RSAConference2019
Asia Pacific & Japan
Singapore | 16–18 July | Marina Bay Sands

SESSION ID: PGR-R04

Future of Data Protection Legislation: India's Journey and Way Forward

Vikash Chourasia
Scientist 'C'

Government of India
Ministry of Electronics & Information Technology

Our Session:

- Future of Data Protection Legislation
- The core design principles adopted by India
- Glance on the features of the proposed Indian Data protection framework
- Re-engineering requirements from organizations
- Personal Data Protection Bill -2019 (PDPB) in comparison to GDPR.
- Proposed provisos around Data Localization & Cross-Border data flows.

India is rapidly transforming into a digital society

- The 21st century has witnessed exponential rise in a number of ways in which we use information, that it is widely referred to as **‘the information age’**
- Global societies are transiting to a largely digital economy wherein the processing of personal data has already become omnipresent
- The reality of the digital environment today, is that almost every single activity undertaken by an individual involves some sort of data transaction – this is happening all across the world in different economies.
- Some of the largest companies in the world today are data driven.

Digital society without Data Protection Norms

While data can be put to beneficial use, the unregulated and arbitrary use of data, especially personal data, has raised concerns regarding the privacy and autonomy of an individual.

Without data protection…

Increased surveillance

Profiling of individuals

An Impact on individual independence

RSAConference2019
Asia Pacific & Japan

Global scenario : Data protection legislation

What was happening around the globe

APPROACHES TO DATA PROTECTION

The EU model provides a comprehensive data protection law (EU-GDPR) for processing of personal data. GDPR to come into effect from 25th May 2018.

No comprehensive set of privacy rights/principles that collectively address the use, collection and disclosure of data in the US except for California. There are sector specific regulation HIPPA, GLBA etc.

Stresses circumstances of collection, use and disclosure rather than always using an umbrella term of processing. It is less prescriptive in other aspects; eg. Sensitive personal data.

Australia differentiates amongst data controllers, i.e. between state actors and non-state actors and also between small businesses and other commercial enterprises.

The california consumer privacy act of 2018

June 28, 2018, a landmark privacy bill that is being compared to the EU General Data Protection Regulation for its overarching approach and strong privacy protections.

Which is to be Effective from January 1, 2020.

Consumers have the ability to request a record of what types of data an organization holds about them, plus information about what's being done with their data in terms of both business use and third-party sharing.

Organizations will have to disclose to whom they sell data, and consumers will have the ability to object to the sale of their data. Businesses will have to put a special **"Do Not Sell My Personal Information"** button on their web sites to make it easy for consumers to object.

RSAConference2019
Asia Pacific & Japan

India’s progress

ensuring citizen’s data protection

Evolution of Privacy Legislation and Data Protection

- A landmark judgment by the nine Judge Constitution Bench of the Supreme Court of India on 24.8.2017 declaring Privacy as a Fundamental Right under Article 21 of the Constitution. The Court impressed upon the Government to bring out a robust data protection regime

Court Observed : Privacy is a constitutionally protected right which emerges primarily from the guarantee of life and personal liberty in Article 21 of the Constitution. Elements of privacy also arise in varying contexts from the other facets of freedom and dignity recognized and guaranteed by the fundamental rights contained in Part III; Informational privacy is a facet of the right to privacy.

Constitution of Expert Committee :

To study various issues relating to data protection in India, an expert committee on Data Protection, under the chairpersonship of Justice B.N. Srikrishna (Retd.) in July 2017

The committee submitted its Report along with a draft bill in July 2018.

Consultative process of coming on to a draft bill

- Release of White paper: as Concept Note
- Solicited Public comments White Paper
- Deliberations on the input received.
- Expert Committee drafted comprehensive draft bill & Submitted its report
- Stakeholder consultations on the draft bill

The core design principles adopted by India

Technology agnosticism

- Flexible to take into account changing technologies

Holistic application

- The law must apply to both private sector entities and government.

Informed consent

- Consent must be informed and meaningful.

