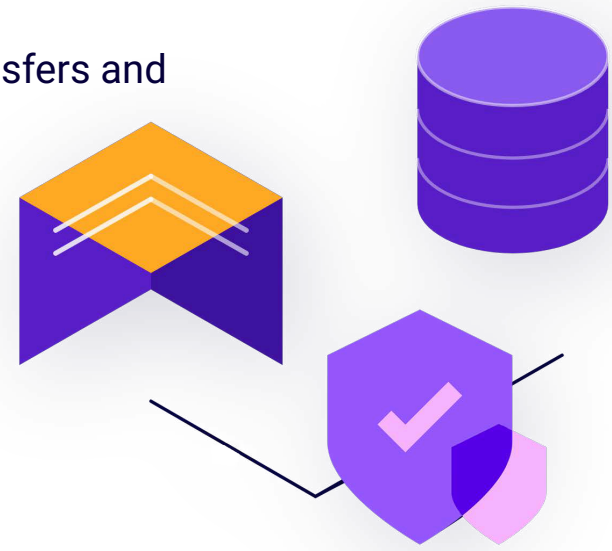
Consentin

A PRACTICAL GUIDE TO

DPDP Compliance for Digital Lenders

- Where consent collection fits in your customer journey
- Handling customer rights, deletion and retention across your systems
- Managing vendor risk, data transfers and breach response



2026 · First edition

www.consent.in

Table of Contents

Introduction 04

01. The Basics 06

02. Consent Collection 13

03. Rights of Data Principals 21

04. Exceptions 25

05. Deletion and Retention 32

06. Managing Third Party Risk 35

07. Data Breach 42

08. Data Visibility and Proof 46

09. Responsible Business Conduct Amendments 49

10. Legal Provisions 51

List of abbreviations

Abbreviation	Definition
AA	Account Aggregator
BPO	Business Process Outsourcing
CRM	Customer Relationship Management
DLA	Digital Lending App
DMA	Direct Marketing Agent
DPB	Data Protection Board
DPDP Act	Digital Personal Data Protection Act, 2023
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
DSA	Direct Selling Agent
FIU	Financial Intelligence Unit
KYC	Know Your Customer
LMS	Loan Management System
LOS	Loan Origination System
LSP	Lending Service Provider
MeitY	Ministry of Electronics and Information Technology
NBFC	Non-Banking Financial Company
OTP	One-Time Password
PAN	Permanent Account Number
PMLA	Prevention of Money Laundering Act
RBC	Responsible Business Conduct
RBI	Reserve Bank of India
RE	Regulated Entity
ROPA	Record of Processing Activities
SDF	Significant Data Fiduciary

INTRODUCTION

The DPDP Act seeks to regulate the core business model of digital lending



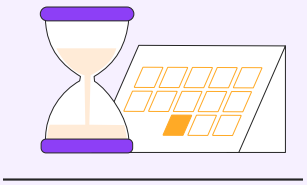
Digital lending runs on a grand data exchange. The customer hands over their data - identity documents, income and transaction proofs, and bank statements to get a loan. In turn, the lender delivers that loan and provides support services. The lender also uses the same data to cross-sell, retarget, and send the customer his next offer.

The DPDP Act and RBI's data privacy and governance rules regulate the lender's ability to collect customer data and reuse it at will. Lenders' ability to collect and harness data is now restricted in three important ways:

- **Consent must be specific and revocable:** The customer agrees to each purpose separately, and can withdraw that consent at any time.
- **Data must be deleted once its purpose ends:** You can't hold it indefinitely or quietly repurpose it for the next offer.
- **Every transfer must be accounted for:** Data moving to a co-lender, LSP, or KYC vendor needs consent and a record.

The digital lending model relying on the free, one-way flow of data is now regulated.

DPDP enforcement	13 May 2027
RBI privacy directions	Already binding
Maximum penalty	up to ₹250 crore



This guide walks you through the customer journey step by step, and shows you what the DPDP Act and RBI rules require you to do:

- **Who's who:** the DPDP roles you and your partners play, and who regulates you
- **Consent:** where to collect it, what it must contain and how to design a notice that doesn't lead to drop-offs
- **Customer rights:** how to allow your customers to access, correct, and withdraw their data and make your systems act on them
- **Deletion vs retention:** what to do when DPDP says erase data but RBI asks you to keep it
- **Data transfers:** how to share data with co-lenders, LSPs (Lending Service Providers) and vendors without a consent gap
- **Breaches:** how to respond and how to retain logs that prove you complied

CHAPTER

01

The Basics



The DPDP Act seeks to regulate “personal data”, but what exactly is personal data?

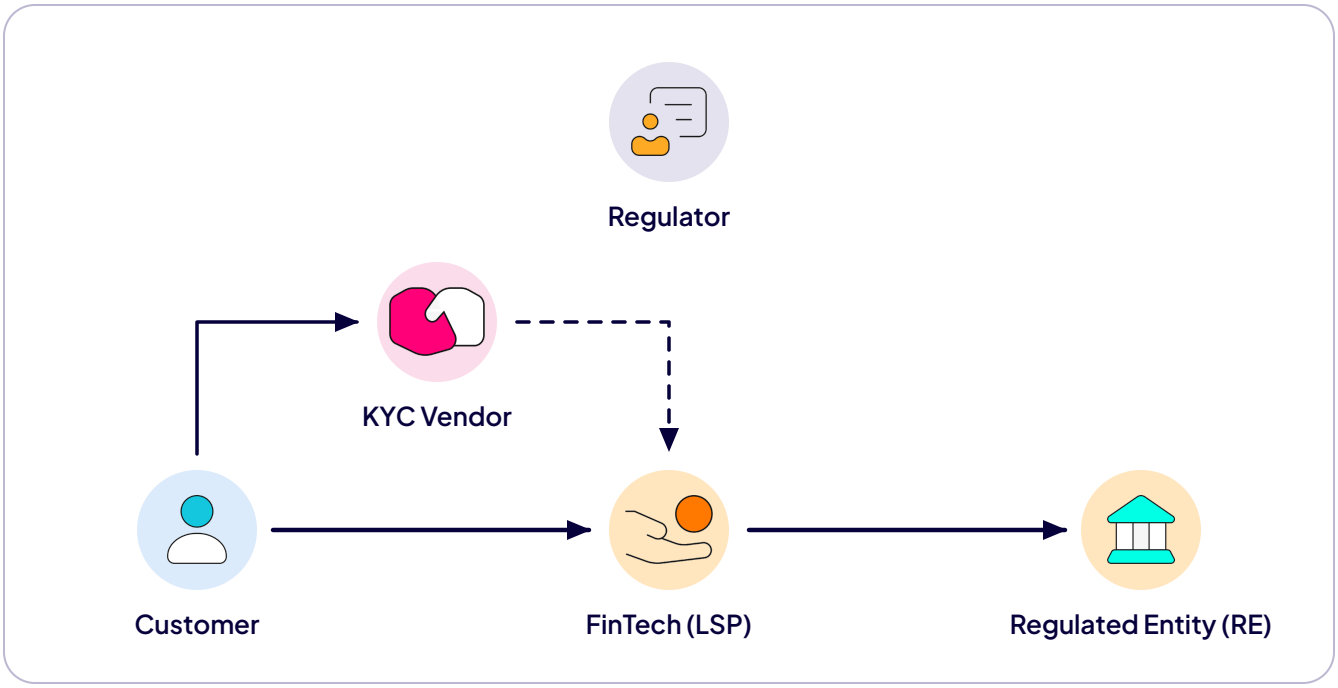
Personal data is any data about an individual who can be identified from that data.

