Data privacy in india

Data is a set of values, it can be facts, numbers, text or images. The word data originated from a Latin word “ Datum” in mid 18 th century, which means “ something given”. Data that is accurately & timely organized & processed for a purpose and presented within a context that makes it meaningful & relevant forms an information. Information is very valuable asset as it can impact the behavior, decision or outcome of things.

In today’s technology world, with the tremendous use of Internet & rise in transfer of data, encompassing multiple technologies & geographies, preserving the data assumes a greater importance. Moreover, Privacy concerns also exist whereverpersonally identifiable informationis collected, stored & transferred in digital form or otherwise.

Article 21 of constitution of India speaks of right to life & personal liberty.

Thus, failure of disclosure controls can become the cause for privacy issues. Data privacy issues can arise as a result of information that are collected from different sources, such as:

- Medical & healthrecords
- Court proceedings or criminal records
- Bank details & transaction
- Biometrics & Genetic informations
- Residenceand geographic records
- Race &Ethnicity

The main challenge in data privacy is to process, stored & share data while protecting it.

Protecting the data comes in light due the susceptibility of data & increase rate of cyber crime. Cyber crime means any criminal activities done using the medium of computers, the Internet, cyber space and the worldwide web. To name a few cyber crime are : Hacking, Email spooling, Data theft, Identity theft, Spreading viruses & worms, etc.

Data theft is a potential crime resulting in data privacy breach which can happen due to the following

- Poor Networking / Internet connection Choices
- Improper Shredding/ Deleting/ Document Management Practices
- Identity Theft Resulting From Public Databases
- Tax Records Theft
- Inadequate Protection or Monitoring process
- Poor E-mailing Standards
- Failing to Choose a Secure Password
- Not Securing New Computers, Hard Drives & dongles, etc

Thus to address the above data privacy breach issues, the concepts of data protection were introduced in Information Technology Act 2000 (Amended 2008), through:

“ Section 43A, which deals with implementation ofreasonable security practicesforsensitive personal data or informationand provides for the compensation of the person affected bysuch data breach ”.

“ Section 72A, states that in case of breach of data privacy , there would be imprisonment for a period extending to 3 years and/or a fine which can be upto Rs. 5, 00, 000 for a person who causeswrongful loss or gainby

disclosing personal information of another person while providing services for the designated & lawful purpose as per contract.”

The Ministry of communication & Information Technology, released rules- IT (reasonable security practices & procedures & sensitive personal data or Information) Rules, 2011, which throws light on

1. Applicability

2. Collection of sensitive data

3. Processing of sensitive data

4. Access to sensitive data

5. Disclosure of sensitive data

6. Publication of sensitive data

7. Security measures & Penalties

1. Applicability:

The rule says that the Body corporate have to implement such security practices & standards that commensurate with the information assets protection policy.

Rules also set out that ISO 27001/IEC 27001 or any international standard in par with these standards could also be implemented by a body corporate.

The Body corporate needs to get certified/audited by an independent auditor approved by Central Government annually

2. Collection of sensitive personal data:

Data must be collected for a lawful purpose & for a function of the body corporate for which such data is required & necessary. Prior written consent of the data provider must be obtained for the data collection.

3. Processing and Retention of Data

The timeframes for retention of Sensitive Data is not specifically defined in the Data Privacy rules. However , it says that the rules do not override any provisions of any other laws, wherein it is specified that the maximum period of retention of sensitive data is for say 5 years or so.

Sensitive Data should be used only for the purpose for which it is collected & not otherwise. “ Section 67C of the IT Act requires the intermediaries to retains such information, and for such period of time, as mandated by the Central Government.

4. Access Restrictions

Sensitive Personal Data/ Information (SPDI) can be reviewed/amended by the information provider. They can withdraw the consent at any point of time as well. The rules provide that they could be transfer of SPDI in case of necessity for performance of lawful contract.

The detail procedure & the timeline within which the data provider has the right to access the information & make changes is not clearly defined in the Data privacy rules.

5. Disclosure of Information

SPDI can not be disclosed unless prior consent of the data provider is obtained. However, in the following instances such disclosures can be made

1. Under a provision of a contract between the body corporate and Provider; or
2. Made to Government agencies as stipulated by law to obtain Sensitive Data for the purposes of verification of identity, or for the prevention, detection, investigation, prosecution and punishment of offences, including cyber incidents; or
3. In pursuant to an order under the law.

6. Publication of sensitive data

Neither the body corporate nor the Data Processor are permitted to publish Sensitive Data in any manner. A third party that receives Sensitive Data from any body corporate or Data Processor is prohibited from disclosing it further.

A body corporate and a Data Processor are required to publish on their respective websites a privacy policy in regard to the processing of Sensitive Data

7. Security measures & Penalties

The Data Privacy Rules require that they must contain managerial, technical, operational and physical security control measures that are commensurate with the information assets being protected and with the nature of business.

The International Standard IS/ISO/IEC 27001 is recognized as an approved security practices that the body corporate or the information provider should implement to comply with security measures under the Data Privacy Rules.

If there is an information security breach, then the body corporate & information provider needs to prove that they have implemented the security control measures as per information security program and policies.

Body corporate has to appoint a Grievance Officer to resolve the grievances of the Data Provider. The communication details of the Grievance Officer must be available on the website of the body corporate. It is the duty of the grievance officer to resolve/address the grievances within 1 month.

Conclusion

Human resources, software , hardware, information security design can be utilized for addressing the data privacy issues. Ignorance of the implication of the Acts & regulation is a major hindrance. The laws & regulations relating to data protection are constantly changing thus its important to keep up-to-date of any changes & implement such procedures & practices to combat the Data privacy breaches. As the regulations & acts prescribes that such data privacy breaches are liable for criminal prosecution & penalties, it is the responsibility of SPDI Provider & the organization using the data to ensure proper & adequate controls are in place as a counter measure for such data privacy breaches.