ADVOCATES & SOLICITORS

THE GLOBAL DATA HIGHWAY

A PRACTICAL GUIDE TO CROSS-BORDER DATA TRANSFERS

Unlocking Cross-Border Data Transfers, Navigating Compliance, Safeguards, Operational Insights, and Strategic Frameworks under India's DPDP and RBI Mandates

Prepared by:

Ak & Partners

2025

About the Founders

Anuroop is known for his strategic counsel to foreign investors, financial institutions, and fintech companies in India. With a decade of cross-border advisory experience, he has led mandates across banking regulation, digital lending, and insolvency turnaround. His blend of legal insight and commercial foresight makes him a trusted advisor. Anuroop is also a noted speaker and author on fintech policy and RBI regulations. He is committed to delivering fast, viable, and regulatorily sound solutions.

Anuroop Omkar
Managing Partner

Kritika specialises in business advisory, from developing the most efficient strategy to expanding the business with growth capital, along with managing all material risks that come in the way. She advises banks, fintechs, and global investors on regulatory strategy, negotiations, enforcement, and cross-border transactions, with expertise in digital lending, PPI, and financial regulation. A published author and speaker on fintech governance, she is known for her fast, solution-driven, and business-aligned approach.

Kritika Krishnamurthy
Managing Partner

Awards & Recognitions

Chambers RANKED IN FinTech 2025 Leading Firm

The LEGAL 500 ASIA PACIFIC TOP TIER LIST 2023

The LEGAL 500 ASIA PACIFIC LEADING FIRM 2024

The LEGAL 500 ASIA PACIFIC INDIA CITY FOCUS 2023

The LEGAL 500 ASIA PACIFIC INDIA CITY FOCUS 2024

IFLR1000 RECOMMENDED FIRM 2024

BW LEGAL WORLD 40 UNDER 40

Forbes India Presents LEGAL POWERLIST 2020 in association with legitquest BANKING & FINANCE ENLISTED AS THE TOP LAW FIRM

Forbes India Presents LEGAL POWERLIST 2021 in association with legitquest BANKING & FINANCE ENLISTED AS THE TOP LAW FIRM

Forbes India Presents LEGAL POWERLIST 2022 in association with legitquest BANKING & FINANCE ENLISTED AS THE TOP LAW FIRM

Forbes India Presents LEGAL POWERLIST 2023 in association with legitquest BANKING & FINANCE ENLISTED AS THE TOP LAW FIRM

