KHAITAN &CO ADVOCATES SINCE 1911

# Digital Personal Data Protection Act, 2023

## Impact on Payment Aggregators

KHAITAN &CO ADVOCATES SINCE 1911

## Who are Payment Aggregators?

Entities operating payment systems and acting as intermediaries between merchants and customers during the payment process for pooling and settlement of funds

## Data Fiduciary

Collection, analysis, and determination of means and purpose of data processing

Examples: Collecting merchant data for account-based relationship

## Data Processor

Processes data on behalf of Data Fiduciaries

Examples: Processing transaction data to facilitate payments

## What data do Payment Aggregators handle?

Payment Aggregators collect, process and store personal information of merchants and their customers relevant for its functions.

Examples: Name, phone number, address, card details

## What is Personal Data?

Data of an individual who is identifiable by or in relation to such data

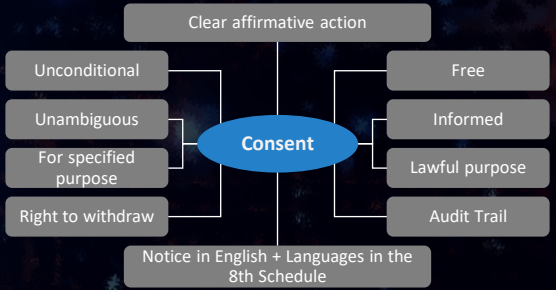
# Consent framework

KHAITAN &CO ADVOCATES SINCE 1911

## Existing Compliance Requirements

- Payment Aggregators must obtain consent from merchants at the time of establishing an account-based relationship before collecting their information
- For providing disbursement services in digital lending:
  - Maintain a clear audit trail of the consent obtained for processing any personal data
  - Consent obtained must be on a "need-based" basis for the specific purpose of facilitation and extension of loans over digital lending platforms
  - Purpose of obtaining consent should be disclosed at each stage of interface with borrowers

## Compliance under the DPDP Act 2023



# Data security

KHAITAN &CO ADVOCATES SINCE 1911

## Existing Compliance Requirements

- Ensure confidentiality of customer's data
- Must check Payment Card Industry-Data Security Standard (PCI-DSS) and Payment Application-Data Security Standard (PA-DSS) certifications
- Report all types of cybersecurity incidents to the RBI and CERT-In

## Compliance under the DPDP Act 2023

- Protection of personal data in possession or control
- Reasonable security standards to prevent breach
- Reporting data breaches to the Data Protection Board and the Data Principal

# Data sharing

KHAITAN &CO ADVOCATES SINCE 1911

## Existing Compliance Requirements

- Payment Aggregators must maintain baseline best practices prescribed by the RBI such as (i) conducting frequent Cyber Security Audit and Reports; (ii) having an IT Governance policy; and (iii) relevant certifications for ensuring confidentiality of customer information
- A Payment Aggregator can only store limited data of customers which is the last four digits of actual card number and card issuer's name through tokenization

## Compliance under the DPDP Act 2023

- Adherence to the notice and consent requirements under the DPDP Act
- For customer data transmitted to any third-party service providers, the Payment Aggregator must ensure its completeness, accuracy and consistency
- No consent requirement for personal data obtained voluntarily for the specified purpose

# Data retention

KHAITAN &CO ADVOCATES SINCE 1911

## Existing Compliance Requirements

- Maintenance of the customer data in relation to transaction history
- Such records to be made available to RBI when requested

## Compliance under the DPDP Act 2023

- Personal data to be deleted once
  - Consent is revoked, or
  - The purpose of processing is fulfilled
- Data can be retained notwithstanding consent revocation, if required under the law

# Data localization

KHAITAN &CO ADVOCATES SINCE 1911

## Existing Compliance Requirements

- Payment Aggregators to ensure all data handled by them is stored in India only

## Compliance under the DPDP Act 2023

- Data can be transferred to any jurisdiction except those specified by the Central Government.
- If other laws offer stronger data protection or limitations on such transfers, those laws take precedence

## Certain additional compliances under the DPDP Act

KHAITAN &CO ADVOCATES SINCE 1911

- Amendment of the existing privacy policy and merchant agreements in line with DPDP Act
- Provide for interface with consent managers
- Amendment of agreements with third-party service providers to ensure compliance with the DPDP Act