Regulatory, Policy and Government view

on

Digital Personal Data Protection Act, 2023 (DPDP Act)

27th National Conference on e-Governance, 2024

4.9.2024

Amit Agrawal

Flow of presentation

- India’s approach to personal data protection
- Key provisions of DPDP Act
- Reorienting for digital personal data protection

India’s approach to personal data protection

Essence of the approach

- Principles in alignment with global norm
- Difference lies in the approach adopted:
  - Aim — Protects personal data, and also enable its processing
  - Digital-by-design — Both in its scope & application
  - SARAL — Simple, Accessible, Rational & Actionable Law
  - Makes existing processing accountable without disrupting it
  - Ease of Living and Ease of Doing Business ensured

Principles

- Lawful and fair use
- Purpose limitation
- Data minimisation
- Data accuracy
- Storage limitation
- Reasonable security safeguards
- Accountability

SARAL: Simple, Accessible, Rational & Actionable Law

- Short – 9 chapters & 44 sections
- Easy-to-understand, plain language
- Illustrations
- No provisos
- Minimal cross-referencing
- Only rules, no regulations

Introducing law without disruption

- Pre-existing consent to be notified to persons whose personal data is being processed
- Processing without consent may be done only for certain legitimate uses
- Enables processing outside India, while retaining India’s right to restrict it
- Suitable exemptions
- Other laws apply – Unless inconsistent

Ease of Living & Ease of Doing Business

- Principles laid down, avoiding prescriptive approach & intrusive regulation
- No multiple data classes — All data uniformly protected
- Alternate Dispute Resolution & Voluntary Undertaking for faster resolution
- Digital means recognised for fulfilling obligations, exercising rights & resolving issues

Freedom with responsibility

- Only obligations laid down, not the manner of discharging them
- No regulator
- Functional freedom for lawfully processing entities to decide the manner in which they would discharge their obligations
- This freedom comes with responsibility:
    - To read, understand & discharge obligations
    - To establish compliance if adjudicated

Key provisions of DPDP Act

Four foundations

- Protects “**digital personal data**” – Data by which an individual may be identified
- Lays down rights & duties of “**Data Principal**” – The individual to whom the data relates
- Lays down obligations of “**Data Fiduciary**” – The individual/company/govt entity processing personal data
- Rights, duties & obligations are specified in relation to “**processing**” – Any operation with respect to personal data, including mere collection or storage of data

Applicability

- Applicable to processing in India of personal data—
  - In digital form
  - Collected in non-digital form and digitised subsequently
- Not applicable to processing of personal data—
  - Made publicly available by law
  - Made publicly available by Data Principal
  - For personal or domestic purpose
- Applicable to processing outside India for offering goods & services in India

Requirements to be met for processing

Processing should not be for purpose forbidden by law & should be done—

- Only with consent, or
- For certain legitimate uses

Consent and notice

- Notice specifying purpose must be given before or at the time of requesting consent
- Consent to be free, specific, informed and unambiguous
- Consent valid only for data which is necessary for specified purpose
- Consent withdrawable at any time, with same ease as that of giving consent
- Notice & request for consent viewable in any 8th Schedule language & English

Certain legitimate uses

- Compliance with judgement or legal order
- Protection/assistance/service during medical emergency, disaster or public order
- For employment purposes
- In relation to employees, for safeguarding employer from potential loss/liability or for giving benefit/services
- When individual submits data voluntarily for a particular purpose
- Certain functions of the State & its instrumentalities

Obligations of Data Fiduciary

- To engage or involve a Data Processor only under a valid contract
  - However, liability for non-compliance rests with Data Fiduciary
- Intimation of breach to Data Principals & Data Protection Board
- Reasonable security safeguards to prevent personal data breach
- Implement technical & organisational measures to ensure compliance
- Ensure completeness & accuracy of personal data
- Erase data when no longer needed for specified purpose
- Establish effective grievance redressal system
- Publish contact details for answering queries

Processing of children’s data

- To process only with parental consent
- To not do processing which is detrimental to children's well-being
- To not track, behavioural monitoring or targeted advertising
- Processing without parental consent or/& with tracking etc. may be allowed for purposes & for classes of Data Fiduciaries prescribed by rules

Rights of Data Principal

- Right to access information about personal data
- Right to correction and erasure of personal data
- Right of grievance redressal
- Right to nominate another person to exercise these rights in case of incapacity or death

Exemptions

- Exemption from obligations other than reasonable security safeguards:
  - To perform judicial, regulatory & supervisory functions under law
  - To enforce legal rights & claims
  - To prevent/detect/investigate/prosecute offences or contraventions of law
- Certain exemption to startups to reduce compliance burden
- Outright exemption
  - For research, archiving or statistical purposes
  - Notified State instrumentalities for reasons of security, sovereignty, public order etc.

Reorienting for Digital Personal Data Protection

DPDP readiness as business strategy

- Legal certainty is already there — Rules will only mention procedure
- There is freedom to choose appropriate organisational & technical measures
- Since principles are aligned with global norms, global practices may be leveraged
- Since obligations are simple & broad, adherence can be readily secured by automation
- Adherence will ensure sound data management, reduce risk & enhance customer trust

Therefore, proceeding to implement the principles is sound business strategy

Basics for DPDP readiness

- Identify all personal data held & locate the consent for its processing
- Delete unnecessary data & data held without consent (or obtain consent)
- Begin clearly stating the purpose while seeking consent & collect only necessary data
- Equip Principals to digitally know & update data, seek redress & make nominations
- Get both applications & hosting infrastructure comprehensively audited & secured
- Define & minimise internal data access rights
- Keep data encrypted at rest and in motion
- Review contracts with agencies/vendors & monitor/audit for compliance

Thank you