ALB INDIA FIRMS TO WATCH 2023 THOMSON REUTERS

RECOGNIZING EXCELLENCE IN CLIENT SERVICE CLIENT CHOICE

INDIA BUSINESS LAW JOURNAL AWARD WINNING LAW FIRM 2024 LAW ASIA

INDIA BUSINESS LAW JOURNAL FUTURE LEGAL LEADERS 2020 LAW ASIA

INDIA BUSINESS LAW JOURNAL AWARD WINNING LAW FIRM 2024 LAW ASIA

RECOGNIZING EXCELLENCE IN CLIENT SERVICE CLIENT CHOICE

Forbes INDIA | LEGAL POWERLIST 2021

Top Law Firm in Banking & Finance

The LEGAL 500 FIRMS TO WATCH

ASSOCHAM INDIA

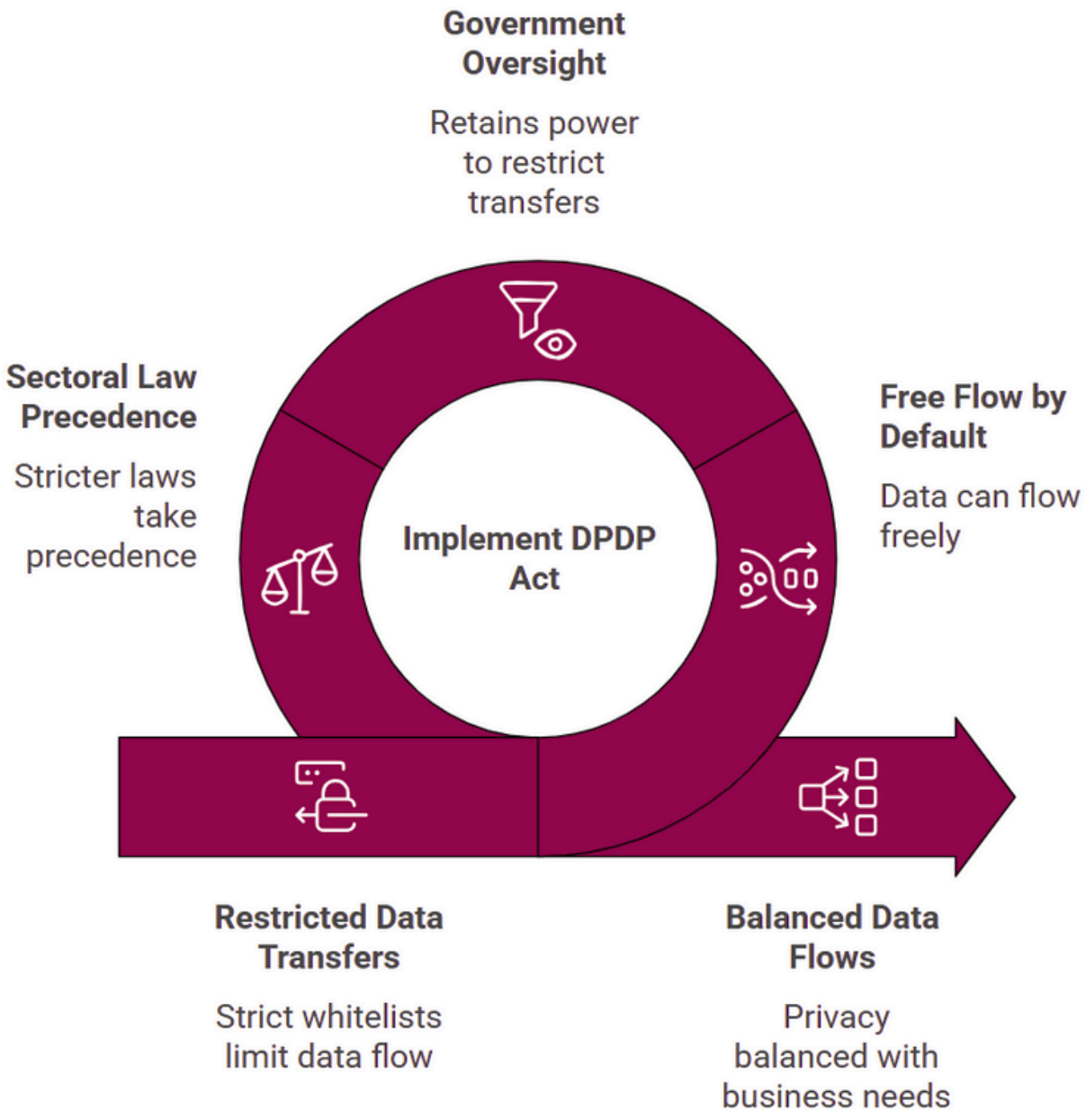
Executive Summary

The Ministry of Electronics and Information Technology (MeitY) has officially notified the Digital Personal Data Protection Rules (“**DPDP Rules**”), 2025, operationalising the Digital Personal Data Protection Act (“**DPDP Act**”), 2023. The document provides a detailed analysis of cross-border data transfer regulations under India's DPDP Act and its associated Rules, 2025, with a focus on sector-specific compliance particularly in the FinTech sector. It highlights India’s default "free flow by default" approach that permits international transfer of personal data unless specifically restricted by future government notifications, marking a significant shift from earlier restrictive regimes. Despite this liberal stance, the document underscores that data fiduciaries remain fully accountable for the protection of personal data transferred abroad, mandating robust contractual safeguards with overseas processors to uphold protections akin to those mandated by the DPDP Act.

Additionally, the guide stresses the precedence of sectoral regulations, which impose stricter requirements notably in financial services regulated by the Reserve Bank of India (“**RBI**”), where data localisation mandates obligate lending and payment data to be stored exclusively on Indian servers with limited and tightly controlled overseas processing allowed. Further, outlines practical compliance strategies for FinTech entities dealing with global cloud infrastructure, analytics vendors, and outsourcing scenarios, emphasizing privacy-by-design principles, contractual enforceability of DPDP standards, and operational measures such as data mirroring and localised backups to future-proof against possible tightening of localisation mandates. It addresses the enhanced regulatory obligations for "Significant Data Fiduciaries" (**“SDF”**), who may face additional restrictions including mandatory localisation or restricted cross-border transfers imposed by government notification.

