Data Protection & Cyber Security Laws in India

Halder & Associates
Advocates | Delhi | India
August 2019

sushmita.haldar@halderassociates.com
priyanka.havelia@halderassociates.com
ajoy.halder@halderassociates.com

www.halderassociates.com

APPLICABILITY

To whom does it apply

- The date protection laws are applicable to all entities/individuals who are collecting and/or sharing personal data and/or personal sensitive data.

- For example, banks, retailers, infrastructure companies, etc.

APPLICABLE LAWS
&
REGULATIONS

Applicable Laws & Regulations

A. Constitution of India

B. Tort Law

C. Information & Technology Act, 2000 (IT Act)

D. IT (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ("Privacy Rules") read along with IT Act

E. EU's General Data Protection Regulation (GDPR)

F. Data Protection Bill, 2018 (*expected to be enacted soon*)

(A) Constitution of India

- The Supreme Court has held that the right to privacy is a **fundamental right** flowing from the right to life and personal liberty.
- **Individual dignity** is the basis for the right.
- The **sphere of privacy** includes **a right to protect one's identity**.
- This right recognises the fact that all information about a person is fundamentally her own, and she is free to communicate or retain it for herself.
- This **core of informational privacy**, thus, is a **right to autonomy** and **self-determination in respect of one's personal data**.

(B) Tort/Common Law

- Under common law (law which evolved with judicial pronouncement), **duty of care** is owed by one party to another, where there is a reasonably foreseeability that certain act or omission by one party may cause injure to the another party.

- Given the foreseeable risk of a data breach, the **entity (i) possessing, (ii) dealing or (iii) handling data**, owes a duty of care to safeguard the data in its custody.

- If there is **breach of this duty of care** resulting in injury and damage to the data holder, then the entity could be held liable.

- The court will typically look into the facts and circumstances, including the **reasonable security measures** that has been put in place before holding an **entity liable**.

(C) Information Technology Act, 2000

- **Scope**: IT Act protects personal data in India and is applicable to all body corporates.
- **Obligation**: Imposes an obligation on the entity that possesses, deals or handles any "**sensitive personal information"** to "**maintain reasonable security**" to protect such information.
- Currently, the law only protects "**Personal Information**" and "**Sensitive Personal Information**".
  - **Sensitive Personal Information: I**nformation relating to password, financial information, physical, physiological and mental health condition, sexual orientation, medical records and history, biometric information and details related to the above [Limited in definition]
  - **Personal Information**: Any information relating to an individual which (either by itself or in combination with other information available with a body corporate) is capable of identifying such individual.
- **Breach**: Where a body corporate is negligent/fails to maintain reasonable security practices and procedures causing wrongful loss, it is liable to pay damages by way of compensation to the person so affected.

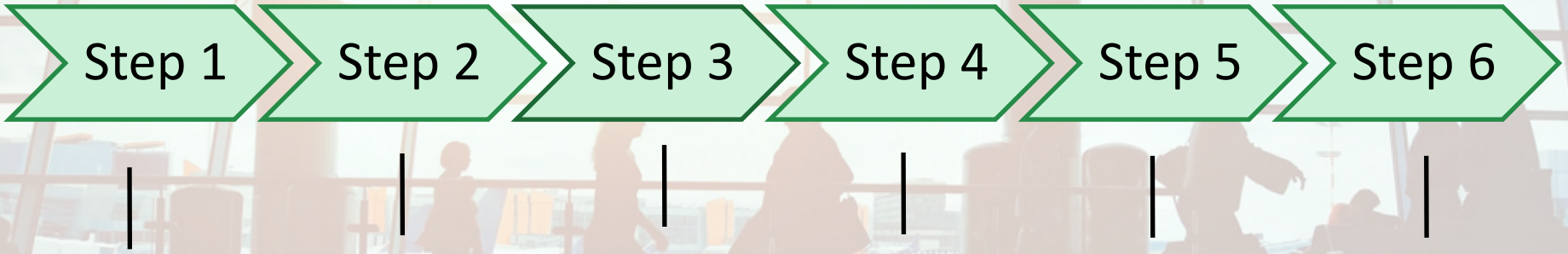
(D) Privacy Rules

- IT Act is to be read along with the Privacy Rules.
- Privacy Rules imposes obligations on the entity that **possesses**, **deals** or **handles** (i) "**personal information"** and (ii) "**sensitive personal information"**:
  - To maintain **Privacy** and **Disclosure Policy**;
  - Obtain consent from the provider of "**sensitive personal data**" for collecting and using the data;
  - Provide the data subject the right to **review and correct the data** or **withdraw consent**;
  - To **obtain prior permission** from the data subject before disclosure of data to any third party, except for Government agencies mandated under the law;
  - Transfer of information outside India is allowed provided the **same level of data protection** is adhered by such body corporate abroad and only if it is **necessary for the performance** of the lawful contract;
  - Maintain "**Reasonable Security Practices and Procedures"**; and
  - Appoint a **Grievance Officer** to redress the grievances of data subject

