KHAITAN &CO ADVOCATES SINCE 1911



Regulatory Framework for Processing of Personal Data in the Digital Lending Ecosystem

Regulatory Framework for Processing of Personal Data for the Digital Lending Ecosystem

DPDP Act 2023

Background

- **Personal data:** Any data about an individual which leads to identification of such individual.
- **Applicability:** Processing of personal data within India, or outside India when such processing is for delivery of goods or services to Data Principals within India, where such data is:
  - Collected in digital form
  - Collected in non-digital form and digitised subsequently.
- **Governs:** Processing in relation to personal data.
  - Processing wholly or partly automated operation or set of operations performed on personal data.

Includes. collection, recording, organisation, structuring, storage, adaptation, retrieval, use, alignment or combination, indexing, sharing, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction.

Data Processor
Entity undertaking personal data processing functions on behalf of the Data Fiduciary

Data Fiduciary
Entity who determines the purpose and means of processing personal data

Data Principal
Individual to whom such personal data relates

Digital Lending Guidelines

Background

- **Digital lending:** Remote and automated lending process largely by use of seamless digital technologies for customer acquisition, credit assessment, loan approval, disbursement, recovery, and associated customer service.
- **Applicability:**
  - Regulated Entity (RE)
  - Lending Service Provider (LSP)
  - Digital Lending App (DLA) of the RE/ LSP
- **Governs:** Collection, usage and storage of any data of the customers in a digital lending transaction.

An RE or LSP could be considered as a Data Fiduciary or a Data Processor on a case-to-case basis, depending on their respective roles in a data transaction flow.

The RE engages the LSP to seek the personal details of potential borrowers for the purpose of extending loan – *Qualifies as a Data Fiduciary as the RE determine the purpose of processing the personal data of the borrowers*

The LSP engaged by the RE only processes such data on behalf of the RE – *Qualifies as the Data Processor as they are processing personal data on behalf of the RE in the instant data flow*

Regulatory Framework for Processing of Personal Data for the Digital Lending Ecosystem

DPDP Act 2023

Obtaining Consent

- **Consent requirement:** Prior consent of the Data Principals concerned, except for certain legitimate uses, including but not limited to:



Data provided voluntarily for specified purpose



For state or its instrumentalities to perform its functions under law



Compliance with any judgement, order etc.

- **Attributes of consent**

specific — informed — unconditional — unambiguous — clear affirmative action

- **Purpose limitation**
- **Notice.** Consent request must be accompanied or preceded by a notice.

Contents of notice

- Details of personal data sought with corresponding purpose
- Manner in which Data Principal may revoke consent
- Grievance redressal mechanism

Digital Lending Guidelines

Obtaining Consent

- **Consent requirement:**



Must have clear audit trail



For specific purpose of facilitation and extension of loans over digital platforms

- **Restrictions.** Accessing mobile phone resources – file and media, contact list, call logs etc.

  Exemption. *One time access to camera, microphone, location etc. for onboarding / KYC requirements, with explicit consent of the borrower.*



- **Purpose limitation**
- **Notice.** Purpose to be disclosed at each interface with the borrower.

Regulatory Framework for Processing of Personal Data for the Digital Lending Ecosystem

DPDP Act 2023

Digital Lending Guidelines

Revocation of Consent

- Data Principal has the right to withdraw consent at any time.
- Data Fiduciary has the duty to delete personal data within a reasonable time of consent withdrawal, unless such deletion is restricted by law.
- The ease of withdrawal of consent must be proportional to the ease with which the consent was given by the data principal.

- Borrower can revoke consent already granted to collect her personal data.
- Borrower can request the DLA to forget / delete her personal data.
- No explicit requirement for the ease of revocation of the consent.

Sharing of Personal Data

- Subject to consent and notice requirements under the DPDP Act.

  Exemptions. Where notice is not required

Enforcing any legal right or claim

Authorized judicial, quasi judicial, regulatory, or supervisory function

Prevention, detection, investigation or prosecution of any offence or contravention of any law

Ascertaining financial information of any person who has defaulted in payment due on account of a loan or advance taken from a financial institution

- Subject to the following conditions:
  - *with explicit prior consent of the borrower, or*
  - *where such sharing is required as per statutory or regulatory requirement*



- DLA must disclose details of third parties allowed to collect personal information through the DLA in its privacy policy.