Table of Contents

Cross-Border Data Transfers: DPDP Act 2025, DPDP Rules 2025 and Sectoral Rules Compliance



Safeguard and Accountability

- **Data Fiduciary's Ongoing Accountability:** The Indian data exporter remains fully responsible for protecting personal data even after it crosses borders.

- **Mandatory Contracts with Foreign Processors:** Any third-party or processor handling personal data outside India on behalf of the fiduciary must be bound by a legally enforceable contract ensuring DPDP compliance.

- **Protection Obligations "Travel" with Data:** Safeguards under the DPDP (encryption, access control, confidentiality) must be maintained abroad; legal obligations remain intact.

- **Model Clauses Similar to EU's Standard Contractual Clauses (SCCs):** Contracts should include provisions for:

(a) Adequate security measures (encryption, access controls)
(b) No onward sharing without consent
(c) Prompt breach notification to the Indian fiduciary
(d) Assistance with data principals' rights requests (deletion, correction)

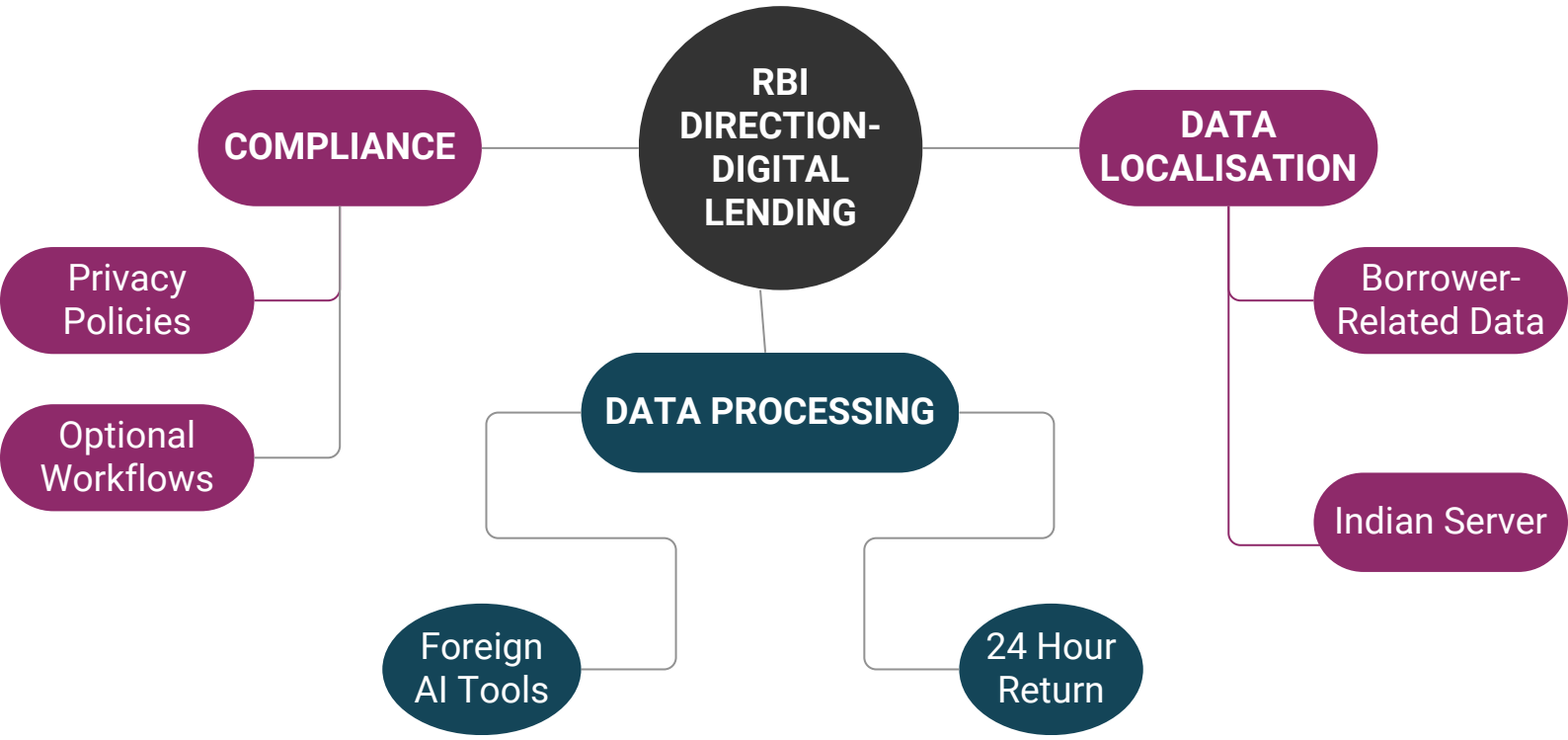
- **Data Return or Deletion Post-Processing:** The foreign processor must delete or return personal data after processing or upon demand, ensuring no unsecured continued retention**.**

- **Due Diligence and Oversight:** Indian companies must conduct due diligence when selecting foreign partners and maintain oversight (audit rights) to verify proper data handling.

