information
2. Rule 5 – Collection of information
    - Mandatory consent from provider of information while collecting information

- Disclosure of purpose and intended recipients
- Review of Information by the provider
- Option for the provider of information to pull out
- Duty to keep the information secure
- Mandatory appointment of Grievance Officer to address complaints

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

Compliance under "The Information Technology (Intermediary Guidelines) Rules, 2011

Apart from the aforementioned compliance requirements, "Intermediaries" must also adhere to the guidelines under Section 79 of the Information Technology Act. An 'Intermediary' shall not knowingly host or publish any information or shall not initiate the transmission, select the receiver of transmission, and select or modify the information contained in the transmission. Upon obtaining actual knowledge of a violation must act expeditiously [within thirty six hours] to remove access to such information.

An 'Intermediary' is under a legal obligation to:

1. publish the terms and conditions of use of its website, user agreement and privacy policy
2. inform its users that in case of non-compliance with terms, the Intermediary has the right to immediately terminate the access rights of the users
3. provide information to government agencies that are lawfully authorized for investigative, protective, cyber security or intelligence activity

4. report cyber security incidents and also share cyber security incidents related information with the Indian Computer Emergency Response Team.
5. not deploy or install or modify the technological measures which may change the normal course of operation of the computer resource
6. publish the details of the Grievance Officer on its website and the designated agent to receive notification of claimed infringements

An 'Intermediary' must also notify users of the computer resource not to host, display, upload, modify, publish, transmit, update, share or store any information that:

1. belongs to another person
2. is harmful, threatening, abusive, harassing, blasphemous, objectionable, defamatory, vulgar, obscene, pornographic, pedophilic, libelous, invasive of another's privacy, hateful, or racially, ethnically or otherwise objectionable, disparaging, relating or encouraging money laundering or gambling, or otherwise unlawful in any manner whatever
3. infringes any patent, trademark, copyright or other proprietary rights
4. violates any law for the time being in force
5. impersonate another person
6. contains software viruses or any other computer code, files or programs designed to interrupt, destroy or limit the functionality of any computer resource

Achieving E-Security through documented policies

The Policies required to e-secure an organization are listed below:

1. Information and Communication Technology Policy - A policy to govern the ICT structure of a company by providing the acceptable standards of IT usage or related services.
2. Privacy Policy - A policy to govern the collection, usage, handling, processing and disclosure of personal information / data of a customer. It is like reconciling privacy expectations with privacy rights.
3. Cyber Law Policy - A policy to seek compliance with the cyber laws for the time being in force in the Union of India such as the Information Technology Act, various 'Rules' and clarifications.
4. E-Security Policy - A policy to ensure that the basic computer security [e-security] perimeters are well in place. Perimeters like firewalls with secure passwords, correct maintenance of routers, encryption, etc.
5. Software Usage Policy - A policy to counter Soft-lifting, Counterfeiting, Renting, Original equipment manufacturer (OEM) unbundling, Uploading and downloading, Hard disk loading, etc with respect to software.
6. Internet Usage Policy - A policy to keep employees in line while they are online by banning inappropriate sites, prohibit the wasting of computer resources, enforce language guidelines, keep web copy clean and using various other measures to secure internet usage.
7. E-Mail Policy - A policy clarifying contentious points like E-Mail retention and deletion and rules to work by.
8. Cyber Insurance Policy - A policy to govern cyber insurance to help limit employment practices liability, limit E-mail risks, insure against

Copyright & Trademark Infringement, Patent Infringement, protect your computer assets and guard against E-Theft, to name a few.

9. E-Writing Policy - A policy formulated for safe and secure electronic writing understanding the employees' electronic writing concerns, managerial writing and assessing / addressing employees' electronic writing needs.
10. E-Crisis Communications Policy - An e-crisis management policy is document prepared on the lines of the long established formula 'hoping for the best, preparing for the worst'. The policy lays down guidelines for assessing the potential for electronic crises and the methodology to handle the crisis.

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.