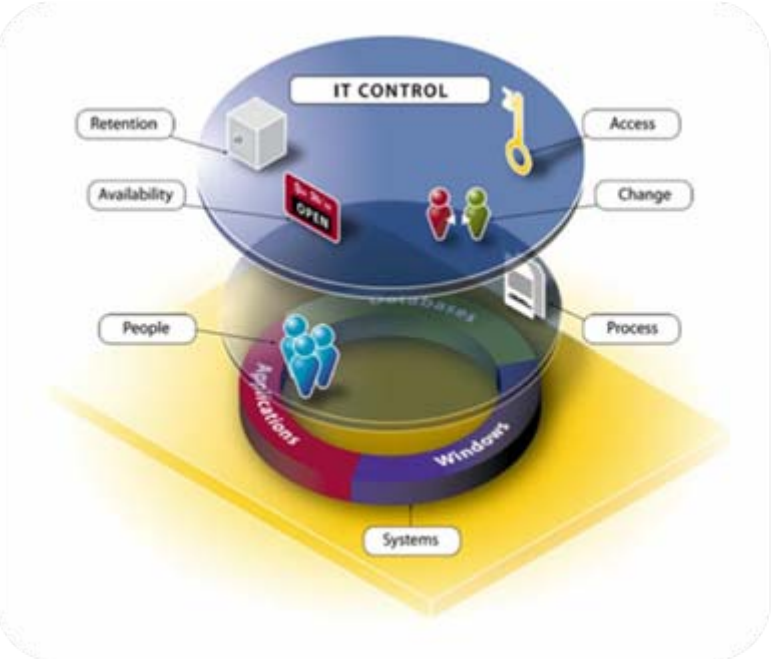

Sec. 43A Information Technology Act 2000 (IT Act) Compliance

Cases

- Nadeem Kashmiri and HSBC
- Karan Bahree and Mphasis
- Bazee.Com

Issues

- Liability of Company
- Protection of data – Concern for Outsourcing industry
- Privacy of data – Individual's concern

Sec. 43A – Compensation for failure to protect data

If body corporate, possessing, dealing or handling any **sensitive personal data or information** in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining **reasonable security practices and procedures** and thereby **causes wrongful loss or wrongful gain to any person**

- **Liability –** Damages by the way of Compensation

Adjudication

- The Adjudicating Officers (Secretary of the IT Dept) will have jurisdiction for cases where the claim is upto **Rs. 5 crore.**

- Above that, the case will need to be filed before the civil courts (Unlimited liability)

Sec 72(A) (Criminal offence)

- **Punishment for Disclosure of information in breach of lawful contract -**
- Knowling or intentionally disclosing "**Personal Information**"in breach of lawful contract
- Imprisonment up to 3 years or with fine up to 5 lakh or with both (Cognizable but Bailable)

Who is liable?

- **Sec.85**: Offences by companies
  - The company itself, being a legal person;
  - The top management including directors; and
  - The managers

  If it is proved that
  - they had knowledge of a contravention; or
  - they have not used due diligence
  - that it was caused due to their negligence

Issues

- What is ***Sensitive Personal Information***?

- What are ***Reasonable Security Practices and Procedures***?

The solution

- The Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011
- Enforceable from 11th April, 11
- To be read with Sec. 43A and Sec. 72A

Sensitive Personal Information

- Password;
- User details as provided at the time of
- Registration or thereafter;
- Information related to financial information such as Bank account / credit card / debit card, etc.
- Physiological and mental health condition;

Sensitive Personal Information

- Medical records and history;
- Biometric information;
- Information received by body corporate for processing, stored or processed under lawful contract or otherwise;
- Call data records;
- ***Exception:- Info available under RTI.***

Reasonable Security Practices

- Implementing comprehensive documented information security programme and information security policies
- Containing managerial, technical, operational and physical security control measures which are commensurate with the information assets being protected with the nature of business.

Reasonable Security Practices

- The International Standard IS/ISO/IEC 27001 on "Information Technology – Security Techniques – Information Security Management System – Requirements" is one such standard OR
- If following other than IS/ISO/IEC codes of best practices for data protection, shall get it duly approved and notified by the Central Government OR

Reasonable Security Practices

- An agreement between the parties regarding protection of “Sensitive Personal Information”

Auditing

- Necessary to get the codes or procedure certified or audited on regular basis
- Needs to be done by Government Certified Auditor
- Will be known as ***"Govt. Certified IT Auditor"***
- Not appointed yet
- CERT-IN has empanelled IT Auditing organisations

Benefits

- Compliance with legislation
- No liability on organisation U/Sec. 85
- Increased reliability and security of systems
- Systems rationalization
- Improved management controls
- Improved risk management and contingency planning

Collection of Information

- Necessary to obtain written consent from provider regarding purpose of usage before collection
- Provider should know –
  - Purpose of collection
  - Intended recipients
  - Details of the agency collecting the information; and agency retaining the information

Collection of Information

- Body Corporate not to retain information longer than required
- Option should be given to withdraw the information provided
- Shall appoint “Grievance Officer” to address any discrepancies and grievances about information in a timely manner – Max. time – One month

Privacy and Disclosure of Information policy

- Policy for handling of Sensitive personal information
- Shall be published on website or should be available to view/inspect
- Prior permission of provider necessary for disclosure to third party OR
- It is mentioned in the contract OR
- Necessary under Law

Contents of Privacy policy

- Type of personal or sensitive personal data or information collected
- Purpose of collection and usage of such information
- Disclosure of information including sensitive personal data or information
- Reasonable security practices and procedures as provided

Transfer of information

- Transfer to be made only if it is necessary for performance of lawful contract
- Body corporate to ensure same level of data protection is adhered while transferring


QUESTIONS

contact@sagarrahurkar.com

09623444448