AZB & PARTNERS
ADVOCATES & SOLICITORS

DECODING THE DATA PROTECTION FRAMEWORK IN INDIA

March 25, 2021

Current Legal / Regulatory Landscape in India

- Information Technology Act, 2000 - Section 43-A + IT (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.

- Simplistic consent-based regime.

- Applicability - Sensitive personal data OR personal data

- Sensitive personal data – Includes passwords, financial information (bank account or credit card or debit card or other payment instrument details) (Financial Data), physical, physiological and mental health condition, sexual orientation, *medical records and history*, biometric information (*Health Data*).

- Personal data/ information – information that *relates to a natural person* which, either *directly or indirectly*, in combination with other information available or likely to be available with a body corporate, *is capable of identifying such person*.

Current Legal / Regulatory Landscape in India

- Prior written consent required regarding purpose of usage.
- Lawful purpose connected with the function of the entity collecting Sensitive Personal Data & collection of such data should be essential for that purpose.
- Principles of purpose and storage limitation.
- Providing an option not to provide Sensitive Personal Data.
- Prior permission for disclosure of Sensitive Personal Data. Exceptions – Disclosure as may be required by law or requests received from Government agencies for certain prescribed purposes.
- Sensitive Personal Data cannot be published.
- Third parties who receive Sensitive Personal Data cannot disclose it further.
- Cross-border flow of Sensitive Personal Data is permitted freely. Only security procedures need to be implemented.

Current Sector Specific Requirements

Financial Services:

- Reserve Bank of India: Circular dated April 06, 2018, RBI Guidelines on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds dated April 29, 2011 read with RBI Cyber Security Framework in Banks circular dated June 02, 2016 ("RBI IT Guidelines") applicable to banks; RBI Master Direction - Information Technology Framework for the NBFC Sector dated June 08, 2017 applicable to NBFCs ("NBFC IT Guidelines")

Securities:

- Securities Exchange Board of India: SEBI Cyber Security & Cyber Resilience frameworks for specific intermediaries, *viz*. stock exchanges, clearing corporations, depositories, stock brokers, depository participants, registrars to an issue/ share transfer agents, KYC registration agencies and mutual funds ("SEBI Cyber Security Framework")

Insurance:

- Insurance Regulatory and Development Authority: Guidelines on Information and Cyber Security for insurers dated April 07, 2017 ("IRDA Cyber Security Guidelines")

Medical / Health:

- National Medical Commission Act, 2019 (replaces the Indian Medical Council Act, 1956).
- Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations, 2002.
- Telemedicine Practice Guidelines, 2020.
- Pharmacy Act and the Pharmacy Practice Regulations, 2015.
- Clinical Establishments (Registration and Regulation) Act, 2010 and the Clinical Establishments (Central Government) Rules, 2012.
- Drugs and Cosmetics Act, 1940 and the New Drugs and Clinical Trials Rules, 2019.

EVOLUTION – MAJOR MILESTONES

Puttaswamy Decision – Privacy is a fundamental right	August 2017
Personal Data Protection Bill, 2018	July 2018
Personal Data Protection Bill, 2019	December 2019
Referral to JPC	February, 2020
Non-Personal Data Governance Framework	July 2020
JPC, stakeholder consultations and present status	December 2020