Reasonable Security Practices & Procedures

- Privacy Rules set out certain parameters with respect to the "**Reasonable Security Practices & Procedures**" for entities to comply with their legal obligations, these include:
  - Corporate to have a comprehensive documented information security program and information security policies.
  - Such security policies to include managerial, technical, operational and physical security control measures.
  - If there is a security breach, then the body corporate will be required to demonstrate that it has implemented relevant security control.
  - Corporate to conduct **audit of reasonable security practices and procedures** at least **once a year**.
  - **International Standard of IS/ ISO / IEC 27001** is one such standard which can be implemented by a body corporate to maintain data security.
  - Body corporate will be **deemed to have complied with security measure** if best practices have been **certified/audited on a regular basis through independent auditor** who is approved by the Central Government.

Steps – Compliance under IT Act & Privacy Rules



Appointment of Compliance Officer

Information Classification: "Personal Information" and "Sensitive Personal Information"

Formulation of Privacy Policy

Formulation of Disclosure Policy

Technical & Non-Technical Controls (Legal)

Yearly Audit

(E) GDPR

- **Purpose**: GDPR has been implemented to ensure that an uniform data security law is applicable to all EU members.

- **Extra-Territorial Jurisdiction**: GDPR is applicable to an entity not located in the EU, if such entity is to (a) offer free or paid goods or services to EU residents, or (b) monitor the behavior of EU residents.

- **Meaning of "Offer of Goods and Services"**:
  - Mere accessibility of the entity's website in the EU, of an email address or of other contact details, or the use of a language generally used in the third country is insufficient.
  - Applicability requires factors such as the use of a language or a currency generally used in EU States, possibility of ordering goods and services in that language, or the mentioning of customers or users who are in the EU.

- **Meaning of "Monitor the behavior of EU residents"**:
  - It should be ascertained whether natural persons are tracked on the internet.
  - Potential subsequent use of personal data, which consists of profiling a natural person in order to analyse or predict the data subject's personal preferences, behavior and attitude.
  - **Therefore, if a non-EU entity uses web tools that allow it to track cookies or the IP addresses of people who visit the website from EU countries, then it may fall within the scope of GDPR.**
  - **Practically, it may cause concern as an EU resident may accidently stumble upon a non EU entity website resulting its data being monitored.**

Obligations of Companies

Obligations under GDPS:

- A company can only **process personal data** under certain conditions:
  - the processing should be fair and transparent,
  - for a specified and legitimate purpose, and
  - limited to the data necessary to fulfil this purpose.

- **Pre-Conditions**: Personal data can only be processed on one of the following legal grounds:
  - Upon consent of the individual concerned.
  - A contractual obligation with the individual.
  - To satisfy a legal obligation.
  - To protect the vital interests of the individual.
  - To carry out a task that is in the public interest.
  - For the processor/company's legitimate interests, but only after having checked that the fundamental rights and freedoms of the individual whose data you are processing are not seriously impacted.

- **Security Measures**: GDPR provides for the requirement to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

Enforcement outside EU

Enforcement of GDPR outside EU:

- There is no clear guidance on how GDPR is to be implemented outside EU states. Principles of jurisdiction under international law will probably determine how the EU can exercise jurisdiction and whether such authority is lawful.

- It is plausible that Data Protection Authority (DPA) under GDPR could seek a court injunction in the non-EU countries to block a service if personal data is being unlawfully processed.

(F) Data Protection Bill, 2018

Reason for enactment of Data Protection Bill, 2018 ("Bill"):

- The existing law is no longer adequate.
- The definition of sensitive personal data is unduly narrow, leaving out several categories of personal data from its ambit.
- Data protection obligation is not applicable to the government.
- On a strict reading, the law can be overridden by contract.
- Implementation delays in appointments of the adjudicatory mechanisms created under the IT Act.
- The treatment of free data has been against the interest of the data provider.
- In the recent practices where Facebook had placed the interests of the individual whose information it shares secondary to the interests of companies which uses such data.
- Aligning the Indian law in-line with international laws.

Data Protection Bill, 2018

- **Scope**: The Bill is applicable to processing of personal data by:
  - both government and private entities incorporated in India, and
  - entities incorporated overseas, if they systematically deal with data subject within the territory of India.

- **Jurisdiction**: The Bill is based on the GDPR model and has been provided with extra-territorial jurisdiction.

Rights of Individual

- **Rights of the data subject/principal**: These includes:
  - the right to obtain a summary of their personal data held and the processing activities undertaken by the data fiduciary,
  - the right to seek correction of inaccurate, incomplete, or outdated personal data,
  - the right to have personal data transferred to any other data fiduciary in certain circumstances, and
  - right to restrict disclosure of personal data where such information has served the purpose, or was made contrary to law.

- **Exception**: The above rule does not apply:
  - if data is processed for the purposes of national security, prevention, investigation and prosecution of violations of a law, legal proceedings, personal or domestic purposes, and research and journalistic purposes.