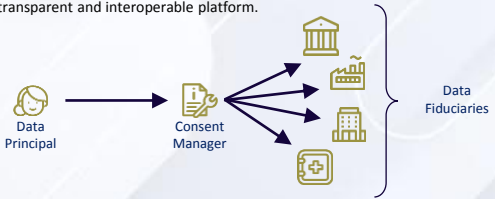
Regulatory Framework for Processing of Personal Data for the Digital Lending Ecosystem

DPDP Act 2023

Digital Lending Guidelines

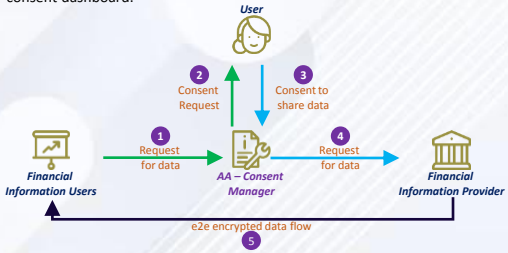
Consent Manager

- Acts as a single point of contact enabling Data Principal to: (i) give, (ii) manage, (iii) review and (iv) withdraw consent - through an accessible, transparent and interoperable platform.



- To be registered with the Data Protection Board of India (“**DPBIA**”)

- No mention of consent manager. All consent receipt is directly from the borrower.
- The Account Aggregator (“**AA**”) framework enables seamless sharing of financial data between regulated financial service entities through its consent dashboard.



Regulatory Framework for Processing of Personal Data for the Digital Lending Ecosystem

DPDP Act 2023

Digital Lending Guidelines

Data Storage and Erasure

- Deletion of personal data (i) when purpose of processing personal data is fulfilled, or (ii) when the Data Principal withdraws her consent.

  Exemption. Personal data can be retained if it is necessary for legal purposes.

- Data is required to be deleted only upon borrower's request.
- Silent on the requirement of deletion once its purpose is served.

  – *REs would be permitted to store KYC related personal data of customers obtained at the time of account opening and the course of the relationship, for at least a period of 5 years after the business relationship ends. This is a statutory requirement under the RBI KYC Master Directions, 2016 and shall therefore apply notwithstanding the consent revocation by the borrower.*

  – *REs / LSPs would qualify as Data Fiduciaries and would be liable to delete the data of the borrower once the specified purpose of processing of such data is served and the regulatory requirement for timelines for preservation / storage of data have lapsed.*

Data Storage and Erasure

- Permitted, except to such jurisdictions as prescribed by the Central Government.
- **Qualification**. Any existing law that provides for a higher degree of restriction will prevail.



- Prohibits cross-border transfer of lending related data. All data to be stored in servers located within India.

  – *Since the Digital Lending Guidelines prohibits cross border transfer of data, REs will be required to adhere to data localisation requirements.*

Regulatory Framework for Processing of Personal Data for the Digital Lending Ecosystem

DPDP Act 2023	Digital Lending Guidelines

Data Breach and Reporting

- Data Fiduciaries to adopt reasonable security safeguards to protect personal data in its possession or control and prevent breach.
- Data Fiduciary must intimate the DPBIA and each affected Data Principal in the event of a data breach.

- REs to formulate standards for handling data security breach.
- DLAs and LSPs of the REs are required to prominently always display such standards on their respective website and the apps.



Grievance Redressal

- Data Principals have the right to approach the grievance redressal mechanism established by the Data Fiduciary and Consent Managers.
- **Timeline for redressal**. Presently not prescribed.
- **Escalation**. After exhausting the mechanism provided by the Data Fiduciary / Consent Manager, Data Principal may approach the DPBIA.
- **Appeal mechanism**. Appeals against the decisions of the DPBIA should be filed within 60 days before to the Telecom Disputes Settlement and Appellate Tribunal.

- REs and LSPs are required to appoint nodal grievance redressal officers to address complaints pertaining to digital lending.
- Ultimate responsibility of grievance redressal remains with the RE.
- **Timeline for redressal**. 30 days.
- **Escalation**. Complaint Management System portal under the RBI's Integrated Ombudsman Scheme.
- No further appeal mechanism prescribed.

Regulatory Framework for Processing of Personal Data for the Digital Lending Ecosystem

DPDP Act 2023

Digital Lending Guidelines

Penalties

- Substantial monetary penalties have been prescribed, which inter alia include:
  - *Fine of up to INR 250 Crores for a breach in observance of obligations by Data Fiduciary to take reasonable security standards and prevent personal data breach.*
  - *Fine of up to INR 200 Crores for breach in giving intimation of a personal data breach to the Data Protection Board or affected Data Principals.*



- The RBI Act, 1934 prescribes penalties for violation of guidelines issued by the RBI, including the Digital Lending Guidelines.
- Includes imprisonment up to 3 years.
- In case of NBFCs, a fine of INR 500,000 or twice the amount involved in the contravention or default where the amount is quantifiable, whichever is more can be imposed.