SNAPSHOT - PDP, 2019 | APPLICABILITY

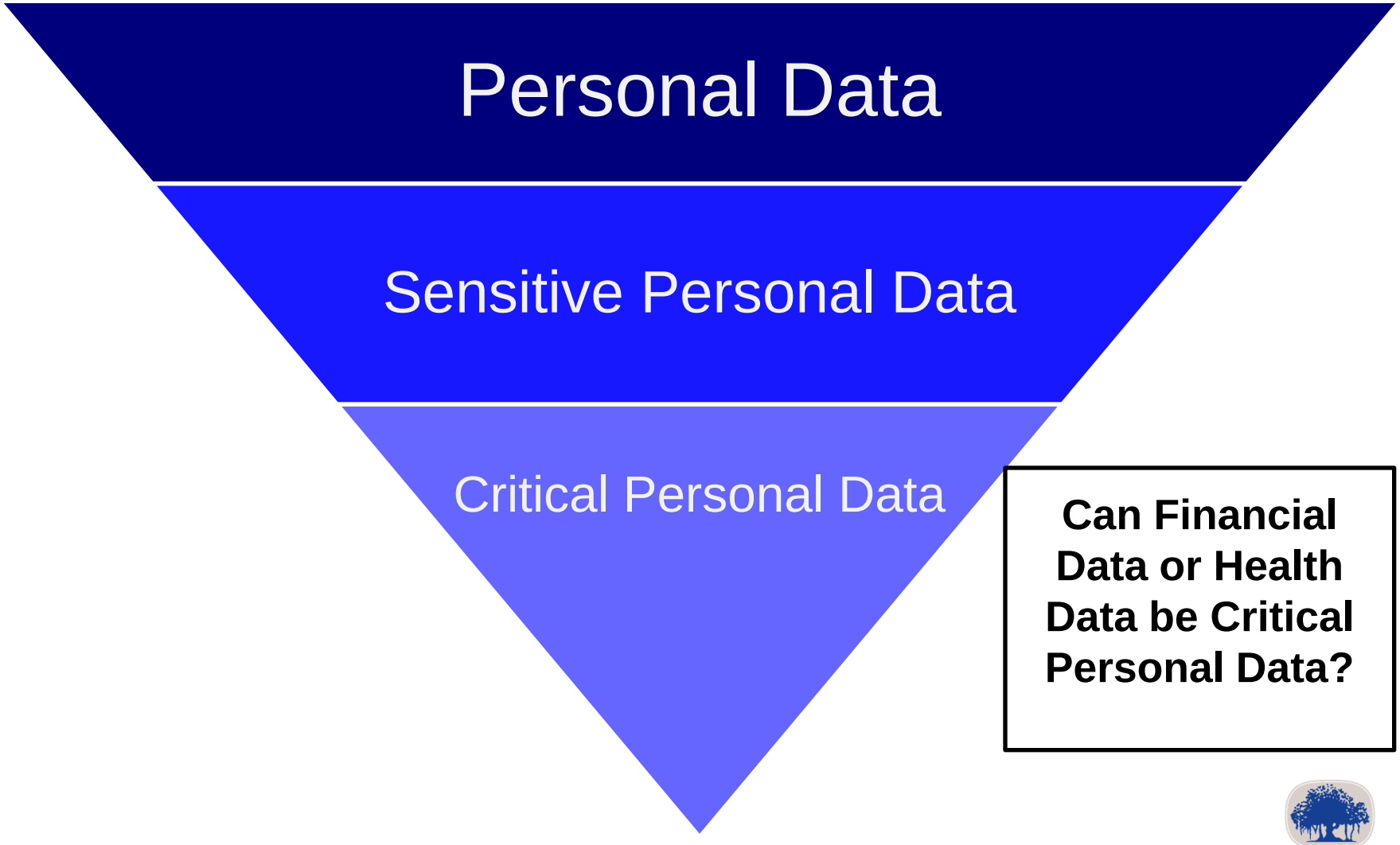
Territorial	Extraterritorial
➢ Where 'personal data' is collected, disclosed, shared or processed within India. ➢ To State, Indian company, Indian citizen or body of persons incorporated under Indian law. ➢ To data collected online or offline.	➢ Applies to overseas entities. ➢ Applies to such overseas entities who process personal data in connection with: • any business in India; • any systematic activity of offering goods or services to 'data principals' within the territory of India; and • any activity which involves the profiling of 'data principals' within the territory of India.

AZB & PARTNERS
ADVOCATES & SOLICITORS

PDP, 2019 | KEY TERMS

- "**Processing**" - operations performed on 'personal data'. Operations could include - collection, recording, organizing, storing, using, disclosure by transmission, erasing, destruction etc.
- "**Data Principal**" - *the natural person* (i.e. individual) to whom the 'personal data' relates.
- "**Data Fiduciary**" - who determines the purpose and means of processing personal data.
- "**Data Processor**" - who processes 'personal data' *on behalf of* a 'data fiduciary'.
- "**Personal Data**" – Data about natural persons (directly or indirectly identifiable), having regard to characteristic, attribute, trait or other features of identity (including a combination of such features with any other information) and includes inference drawn from such data for the purpose of profiling.
- "**Sensitive Personal Data**" – Data which *reveals or relates to health data, sexual orientation, biometric data, genetic data*.
- "**Health Data**" – Data relating to *physical or mental health*. Includes *medical records* regarding state of health, *data collected for provision of health services*.
- "**Genetic Data**" – Data relating to inherited or acquired genetic characteristics which give unique information about behavioral characteristics, physiology or health of natural person and which result, in particular, from an analysis of biological sample from the concerned natural person.

PDP, 2019 | DATA CLASSIFICATION



Can Financial Data or Health Data be Critical Personal Data?

AZB & PARTNERS
ADVOCATES & SOLICITORS

PDP BILL, 2019 | KEY PRINCIPLES

- ***Impact of Puttaswamy*** *- No processing of personal data, unless provided by law.*

- Processing only for *specific, clear and lawful purposes*.

