Deloitte.

Enabling Data Privacy

What does this imply for an organization?

Although India's Data Protection Act is yet to be released, however based similar institutional decisions around the globe and growing Privacy regulations, its anticipated that Indian organizations are likely to have a profound impact on their operational and control environment, including:

- Processes and technical solutions deployed across data (personal data) lifecycle, starting from collection to creation to destruction such as:
  - Privacy by design
  - Notice and Consent management
  - Monitoring and data breach notifications
  - Data access and security
  - Processing data for defined purpose and time
  - Keeping a record of processing activities
  - Privacy impact assessments
  - Data Subject Rights – right to erasure
  - Accountability

- Governance framework to drive privacy within an organization

- Culture of privacy in the organization

Privacy – a Fundamental Right

On August 24, 2017 Honourable Supreme Court of India delivered a historic judgment that privacy is a constitutionally protected right which not only emerges from the guarantee of life and personal liberty in Article 21 of the constitution, but also arises in varying contexts from the other facets of freedom and dignity recognized and guaranteed by the fundamental rights contained in Part III of the Indian Constitution.

How can privacy be viewed 'holistically'?

Privacy in essence aims to safeguard data and information that may establish an individual's identity, preferences, activities, etc. It's critical to enhance and strengthen the current practices that govern almost everything from creation, processing, storing, and finally 'destruction' of personal data that belongs to individuals.

A Holistic View of Privacy

Govern: Create a comprehensive Privacy Framework that assigns accountability for its privacy policies & procedures, defines the roles & responsibilities, and aligns with the Information Technology (IT) 2000, and IT (Amendment) Act, 2008.

Assess: Create adequate controls in place for use, processing, storage, transfer and destruction of the data that is being collected.

Protect: Put technological safeguards in place to protect personal data. Privacy must be incorporated by design, within the process.

Monitor: Standardize metrics for Privacy adherence especially against the requirements. Monitor processes, systems and networks to identify data access, use, changes and breaches.

Respond: Create an adequate process to identify and respond to data breaches.

How can Deloitte help?

Data leakage protection

Privacy framework development

Privacy impact assessment

Implementing privacy

Privacy strategy and roadmap development

Privacy breach management

Data discovery, mapping, and inventories

Developing a culture of privacy (via trainings)

Privacy-by-design

Sustaining privacy

Privacy assessment & health check

Assessment against the India IT Act requirements

Key Contacts

Anthony Crasto
President, Risk Advisory
Deloitte India
acrasto@deloitte.com

Abhijit Katkar
Partner, Risk Advisory
Deloitte India
akatkar@deloitte.com

Kamaljit Chawla
Leader – Cyber Operate
Risk Advisory, Deloitte India
kamaljitc@deloitte.com

Tarun Kaura
Leader – Cyber Advisory
Risk Advisory, Deloitte India
tkaura@deloitte.com

Manish Sehgal
Partner, Risk Advisory
Deloitte India
masehgal@deloitte.com