In digital lending, lenders, LSPs, and partners collect a wide range of personal data — location, transaction patterns, app usage, and more. The table below shows the types of personal data typically collected across the digital lending journey.

Data source	Data contains	Usage in digital lending
Location Data	Geo-location tracking	⬢ Verifying customer residency, mobility, and movement patterns
SMS Data	Transaction alerts, expenses, financial interactions	⬢ Evaluating spending habits, repayment reliability, and financial behaviour
Payment Transactions Behaviour	Digital payment habits and consistency	⬢ Assessing reliability of repayments, financial discipline, and creditworthiness
Third-Party App Usage Data	External app usage patterns, lifestyle, spending habits	⬢ Inferring lifestyle choices, consumption patterns, and financial health
Utility Payments	History of utility bill payments (electricity, water, gas)	⬢ Checking consistency in regular payments, indicative of reliability
Other Device Data	Device type, model, usage patterns, device-linked identity	⬢ Identity verification, fraud detection, and behavioural insights

Data source	Data contains	Usage in digital lending
Behavioural Biometrics	Typing speed, swipe patterns, interaction behaviour	Authentication, fraud prevention, and customer behaviour profiling
Social Media Data	Data from social platforms	Assessing borrower credibility, lifestyle stability, and risk profiling
Email Data	Email interactions and communication patterns	Gaining insights into borrower's reliability and financial behaviour
Data on Investments	Investment holdings and behaviours	Gauging financial stability, risk appetite, and repayment capacity

This chapter helps you place your company — and everyone you exchange customer data with — in the right role under the DPDP Act in a typical digital lending flow.



1 Data Principal, Section 2(j)

The Data Principal is the person whose personal data is being processed.

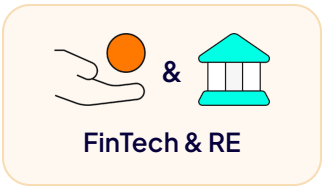
In a lending journey this is usually the customer/borrower[1] (existing or prospective) but it also covers a nominee, a co-borrower, a guarantor, or anyone else whose personal data you collect and process.



2 Data Fiduciary, Section 2(i)

A Data Fiduciary determines the purpose and means of processing - what personal data is collected, and how it is used.

In our example, the FinTech (i.e. LSP as per digital lending) and the Regulated Entity (RE) are both Data Fiduciaries - each decides what customer data is collected and what happens to it.



[1] Note that the term customer/borrower may be used interchangeably in this guide, depending on the context.

3 Data Processor, Section 2(k)

A Data Processor processes personal data on behalf of a Data Fiduciary.



The eKYC platform that does the borrower's KYC is a processor — it acts on the LSP's and the RE's instructions. It is not a Data Fiduciary, because it does not decide the purpose of the processing.

Data Fiduciary or Processor? One simple test.

Just answer this question - **Who decides what is done with the data?**

A Data Fiduciary decides what data it needs and how it will be processed. A Data Processor only acts under the Data Fiduciary's instruction.

The eKYC platform decides nothing about the borrower's data - it is only hired to perform the service. The FinTech (LSP) and the RE decide what happens to the data - without them, no data is collected at all.

4 Data Protection Board, Section 2(c)

The Data Protection Board is the regulator and enforcer of the DPDP Act. It adjudicates disputes on non-compliance and imposes penalties.



In the same way financial sector regulators (eg: RBI and SEBI) govern the financial markets, the Data Protection Board governs anyone who processes personal data. Violate the Act and the Board can investigate and impose penalties of up to ₹250 crore per violation.

5 Consent Manager, Section 2(g)

A Consent Manager is an entity registered with the Data Protection Board that gives a Data Principal a single, interoperable platform to give, manage, review and withdraw consent.



Are there any registered Consent Managers yet?

There are no registered Consent Managers today. The registration window for Consent Managers will become effective on November 13, 2026. See the next page "Who really is a Consent Manager?" for more details.

Are you a Significant Data Fiduciary? (Section 10)

The Central Government can designate a Data Fiduciary that processes large volumes of data, sensitive data, or data carrying a high risk to Data Principals as a Significant Data Fiduciary (SDF). SDFs have some additional obligations:

- Annual Data Protection Impact Assessments (DPIA)
- Annual independent data audit
- Algorithmic risk assessments
- Appointment of a Data Protection Officer (DPO)
- Data localisation restrictions, if the Central Government notifies them

The Government has not yet published the list of SDFs but that notification is expected before the May 2027 enforcement deadline. If you are a large BFSI entity - a lender, insurer, or payment platform processing high volumes of sensitive financial data, you may be designated as an SDF so start preparing for these obligations now.

Who really is a Consent Manager?

The Consent Manager is the most misunderstood entity in the DPDP Act.

Two questions arise constantly: "Are you a registered Consent Manager?" "Do I need one?" Every few days, a new company comes forward claiming that they have applied to become one.

There are the 3 things you need to know about Consent Managers:

- **There are zero registered Consent Managers today.** The registration window only opens on 13 November 2026. You don't need to worry about integrating until one is registered.
- **Your customer chooses the Consent Manager, not you.** Like a UPI app or an Account Aggregator, it is picked by the Data Principal. The system is interoperable: your job is to support it, not to select a provider.
- **A Consent Manager only gives, manages and reviews consent.** As a Data Fiduciary you have to do far more. You have to collect consent correctly, honour withdrawals, retain and delete data on time, manage third-party risk, and prove all of it.

What you actually need: a DPDP compliance platform

A registered Consent Manager does not make you compliant. What you need is a DPDP compliance/operations platform that runs the full lifecycle: consent collection and storage, withdrawal, retention, deletion, and third-party risk, programmatically and across every system that holds customer data. You can choose to build this internally or buy one.

Account Aggregator vs Consent Manager

The Consent Manager is similar to an Account Aggregator (AA), a sector-specific consent system for financial data. Both let an individual give, manage, review and withdraw consent through one interoperable platform.

There are 2 differences:

- An AA is limited to financial information, whereas a Consent Manager can manage every category of personal data.
- An AA is built for consent-based sharing of data between Data Fiduciaries, while a Consent Manager is built for the individual to manage their own consent.