- **No Relaxation of Protection Due to Permission to Transfer:** Legal permission to export data does not reduce the fiduciary's protection duties; accountability is exported alongside the data.

RBI Digital Lending Direction: Mandatory Local Storage of Lending Data

- The Direction applies to Regulated Entities including Non-Banking Finance Companies and their Fintech Lending Service Providers.
- Systems must be designed to prioritize India-based data centers for all lending data. Cloud services should use India regions for storage.
- If a lender uses an overseas credit scoring API, all borrower data transferred must be erased offshore within 24 hours, while master data stays in India



RBI Outsourcing Framework for Payment Operators: Localisation and Controlled Access

All payment system data must be stored exclusively on servers physically located in India

Scope: Applies to Non-bank Payment System Operators (PSO), including payment gateways, card networks, prepaid instrument issuers, and similar entities.

Customer identification info, transaction details, payment credentials (card numbers, OTPs, PINs), and logs must reside within India.

Any payment data processed abroad must be deleted from foreign systems and repatriated to India within 24 hours.

PSOs retain full responsibility for outsourced vendors. Outsourcing cannot compromise India's data security or regulatory access.

Critical tasks like customer data management, transaction processes, and compliance must remain within India.

Overseas personnel can only access masked, anonymized, or aggregated data; raw customer payment data must stay in India.

Vendors must isolate PSO data, ensure encryption and limited access on a need-to-know basis, and prevent data commingling.

Operational Impact: Payment operators must design systems with localisation and restricted foreign access from inception to ensure regulatory compliance.

For FinTech payment startups like wallets or payment gateways, RBI's data localisation framework imposes strict architecture mandates

- All production customer data must be stored in data centers physically located in India.
- If using global cloud providers, data must be geofenced to India regions to prevent unauthorized data migration.
- Functions such as fraud monitoring or customer support handled abroad must access Indian-stored data only through secure remote access, not by exporting full databases overseas.
- System design should enforce that payment data never leaves India freely; only encrypted insights, aggregated metrics, or tokenized references are allowed to cross borders.
- RBI has taken enforcement actions (e.g., banning new card issuance for non-compliance), underscoring the criticality of strict adherence.
- RBI requires full supervisory access to payment data within India; foreign authorities or courts cannot get direct access to this data, a protection ensured by keeping data localized and routing access exclusively through Indian jurisdictions.

Implications for FinTechs Using Global Cloud, Analytics, or Outsourcing

GLOBAL CLOUD INFRASTRUCTURE

- FinTechs often use global cloud providers (AWS, Azure, GCP) with worldwide regional data centers. Under DPDP flexibility, hosting is allowed, but regulated/sensitive data should be hosted in India regions to comply with RBI's data localisation mandates
- Architect systems to restrict replication of sensitive personal data to India-only.
- Keep at least one real-time mirror of all personal data on Indian servers to ensure continuity if foreign transfers are restricted
- Use encryption so foreign nodes only hold unreadable data.

ANALYTICS AND SAAS VENDOR USAGE

- Third-party overseas vendors provide services like fraud analytics, credit scoring, or marketing automation.
- Apply privacy-by-design — transmit minimum necessary data, anonymise/pseudonymise where possible.
- Use strong contracts requiring compliance and data deletion post-processing.
- Enforce the RBI's 24-hour repatriation rule for lending data, with automatic deletion clauses.
- Transparently update privacy policies and obtain user consent if needed.

OUTSOURCING SUPPORT OR PROCESSING (BPO)

- Many FinTechs outsource customer support or back-office processing internationally.
- Transfer bulk raw data overseas only when necessary; prefer secure remote access to data hosted in India.
- Ensure role-based, logged access with stringent confidentiality contracts including breach notification provisions.
- For regulated data, verify compliance with RBI localisation rules.
- Use “remote control” approach where overseas staff access data stored exclusively in Indian systems (screen view only).
- If data is shared overseas (e.g., for collections), ensure prompt deletion within the mandated timelines.