- **Purpose Limitation - Strengthened**

  - Thumb rule is that processing should be *fair and reasonable and should ensure privacy of the individual*.
  - Processing *only for consented purposes* or *incidental purposes – To be judged from the lens of the 'data principal'*.
  - Vague / catch-all consent languages will not work.

- **Storage Limitation – Strengthened**

  - Specify the period in the privacy policies.
  - Storage for longer duration only permissible under exceptional circumstances.
  - Periodic reviews to ascertain if personal data is required to be retained.

- **Collection limitation – Strengthened**

  - Collect personal data only to the extent necessary.
  - Provision of goods and services *cannot be conditional on processing of personal data which is not required for that purpose*.

PDP Bill, 2019 | PROCESSING HEALTH DATA – WITH CONSENT

- *Consent* v *Explicit Consent*
- **Consent** -
  - Free – Complies with contract law standards;
  - Informed – Need to be in the prescribed form and contain relevant details;
  - Specific – Data principals should be able to determine the scope of consent;
  - Clear – Meaningful affirmative action;
  - Capable of being withdrawn – As easily as consent was given.
- **Explicit Consent** -
  - New concept and *applicable to 'sensitive personal data' including health data*.
  - Constituents of Explicit Consent: -
    - Informed – Data principals should know about processing likely to cause significant harm;
    - Clear – No inference from conduct;
    - Specific - Choice of separately consenting to different purposes and different categories of 'sensitive personal data'.
- How can data fiduciaries obtain explicit consent for processing health data.

PDP BILL, 2019 | CROSS-BORDER TRANSFER

Scope	Personal Data	Sensitive Personal Data (including Health Data)	Critical Personal Data
Consent requirement	Not contemplated (Required for "*processing*")	Explicit consent	Not specified
Conditions of transfer		One copy in India AND *Adequacy principle* OR Approved contract / intra-group schemes OR DPA allows transfer for a particular purpose	Permitted only in certain exceptional circumstances. • Transfer to entity engaged in health / emergency services in case of threat to life. Notify DPA. • Transfer on the basis of *adequacy principle* provided Central Government believes that transfer is not prejudicial to security and strategic interest.

AZB & PARTNERS
ADVOCATES & SOLICITORS

PDP BILL, 2019 | RIGHTS OF DATA PRINCIPALS

- Rights have been codified.
- Rights available to data principals include: -
  - Right to confirmation and access.
  - Right to correction and erasure.
  - Right to data portability.
  - Right to be forgotten.
- Procedure to exercise these rights has been prescribed.
- Existence of rights, procedure to exercise them and related contact details need to be specified in the privacy policy.

PDP BILL, 2019 | SECURITY BREACHES

- Security breaches to be notified to the DPA, if likely to cause "harm" to data principal.

- Following details need to be provided: -

  - Nature of personal data under breach;
  - Number of data principals affected;
  - Possible consequences;
  - Action taken to remedy the breach.

- DPA will determine if breach needs to be notified to data principals.

- DPA can: -

  - Require remedial action to be taken;
  - Require data fiduciary to conspicuously post details of breach on its website;
  - Independently post details of breach on DPA website.

PDP BILL, 2019 | OTHER IMPORTANT CONCEPTS

- Security safeguards.
- Significant data fiduciaries and guardian data fiduciaries.
- Transition.

PENALTIES

- IT Act – Compensatory in nature.

- PDP Bill – Penalties depend on the nature of offence.

  - Processing of health data without appropriate consents / transferring of health data in violation of the applicable provisions - Monetary penalties up to the higher of – INR 15 crores (USD 2,100,000 approx.) or 4% of the total worldwide turnover of the preceding financial year.

  - Knowingly or intentionally re-identifying personal data which has been de-identified without consent – Imprisonment up to 3 years and/or fine up to INR 2 lakhs (USD 2,800 approx.).

  - Offences by companies.

  - Compensation to data principals.

Considerations for Stakeholders

- High volume of personal data, increased compliance costs – qualifies such entity as a significant data fiduciary.
- Storage of data in ‘anonymized form’.
- Consent and Purpose – *best practices that may be implemented today to ensure compliance?*
- Robust and publicly available privacy policy standards.
- Data localization and its impact on foreign investment?

Q&A

vipul.jain@azbpartners.com

nandan.pendsey@azbpartners.com

AZB & PARTNERS
ADVOCATES & SOLICITORS

THANK YOU

AZB & PARTNERS
ADVOCATES & SOLICITORS