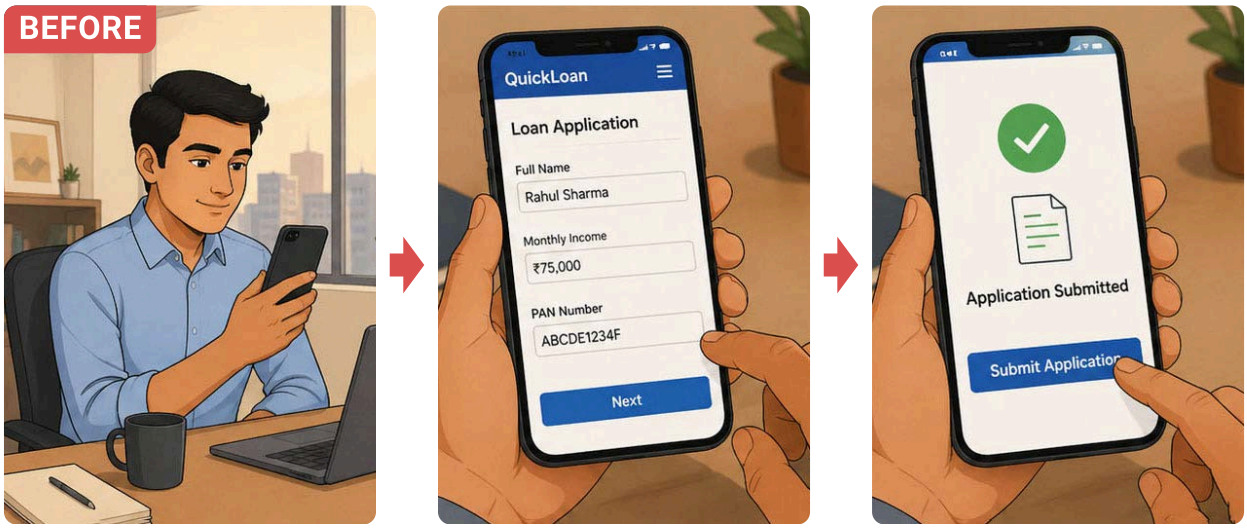
CHAPTER

02

Consent Collection

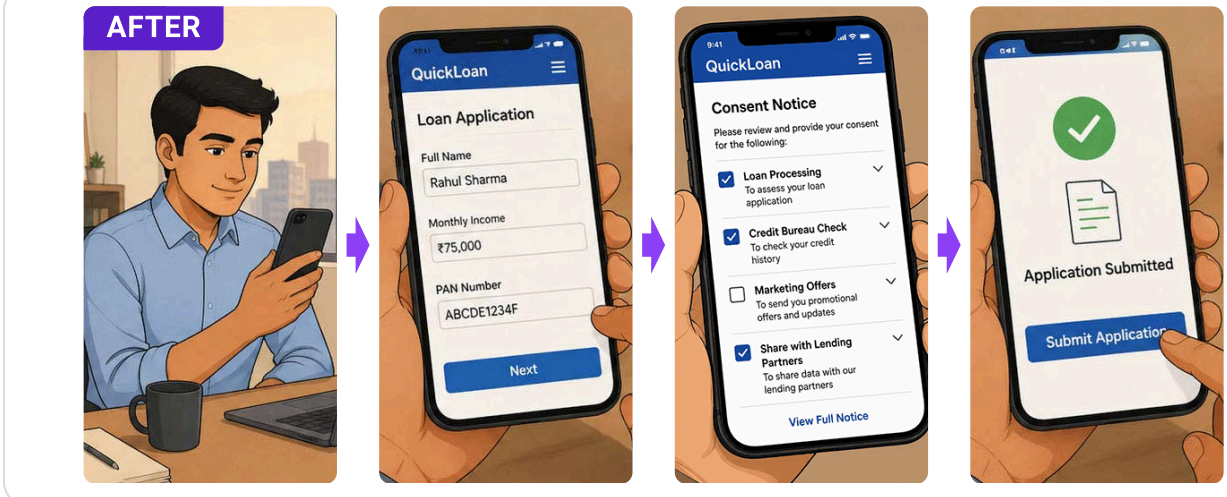


In the last few decades, companies have processed and shared customer data without any restrictions. The customer journey was frictionless and simple.



Both the DPDP Act and RBI's digital-lending rules now require customer consent before you collect and process their personal data.

This adds a new step to every customer-facing journey — **consent collection**.



Without customer consent, REs and FinTechs (LSP) cannot collect and use customer data.

What the law says about consent

Two regimes govern consent for digital lending — the DPDP Act and RBI's digital lending rules.

Under the DPDP Act, you can process personal data only with consent or for a recognised legitimate use.

Under Section 6(1) of the DPDP Act, consent must be:

- **free:** not forced as the price of an unrelated service
- **specific:** tied to a stated purpose
- **informed:** the customer knows what they're agreeing to
- **unconditional**
- **unambiguous, through a clear affirmative action:** a deliberate opt-in, never a pre-ticked box or an assumed yes

Consent must also be limited to the personal data necessary for that purpose. Consent cannot be assumed, bundled, or buried in a long terms-and-conditions clickwrap.

> **RBI's KYC Directions carry the same purpose-bound restriction:** KYC data collected for onboarding cannot be reused for anything else including cross-sell or marketing, without the borrower's express consent for the new purpose.

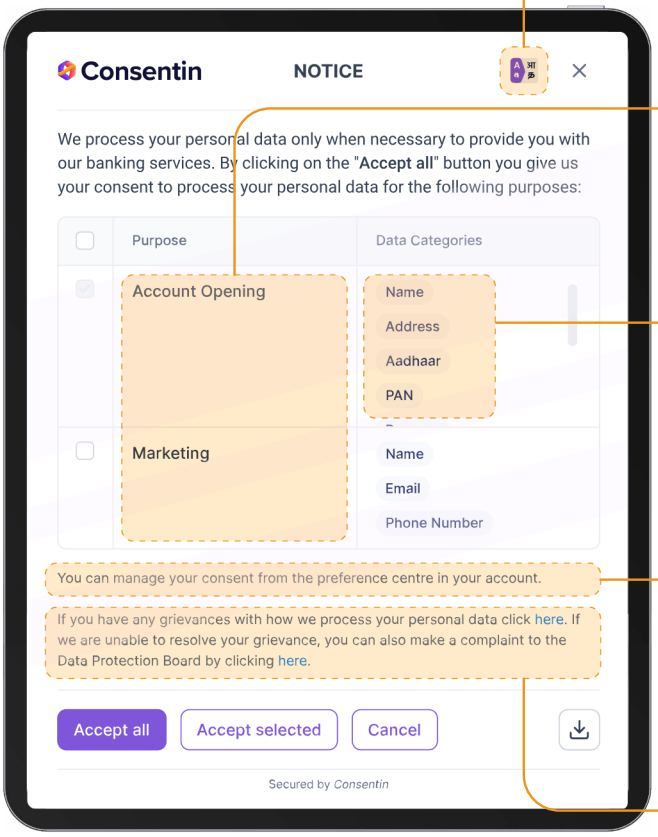
RBI forbids some data collection — even with consent

For digital lending apps, some data collection is barred by the RBI even if you have the customer's explicit consent: (RBI's Credit Facilities Directions, 2025)

- **One-time only, for onboarding/KYC:** a Digital Lending App (DLA) may access the camera, microphone or location once, for onboarding or KYC — not on a standing basis.
- **Off-limits entirely:** a Digital Lending App (DLA) cannot access files and media, the contact list, call logs, and telephony functions, even with customer consent. The only exception is one-time access to camera, microphone, location genuinely needed for KYC with explicit consent of the customer.

What must a DPDP consent collection notice contain?

Below are the 5 essential ingredients for a DPDP compliant consent notice.



Language: the option to access the notice in any of the 22 languages of the Eighth Schedule. (Section 5(3))

Purpose: the precise purpose each piece of personal data is being processed for. Each purpose is its own line item. (Section 5(1)(i))

The personal data collected: every category of personal data you're collecting for that purpose. This must be itemised against each purpose. (Section 5(1)(i))

How to exercise rights: the manner in which the customer can exercise their rights, including withdrawal. (Section 5(1)(ii))

How to complain to the Board: the manner in which the customer can raise a grievance with the Data Protection Board. (Section 5(1)(iii))

Is OTP-based consent valid?