Data minimization

- Data to be minimal and necessary for the purposes for which such data is sought

Controller accountability

- The data controller shall be held accountable for any processing of data

Structured enforcement

- Enforcement must be by a high-powered statutory authority

Deterrent penalties

- Penalties must be adequate to ensure deterrence

Glance on the features of the proposed Indian Data protection framework

- Obligations of data fiduciary- includes prohibition of processing of personal data except for specific, clear and lawful purpose, limitation on purpose of processing and collection, requirement of notice for collection or processing and restriction on quality and retention of personal data, accountability and mandatory consent of data principal for processing of his personal data;
- Grounds for processing of personal data without consent in certain cases, such as in the performance of functions of the State, in compliance with a law or any order of any court or tribunal, and in medical emergencies, etc.;
- Special treatment of personal data of children;

- Rights of data principals, such as right to confirmation and access, correction and erasure of personal data, portability and right to be forgotten, etc.;
- Transparency and accountability measures to be developed and complied with by data fiduciary and data processor, data protection impact assessment, maintenance of records, audit of policies and conduct of processing, etc., and providing for grievance redressal by every data fiduciary;
- Exemptions from the application of the provisions of the Act to certain agencies on certain grounds and for research, archiving or statistical purposes, etc.; and creation of a Sandbox for encouraging innovation, etc.;

- Establishment of a Data Protection Authority of India which shall, among other things, monitor and enforce the application of the provisions of the Act, take prompt and appropriate actions in response to data security breach, receive and inquire into complaints for violation of rights of data principals under this Act or violation of security, transparency and accountability measures.
- Penalties and compensation for violation of the provisions of the Act and adjudication by Adjudicating Officer, constitution of Appellate Tribunal for hearing appeals, etc., and for offences for contravening certain provisions of the Act;

Re-engineering requirements from organizations

- Organizations need to create a robust privacy framework consistent with the obligations specified under PDPB. The bill categorizes organizations as Data Fiduciaries (DF) and Significant Data Fiduciaries (SDF) (to be notified by the DPA) and imposes the following obligations on them:

Data Protection Officer

Record Keeping

Data Protection Impact Assessments

Contractual Requirement with Processors

Privacy by Design

Maintain Transparency

Timely Breach Notification

Data Audits

Grievance redressal

Personal Data Protection Bill -2019 in comparison to GDPR

- The core principles of GDPR such as 'Lawfulness, Fairness and Transparency', 'Purpose Limitation', 'Collection Limitation', 'Data Quality', 'Storage Limitation', and 'Accountability' formulate part of the proposed PDPB as well.

- The definition of individuals under PDPB extends to the residents as well as the citizens, similar to the definition of a natural person under GDPR.

- The major rights of the data subjects under GDPR such as 'right to correction', 'confirmation and access', 'right to portability' and 'right to be forgotten 'will be extended to the data principals under PDPB too.

- Obligations on data fiduciaries on maintaining records of processing, conducting DPIAs, timely notification of breaches and appointing a DPO are very much similar to the obligations put on the data controllers under GDPR
- Penalties fines of 2 percent or 4 percent of the global turnover proposed are similar to fines proposed under GDPR.

Proposed provisos around Data Localization & Cross-Border data flows.

- We are in general supportive of global free flow of data, subject to protecting privacy of our citizens.
- Our data protection law will soon be placed in Parliament for consideration. It proposes framework for protection of citizen's privacy.
- The proposed data regulator in consultation with sectoral regulators will specify certain types of data on which there will be some constraints in line with local laws and to provide for safeguards.
- The bill also provides for reaching adequacy recognition with other countries or regions in order to facilitate free flow of data.

“Apply” Due Diligence- Be Prepared

- Legislations on Personal Data Protection are inevitable. If not deploying dedicated teams & resources, at least start preparing, think of how you will fulfill these most common requirements:
  - Data Protection Officer
  - Record Keeping from privacy view point
  - Contractual Requirement with Processors
  - Inducting Privacy by Design in processes
  - Breach Notification strategies
  - Grievance redressal mechanisms best suited to your businesses.

RSAConference2019
Asia Pacific & Japan

Thank you.