

Cross-Border Data Transfers



Existing Indian Data Protection Rules: A Recap

- Applicability: Section 43A of the Information Technology Act, 2000:

³[43A. **Compensation for failure to protect data.**—Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected.

- What is “sensitive personal data or information”?
- What are penalties for non-compliance, and how does enforcement work?

Existing Indian Data Protection Rules: A Recap



7. Transfer of information.-A body corporate or any person on its behalf may transfer sensitive personal data or information including any information, to any other body corporate or a person in India, or located in any other country, that ensures the same level of data protection that is adhered to by the body corporate as provided for under these Rules. The transfer may be allowed only if it is necessary for the performance of the lawful contract between the body corporate or any person on its behalf and provider of information or where such person has consented to data transfer.

- Same level of data protection.
- Consent or where necessary for the performance of a contract.

Localisation



Upcoming Law: Data Categories



Personal Data

Online or offline data that directly or indirectly, and with respect to characteristics, attributes, traits, or other identity features, identifies an individual.

Any data that identifies an individual when in combination with another data point, is considered personal data too.



Sensitive Personal Data

Certain categories of personal data:

- health or financial data,
- Official identifiers,
- biometric data,
- genetic data,
- sex life or sexual orientation,
- transgender data or intersex status
- caste or tribe,
- religious or political beliefs, and
- any other data notified by the Central Government.



Non-Personal Data

**Critical
Personal
Data**

CROSS-BORDER DATA TRANSFERS

SENSITIVE PERSONAL DATA

In addition to explicit consent, data must be transferred based on:

- ❖ a contract or an intra-group scheme approved by the DPA in consultation with the govt.;
- ❖ an adequacy decision by the Central Government; or
- ❖ an approval by the DPA in consultation with the govt for a specific purpose.

CRITICAL PERSONAL DATA

Can only be transferred to:

- ❖ a person or entity engaged in health or emergency services or related purposes; or
- ❖ country or an entity approved by the Central Government with respect to security and strategic interest of the State.

LOCALISATION

SENSITIVE PERSONAL DATA

A copy of all sensitive personal data must be stored in India.

Data mirroring would be an efficient practice.

Sectoral requirements (for example, RBI regulations on financial data) may be more stringent.

CRITICAL PERSONAL DATA

Mandatory data localisation.

Exemptions limited to state sanctions and health emergencies.

Penalties



Up to INR 15,00,00,000 or 4% of the total worldwide turnover of the preceding financial year.