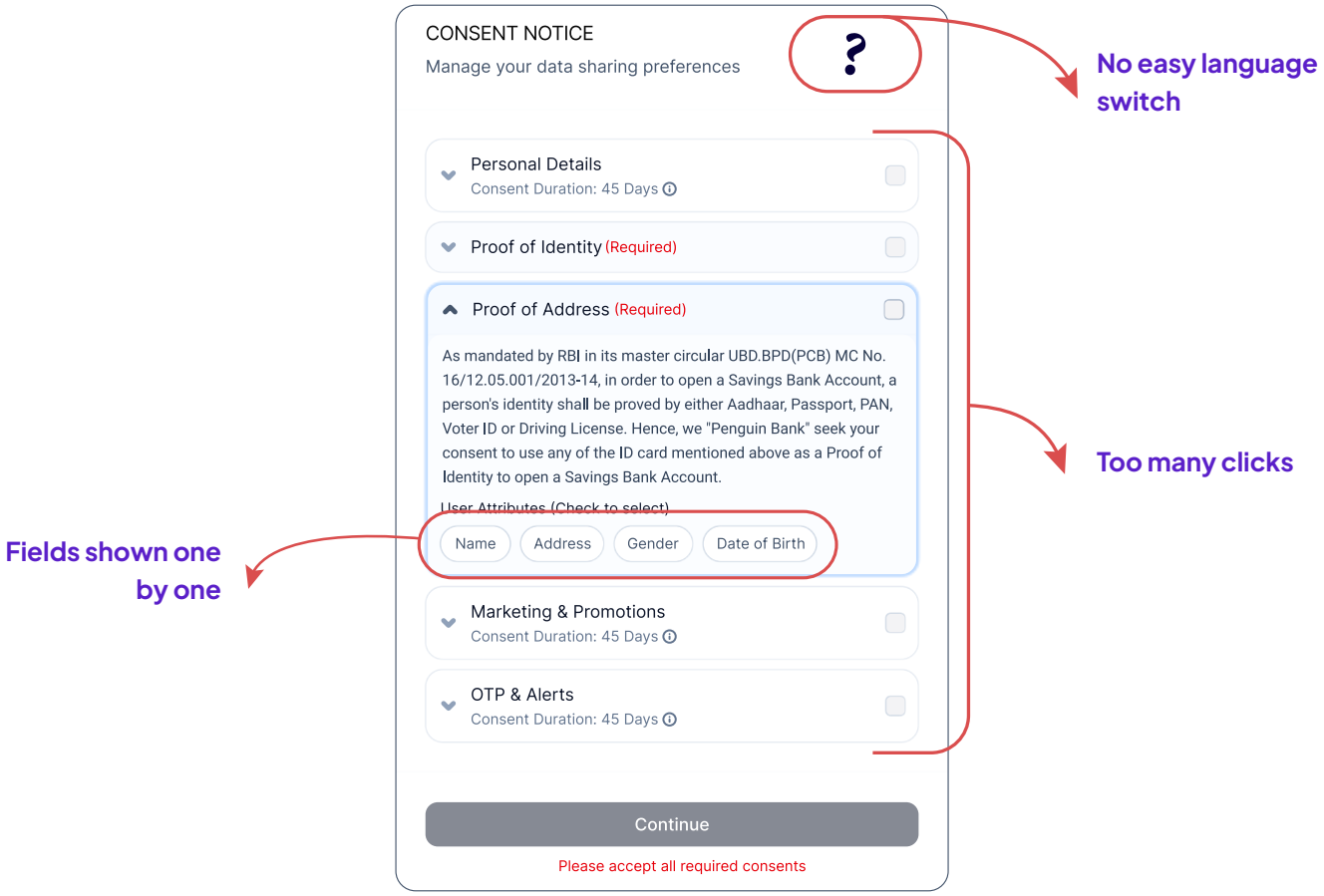
No, OTP based blanket consents will no longer work. Most lending journeys today rely on a single OTP as consent: the customer enters it once and provides consent for everything.

Now you will be required to take consent separately for each purpose, and keep the service consent separate from optional purposes like marketing, so the customer can refuse the optional ones and still get the loan.

How to prevent drop-offs in your consent notice

Consent creates friction in the customer journey, so sometimes your consent notice may cause a lot of drop-offs. Below are examples of two DPDP compliant notices.

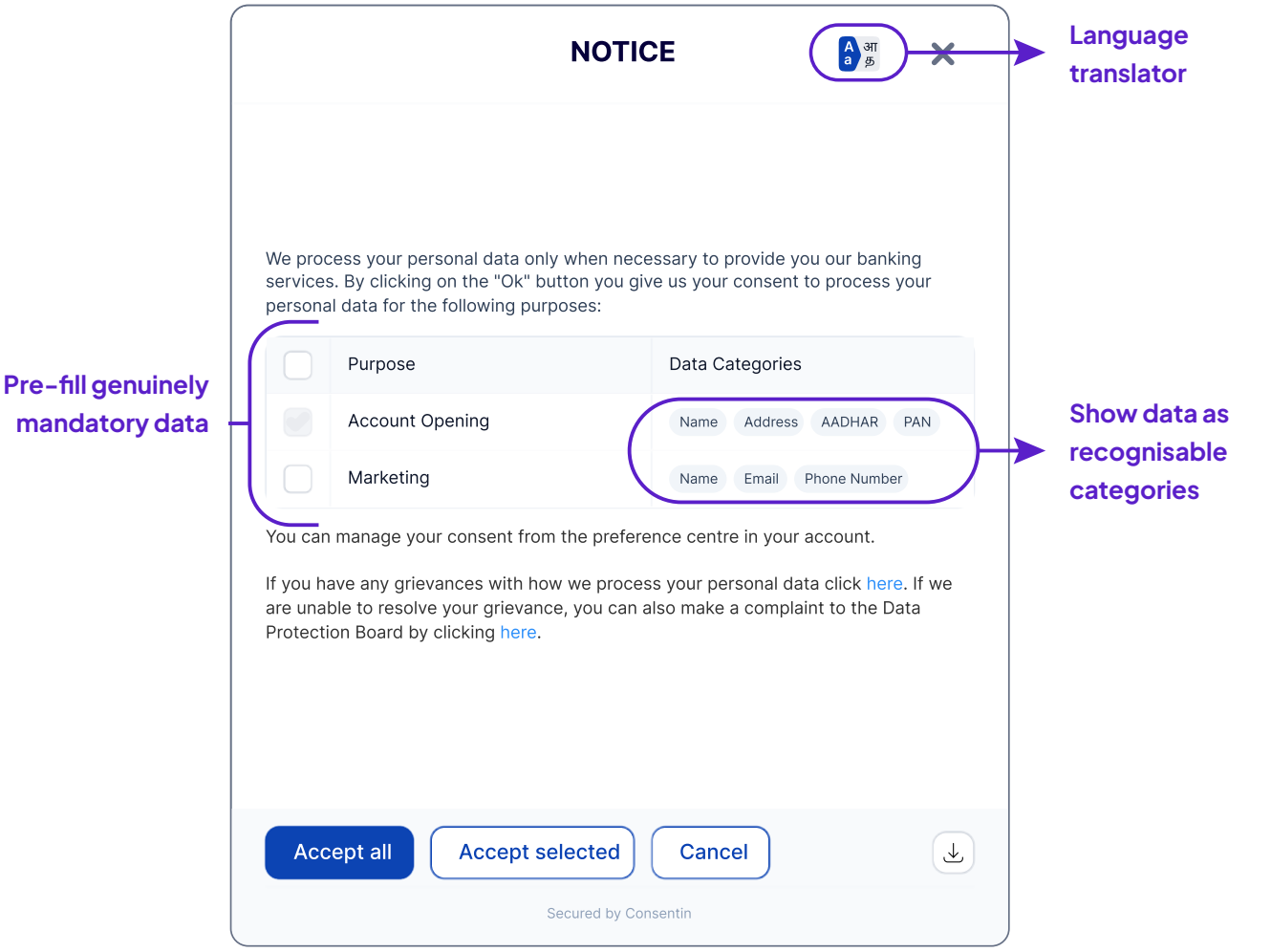
Compliant, but high drop-off. Itemising every field and every purpose forces the customer through many separate steps. You may lose customers for three reasons:



High Drop Offs

- **Too many clicks:** Selecting purposes, data items and then submitting adds up to seven or more clicks, which adds too much friction to the journey, leading to drop offs.
- **Fields shown one by one:** Fields like “name, address, DOB, Aadhaar number” add too much text and are unnecessary. You can label fields as “Aadhaar data” or “KYC documents” to be more concise and understandable.
- **No easy language switch:** English-only interface is both a violation and a way to lose customers who aren't comfortable with English.

Compliant, and low drop-off. The same obligations can be collapsed to one or two clicks with these three steps:



Minimal Drop Offs

- **Pre-fill genuinely mandatory data:** The customer can choose "Accept all" or "Accept selected" tap as the affirmative action. You cannot pre-tick the consent box as Section 6(1) forbids it, but data mandatory for the service can be pre-ticked to reduce the number of clicks.
- **Show data as recognisable categories:** Group fields under labels like "Aadhaar data" or "KYC documents," tied to each purpose.
- **Language translator:** Have the 22-language selector up front and visible.

Consent collection in different scenarios

Do I need to collect consent for KYC?

Yes, you do. Often people say, "KYC is RBI-mandated, so I don't need the customer's consent for it."

This is wrong - under both the DPDP Act and RBI's own rules.

A purpose being mandatory does not remove the consent requirement. The customer is entitled to see what data you hold and why, and that holds even for the purposes you are obliged to perform.

For a mandatory purpose, only the consequence of refusal changes:

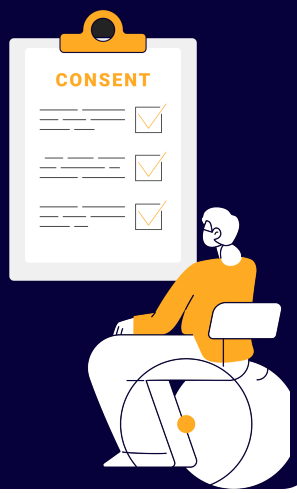
- You **still collect consent** for the KYC data.
- If the customer **refuses**, you **end the journey there**. You cannot proceed with the loan, and you cannot quietly collect the data anyway.



Collecting consent in harder cases

Some customers can't go through a standard tap-to-consent flow. You will need to modify your consent design for this:

- **Children and Persons with Disabilities.** You need verifiable consent from parents or lawful guardians for processing data. For PWDs, you need to verify the customer's identity, the guardian's identity and their status as a lawful guardian. For parental consent, verifying the parent's identity is adequate. DigiLocker-based verification is an accepted mechanism in both cases.
- **Low-literacy customers and persons with visual impairment.** Collect consent through assisted digital flows at a physical touchpoint, or through IVR.



One Time Notice for Existing Data

Once the DPDP Act is in force, you need to notify everyone whose personal data you have collected and are processing even before the Act came into effect. This includes all data collected through implied or bundled consent, Eg: checkbox in a long terms & conditions form or indirectly, via channel partners, field agents, or third-party lead sources.

The law says Data Fiduciaries must, “as soon as reasonably practicable,” send a notice informing the individual of:

- **What personal data you have;**
- **What you’re using it for;**
- **What user rights they now have under the DPDP Act** (like access, correction, and erasure);
- **How they can seek grievance redressal from the Data Protection Board** (DPDP Enforcement Authority) if something goes wrong.

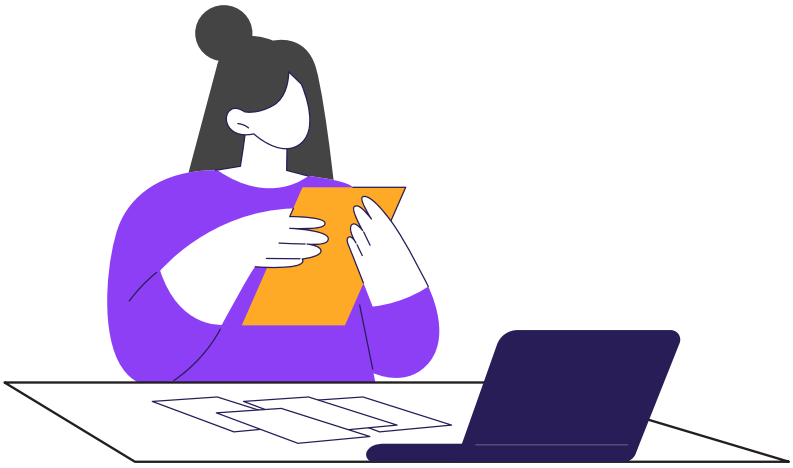
As soon as you satisfy the one time notice obligation, you may continue processing this data unless the user withdraws consent after receiving the notice.

However, if there was never any consent obtained or if there are no records of the same, a one-time notice is not sufficient. You will have to obtain a fresh consent before you continue processing their data.

CHAPTER

03

Rights of Data Principals



What rights do your customers have?

The DPDP Act gives your customers a set of rights over the data they have shared with you. As a Data Fiduciary, you need to build and maintain mechanisms to allow them to exercise these rights.

Six things your customer can ask you to do with their data

Right (section)	What the customer can ask	What you must do
Withdraw consent (Section 6(4); also required of digital lenders by RBI's digital-lending directions)	Take back any consent they gave, at any time, as easily as they gave it.	• Have a withdrawal control always available in the preference centre. • On withdrawal of consent, stop processing (Section 6(6)). • Erase the data where no other ground applies (Section 8(7)).
Access information (Section 11)	A summary of the personal data you process, what you're doing with it, and the identities of every processor and third party you've shared it with.	• Know where the customer's data sits across your systems and vendors. • Produce that summary whenever the customer asks
Correction & completion (Section 12(1))	A right to correct, complete or update inaccurate data. Eg. correct a misspelt name on the loan agreement	• Provide a correction route. • Push the change across every system that holds the field.