This framework enables FinTech firms to leverage global infrastructure and talent while adhering strictly to India’s data protection laws and RBI regulations, managing privacy risk and regulatory compliance proactively.

Significant Data Fiduciary (SDF)

Criteria for SDF Designation: Volume and sensitivity of data, risk to data principals, impact on India's sovereignty, electoral democracy, security, and public order

Enhanced Compliance Duties:	SDFs must appoint a Data Protection Officer (DPO) based in India, conduct independent audits, perform Data Protection Impact Assessments (DPIAs) for high-risk processing, and comply with stricter governance requirements.
Government's Discretion for Additional Obligations	The government can impose further rules, including mandatory data localisation, or enhanced oversight on SDFs via notification to mitigate risks.
Potential Future Localisation Mandates	Although not explicitly required as of now, the government may mandate storage of critical personal or financial data solely in India or require prior approval for cross-border transfers.
Prohibition of Certain Data Transfers (Section 17 DPDP Act)	The law empowers the government to prohibit transfers of specific data categories to protect national interests. This could affect FinTechs handling sensitive datasets.

Operational Recommendations for FinTechs	Build flexible, scalable Indian data infrastructure capable of toggling full localisation on/off without redesign. Maintain parallel global and local systems if needed to adapt quickly to evolving rules.
Policy Monitoring and Risk Management	Stay informed on regulatory updates and consult industry forums to anticipate localisation directives. Many FinTechs adopt conservative localisation strategies preemptively to mitigate compliance risks.

Contractual Controls and Future-Proofing Recommendations

This framework enables FinTech firms to leverage global infrastructure and talent while adhering strictly to India's data protection laws and RBI regulations, managing privacy risk and regulatory compliance proactively.

INCORPORATE STRONG DATA TRANSFER AGREEMENTS	IMPLEMENT MIRRORING AND LOCAL BACKUPS
FinTechs must ensure all personal data shared with foreign entities is governed by a detailed contract or Data Processing Agreement (DPA) aligned with DPDP standards. Such contracts should: • Limit data use to authorised purposes. and to include stringent confidentiality and security obligations. • Restrict sub-processing and onward data transfer without permission • Mandate prompt breach notification within a defined timeframe. • Provide cooperation mechanisms for individual rights requests and governmental inquiries. • Specify data deletion, retrieval, and audit rights.	A best practice is to keep an up-to-date copy of all personal data locally in India, alongside any overseas storage. This can involve architectural designs that write data in parallel to an Indian data center using multi-region cloud replication including an India region. Such mirroring serves as: • Compliance insurance against sudden foreign data storage bans. • Enhanced disaster recovery and operational resilience. Possible segregation of sensitive vs. non-sensitive data to optimise compliance cost.

CONTINUOUS MONITORING OF REGULATIONS

Assign dedicated compliance staff or teams to track new regulatory updates from the central government, MeitY, RBI, and relevant sectoral authorities. Stay subscribed to official notifications and industry bodies (DSCI, NASSCOM, banking forums).

- Early awareness enables proactive compliance adjustments.
- Monitor international developments which may impact cross-border data flows.
- Engage legal expertise regularly to analyze regulatory trends.

EMBRACE DATA LOCALISATION AS A COMPETITIVE ADVANTAGE

Instead of treating data localisation solely as a compliance burden, FinTech companies should leverage it to build user and regulator trust by:

- Transparently communicating India-based data storage and protection policies.
- Incorporating localisation in marketing and customer communications as a security feature.
- Balancing localisation with the controlled use of global innovations (cloud AI, analytics) through compliant mechanisms like anonymisation and contractual safeguards.

CONCLUSION

The Digital Personal Data Protection Act, 2023 represents a crucial regulatory framework that emphasizes the secure and responsible handling of personal data, particularly for the dynamically evolving FinTech sector. By enshrining principles of data ownership, stringent fiduciary accountability, and adaptable cross-border transfer norms, the Act aims to strike a nuanced balance between fostering innovation and enforcing robust privacy protections. FinTech companies must prioritize comprehensive compliance strategies, including adopting data localisation, strong contractual protections, and continuous regulatory vigilance to navigate the complexities of this regulatory landscape effectively and sustainably.

Contact us

Ground Floor, 27-A, Hauz Khas Village,
New Delhi, 110016
Office: +91 11 41727676
info@akandpartners.in
www.akandpartners.in