  - the State may process data without consent for certain functions, such as for provision of services and benefits, and for issuance of certification, licences and permits.

Obligations of fiduciary/controller

- **Obligations of the data fiduciary/controller**: These include
  - processing personal data in a fair and reasonable manner,
  - notifying the data subject/principal of the nature and purposes of data collection, and their rights, among others, and
  - collecting only as much data as is needed for a specified purpose, and storing it no longer than necessary.

- **Issue**:
  - The Bill does not specify any principles or guidelines for what constitutes a ”**fair and reasonable**” manner of personal data processing.
  - The Bill mandates storage of a copy of personal data within India to expedite law enforcement’s access to data.

- **Security Measures:** The Bill imposes obligation on data fiduciary/ controller to put in place relevant security safeguards to protect the data.

Penalty & Regulator

- **Penalty for Breach**: Liable to a penalty which may extend up to **15 crore rupees** or **4%** of its total worldwide turnover of the preceding financial year, whichever is higher

- **DPA**: The Bill provides for the establishment of a Data Protection Authority (DPA). The DPA is empowered to:
  - draft specific regulations for all data fiduciaries across different sectors,
  - supervise and monitor data fiduciaries,
  - assess compliance with the Bill and initiate enforcement actions, and
  - receive, handle and redress complaints from data principals.

COMPLIANCE
&
RISK MITIGATION

Compliance & Risk Mitigation

A. Security Policy
B. Management Training
C. Employees Training
D. Vendors and Partners Training
E. Contract Management
F. Physical and Technical Safeguards

(A) Security Policy

- This is to include the privacy and disclosure policy. The policy will set out the requirements of the law and provide:
  - Clear and easily accessible statements of its practices and policies
  - Provide details of the 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 in place for the data

(B) Management & Employee Training

- **"Top-Down" approach and Management Training:** Top-Down approach to show management's commitment to the establishment, implementation, operation, monitoring, review, maintenance and improvement of the data security.
- Further, it shows that the management understands the seriousness, and initiates the process, which is then systematically percolated down to operations staff.
  - Senior managements, i.e., HR representatives, executives and other senior parties should participate in defining the content, structure and objectives of training programs for data security for employees and other third parties;
  - Regular management training must be organized with respect to data security; and
  - The Senior Management to spread the message of importance of cyber and data security to its employees and staff etc.
- **Employees Training:** As data will be collected, used and handled my employees on a regular basis, all such employees must be trained:
  - to understand the requirements under law, contracts and company policy;
  - to understand their role and responsibilities; and
  - mock training session with practical examples will help reduce the risk of theft, fraud or misuse of facilities.

(C) Vendor & Partner Training

- As data will often be disclosed to partners and third parties for performance of the services, it is important to ensure that such third party are in sync with need of the corporate;

- Help such third party to identify, evaluate and treat cyber risk and improve their organisation's security posture; and

- Undertake responsive measures to reduce business risk exposure to be within risk appetite, with constrained resources and within budget.

(D) Contract Management

The contract entered into between a corporate and a third party (to whom data is disclosed) will have an important role to play to ensure data security. The following may be followed:

- **Due Diligence**: Before entering into a contract, proper due diligence exercise needs to be conducted on the third party (vendor, partner, contractor etc.,) to ensure that:
  - parties are in alliance with each other,
  - correct data security measures are in place, and
  - in compliance with the data protection requirements of law.
- **Contract Content**: The contract should have specific clauses imposing obligation on the entity to comply with the relevant cyber security measures, clarifying the purpose and limitation including:
  - party will only process data based on the instructions of the corporate,
  - persons authorised to process data have committed themselves to confidentiality,
  - will comply with all obligations, including security measures required by law, and
  - will assist the corporate in ensuring compliance with applicable cyber security obligations.

Contract Management

- **Boilerplate IT Security Clauses in Contract**:
  - **Confidentiality**: The confidentiality clause should specifically cater to the requirement to keep data confidential and other requirements under law.
  - **Indemnity**: Indemnity clause should ensure that such third party indemnify the affected party for any breach of cyber security law.
  - **Warranties**: Party must give warranties with respect to the data in its possession. This will give certain additional rights to the corporate in case of breach of data security.
  - **Notice & Consent**: Consent is an important aspect of data security. Therefore, the notice provision should clearly provide procedure and the requirement to obtain consent, with respect to use, any changes etc.

- **Regular/Yearly Due Diligence**: Provision for auditing, inspection and examination must be incorporated in the contract, allowing the corporate to ensure that the relevant party is in compliance with the law.

(E) Physical & Technical Safeguards

- **Physical and environmental security**: To prevent unauthorized physical access, damage and interference to the organization's premises and information.

- **Technical Safeguards**: Corporate to put in place necessary firewalls and technical security to prevent any unauthorized access to the data/information.

- All such measures will be as per the latest technology and the requirement of law.

Thank you!

Halder & Associates Advocates

www.halderassociates.com