Right (section)	What the customer can ask	What you must do
Erasure (Section 12(3); also required of digital lenders by RBI's digital-lending directions)	To delete their personal data.	● Erase it across your own systems and your vendors. ● Keep it only where a law or a still-live purpose requires. Eg. KYC under RBI retention, or if a loan is still being serviced.
Grievance redressal (Section 13)	To raise a grievance when they get no response, or are unhappy with how a request was handled — and escalate to the Data Protection Board.	● Run a grievance channel on your website and app. ● Respond within the period the DPDP Rules allow (no more than 90 days). ● Give the customer a route to complain to the Data Protection Board.
Nominate (Section 14)	Appoint a nominee to exercise their rights if they die or become incapacitated.	● Provide a mechanism to appoint, update or revoke a nominee. ● Verify the nominee's identity and authority before acting.

Can I keep data of applicants I never onboarded?

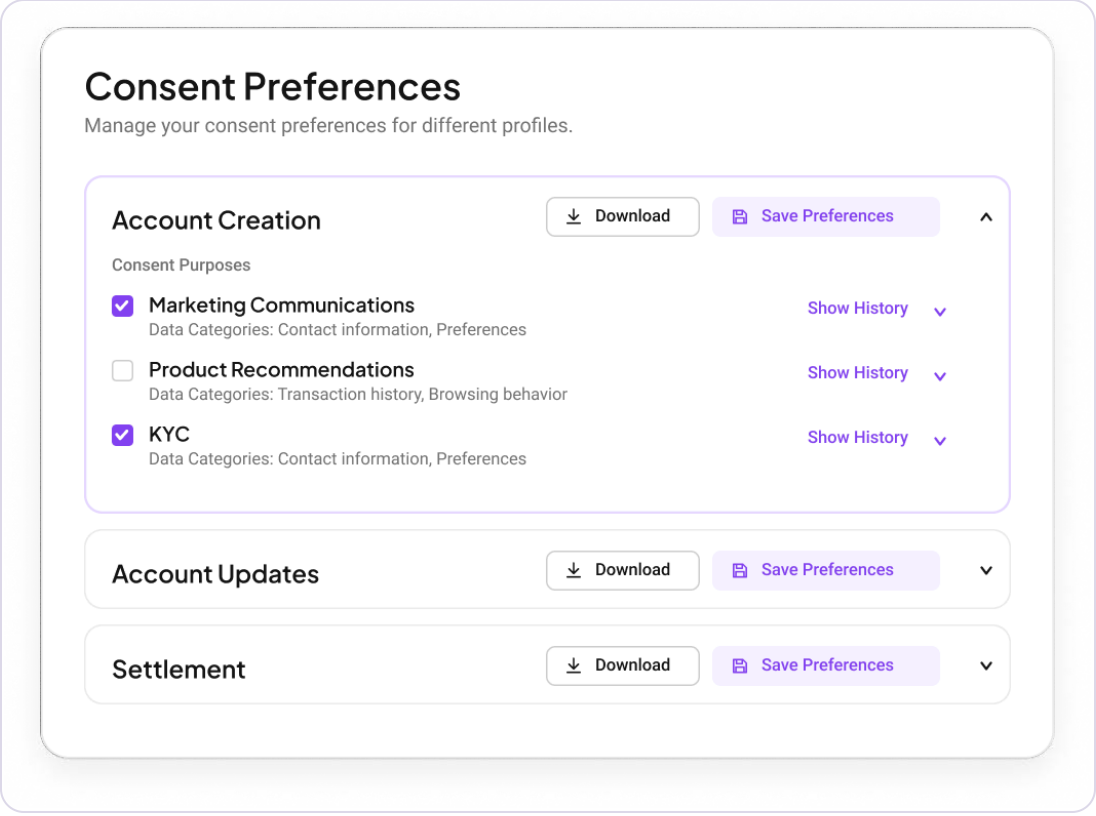
You have to delete it once you make the decision to not onboard since data was shared for that purpose. If the applicant returns, you need to obtain fresh consent. However, you can retain the data if they have separately consented to other purposes like marketing, or if a regulator like RBI requires you to keep it.

Is a preference centre enough?

To allow customers to exercise their rights under the DPDP Act, you need a **Preference Centre**: an easy-to-use interface where customers can view and manage all their consent and requests.

A good preference centre must include 2 things:

- **Authentication**. Before anyone sees or changes a customer's data, you must confirm it's actually them. This can be through an OTP login.
- **An easy interface.** It has to be as easy to use as consent collection flows - you can't bury the ability to withdraw or correct data behind bad UI.

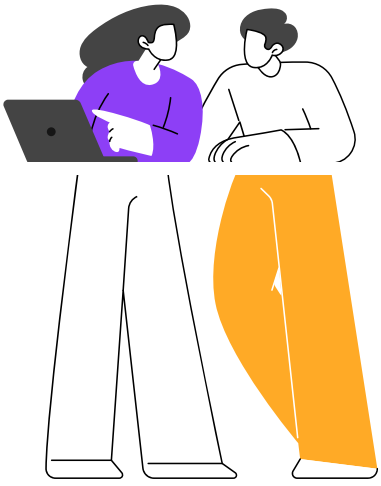


A preference centre is only the customer facing part where requests can be made. To implement these, you need to act on each request and send instructions to downstream systems.

If a customer withdraws consent for marketing, their email address has to be deleted from your marketing platform and email tool, and from the other less obvious places such as a collection agent's spreadsheet or a field agent's phone. But you may need to retain this email address in your LMS (Loan Management System) for loan servicing.

04

Exceptions



When Does the DPDP Act Not Apply?

There are some scenarios where you don't need to collect consent or fully comply with withdrawal/deletion requests. These are the DPDP Act exceptions.

There are 3 types of DPDP Act exceptions:

- Legitimate Uses
- Regulatory Retention
- General Exemptions

The table shows what is exempted and what still applies in each exemption.

Exception	Exempt From	What Still Applies
Legitimate Uses: Where you can process data without obtaining consent. [See Chapter IV (1)]	Consent requirement	• Deletion • Information about data • Grievance Redressal • Data Security obligations • Responsibility for Data Processor actions
Regulatory Retention Where you are permitted or required to retain data even after consent is withdrawn or a deletion request is raised. [See Chapter IV (1)]	• Right to withdraw consent • Right to erasure/deletion	• Consent • Withdrawal • Deletion • Information about data • Grievance Redressal • Data Security obligations • Responsibility for Data Processor actions
General Exemptions Where most of the obligations under the DPDP Act cease to apply. [See Chapter IV (1)]	• Consent • Withdrawal • Retention • Deletion • Information about data • Grievance Redressal	• Data Security obligations • Responsibility for Data Processor actions

Legitimate Uses: Can you ever collect customer data without consent?

Consent is the primary ground of processing personal data under the DPDP Act. But you can process personal data without consent if the processing falls under any of the below **legitimate uses under Section 7**.

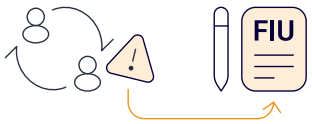
1. **Voluntary Sharing of Personal Data:** If the customer has shared their data with you voluntarily, for a specific purpose, you can process it - for that purpose.

   Eg: A customer emails your support team with their address and personal details for a grievance. You can process that data without consent, only to resolve the complaint and not for any other purpose.



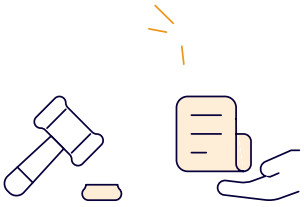
2. **Fulfilling Legal Obligations:** When you are required by the law to disclose the data to the government or any government body.

   Eg: PMLA (Prevention of Money Laundering Act) requires you to report suspicious transactions to the FIU (Financial Intelligence Unit), you can disclose customer data to FIU without consent.



3. **Compliance with Judicial Orders and Other Legal Obligations:** When a court order, decree, or judgment requires you to share the data.

   Eg: A court orders you to produce a customer's transaction records as evidence in a case. You can share this data without the customer's consent.



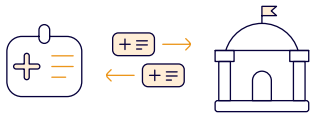
4. **Employment-Related Processing:** When it is required for employment purposes i.e. to protect the employer from loss or liability or to provide services or benefits to employees.

   Eg: A company processes an employee's bank account details to disburse their salary or processes employee attendance and leave records to manage payroll.



5. **Responding to Health and Other Emergencies:** For responding to a medical emergency or to provide medical services during a public health emergency.

   Eg: During a pandemic, healthcare providers might share patient data with government agencies to track and allocate resources effectively.



6. **Disasters and Breakdown of Public Order:** To provide safety or help during a disaster or a breakdown of public order.

7. **Processing by Government Bodies:** The government or any government body can process personal data to (i) issue subsidies, benefits, services, etc. or (ii) carry out its functions under law, or in the interest of national sovereignty, integrity, or security.

Can I collect KYC data without consent?

No. KYC is mandated by law for onboarding, but that does not make it a legitimate use under the DPDP Act.

The legal obligation exemption applies only to disclosures to the government or compliance with court orders — not to internal KYC requirements for onboarding.

Since KYC collection is for your own business purpose, consent must be obtained. If the customer rejects such consent, you can end the journey then and there.

Regulatory Retention: RBI wants me to retain data – but the customer is asking me to delete – what do I do?

The DPDP Act provides specific exceptions for regulatory retention:

- Section 6(6) allows for processing of data for a legal/regulatory purpose even after withdrawal of consent.
- Section 8(7) of the DPDP Act allows retention of data for compliance with any law, even after a customer withdraws consent or the purpose is served.

However this is subject to the following conditions:

1. You can only store/process that data for regulatory retention - you cannot use that data retained for any other purpose like marketing or servicing
2. You must delete the data when the regulatory retention period ends.

Can a customer request deletion of KYC data?

RBI's KYC Master Directions requires REs to retain KYC records for a minimum of five years after account closure. If a customer requests deletion of this data during that period, the RE can continue to retain that data but only for the purpose of KYC compliance.

That data cannot be used for other purposes like marketing.

Exemptions: When does the DPDP Act exempt you from most obligations?

In some cases businesses can be exempt under Section 17 from most DPDP obligations - including requirement to take consent, delete data or provide grievance redressal.

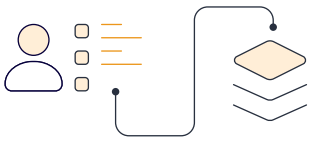
1. **Enforcing Legal Rights:** When necessary to enforce a legal right or claim.

   Eg: A customer defaults on a loan. The lender can process the data to send legal notices and pursue recovery - even if the customer has requested withdrawal of the data.



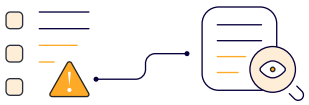
2. **Required by Courts and Regulatory Bodies:** When data is required by courts, tribunals, or regulatory bodies, as per the law.

   Eg: RBI or the DPB directs an NBFC to produce a borrower's records. The lender can retain and share that data for that purpose even after consent is withdrawn.



3. **Prevention and Investigation of Offences:** For prevention, detection, investigation, or prosecution of any offence or violation of law.

   Eg: A company detects some suspicious transactions in the accounts, it can process relevant personal data to investigate under PMLA.



Does KYC data fall under the Prevention and Investigation exemption?

No. Collecting KYC data does not fall under the above 'prevention and investigation' exception. Although KYC data can be used during an investigation, it is not inherently related to an offence.

However, if you are investigating an actual offence involving a specific customer, you can retain and process their KYC data for that investigation. The exception is narrow and only designed to aid investigations into offences and/or prevention of offences and can only be processed for that purpose.

4. **Business Process Outsourcing (BPO):** When an Indian entity processes personal data of individuals outside India under a contract with a foreign entity

   Eg: An Indian IT firm provides customer support to a U.S. e-commerce company's foreign customers. Consent from those customers isn't required.



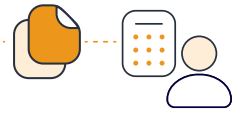
5. **Corporate Restructuring and Mergers:** When necessary for a court-approved merger, demerger, amalgamation, or transfer of undertaking.

   Eg: Two companies merge under a court-approved order. Customer data can be transferred to the merged entity without fresh consent.



6. **Loan Default Investigations:** To ascertain financial information, assets, and liabilities of a person who has defaulted on a loan, subject to applicable disclosure laws.

   Eg: A lender needs to assess the assets and liabilities of a borrower who has defaulted. They can process financial data to determine recovery options.



7. **National Security and Sovereignty:** Processing by a government body notified by the Central Government in the interest of national sovereignty, security, or public order.

   Eg: A notified intelligence agency processes communication data of individuals suspected of posing a security threat.



8. **Research, Archiving, and Statistics:** For research, archiving, or statistical purposes, provided no individual decisions are made on the basis of this data, and subject to standards set out in the DPDP Rules.

   Eg: A credit bureau uses anonymised borrower data to publish industry-wide default rate statistics, without making any individual-level decisions based on the data.



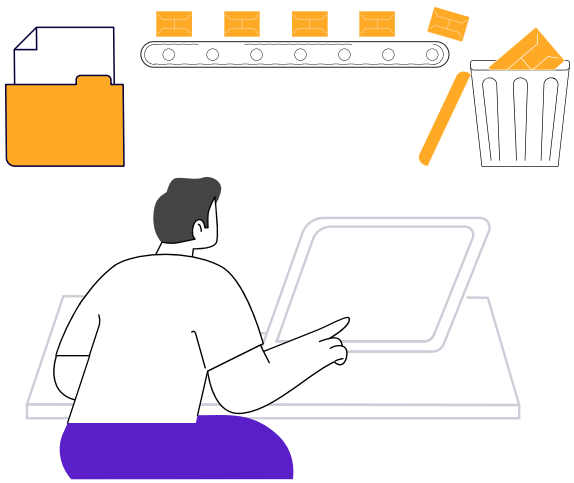
Can I use the research and archiving exception to do customer analytics and targeting for marketing?

No. This exemption bars individual decision-making on the data, so using it to profile customers or target products or marketing isn't permitted.

CHAPTER

05

Deletion and Retention



When must personal data be deleted?

Personal data must be deleted from all of your own and third party systems when any of the following happens:

- Consent is withdrawn
- A deletion or erasure request is raised by the Data Principal
- The purpose for which the data was collected has been served
- A legally mandated retention period ends

How to implement this?

Your customers' data may be lying in various systems - in your CRM, your marketing automation tool, your email platform, your loan management system, and spreadsheets on your team's devices.

When a deletion request comes in, you need to:

- **Identify** every system where the data exists
- **Send the correct instruction** to each system delete, retain, or restrict
- **Ensure** the action is actually taken and recorded

Your ROPA (Record of Processing Activities) map can help you with this since it tells you where data lives, so you know where deletion needs to happen.

How to ensure that my vendors have deleted data?

Since you may not always have visibility over your vendors systems, you can safeguard yourself by ensuring that your contracts with vendors must clearly include:

Explicit deletion protocols	When deletion must happen and what triggers it
Accountability safeguards	Who is responsible and what happens in case of a breach
Acknowledgement of deletion	Written or system-generated proof that deletion has been completed

When must personal data be retained?

There are situations where you are required, or permitted, to retain data even after a deletion request or consent withdrawal:

- If the purpose has not yet been served
- If a specific law or regulation requires it (See Regulatory Retention in Chapter 4)
- If it is required as per any of the exceptions (See Exemptions in Chapter 4)

How to implement this?

When a deletion request comes in, you will need to do the following:

- **Identify** what data is being requested for deletion
- **Check against your ROPA** to determine whether any retention obligation applies to that data (the three stated above)
- If retention is required, **ensure it is stored separately** and used only for the specific purpose it is being retained for
- **Communicate to the Data Principal** why their data is being retained and for how long
- Once the retention period ends, **trigger deletion** across all systems

Is deletion the only option?

No. Whether to delete, archive or anonymise depends on the purpose, type of data and retention requirements.

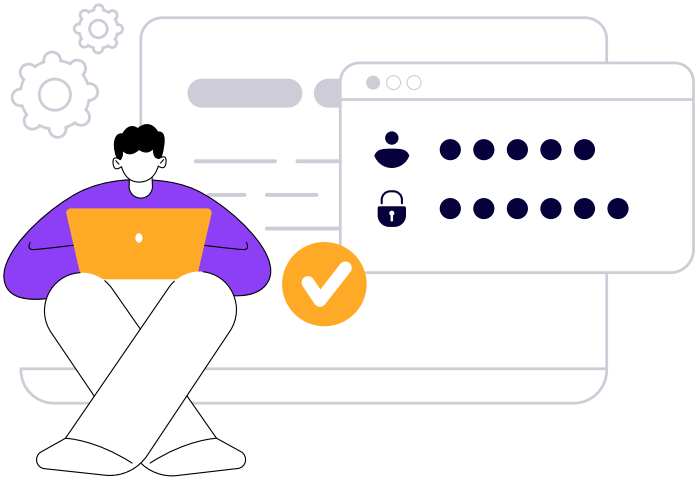
For lenders and NBFCs, hard deletion is often not feasible because loan records are tied to core systems and RBI retention rules. Depending on the scenario, you can either:

- **Archive:** Move data you must retain to separate, access-restricted storage and use it only for the purpose it is being retained for.
- **Anonymise:** Irreversibly remove identifiers so the data no longer points to an individual.
- **Delete:** Actually erase all data from all your systems.

CHAPTER

06

Managing Third Party Risk



Sharing data with third parties

In a digital lending journey, no single entity processes all the data. It flows from a referral partner to KYC and other vendors to the FinTech (LSP) to the RE and on to co-lending REs, credit bureaus and recovery agencies etc.

DPDP Act: Under the DPDP Act, the FinTech (LSP) and the RE are usually both **Data Fiduciaries** (Section 2(i)). Each independently determines a purpose for the customer's data, so each is independently accountable for everything in the Act.

But if you share data with a third party who is your Data Processor, under Sections 8(1) and 8(7)(b) you remain responsible for what your processors do - including their failure to erase, and a vendor's lapse becomes your penalty.

RBI: Under RBI's Credit Facilities Directions, the **RE is the primary accountable entity**. RBI delegates to the RE the job of ensuring the LSP behaves. Specifically, the RE must ensure that:

- consent is collected properly;
- the LSP holds only the minimal data it needs;
- there is a data storage and retention policy;
- data localisation is met.

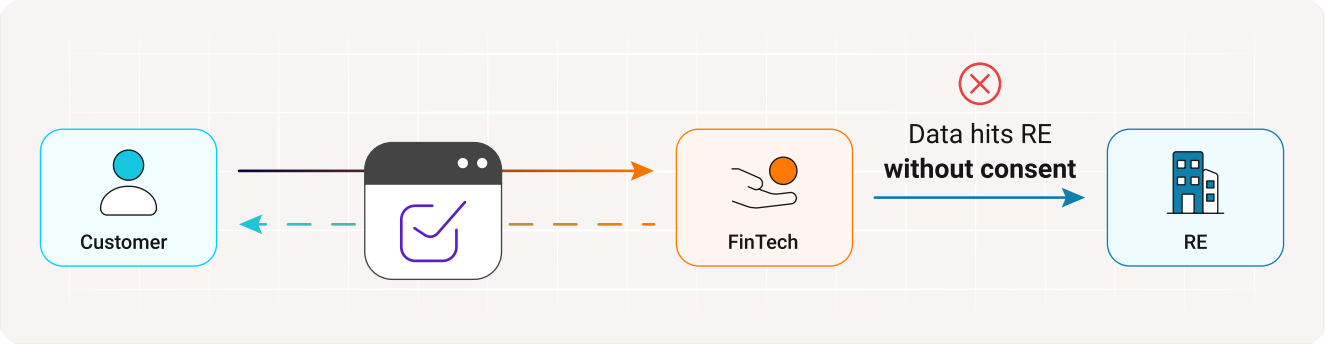
Consent to Transfer:

Clause 13(4) of the RBI Credit Facilities Directions requires explicit consent before you transfer a borrower's data to any third party. REs and FinTechs (LSP) need to factor this into their solutioning.

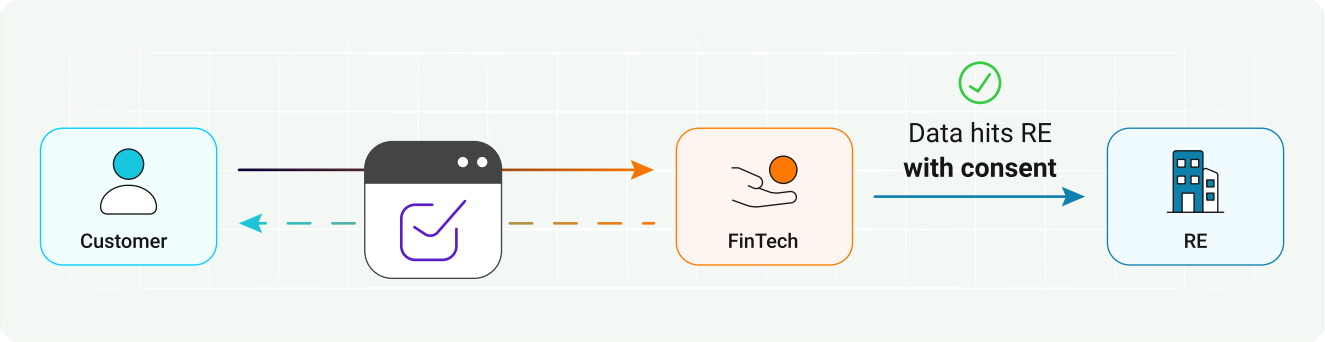
In a non-compliant journey:

1. A borrower gives a FinTech (LSP) consent to process their data for a loan.
2. To actually make the loan, the FinTech (LSP) has to send that data to the RE.
3. But the borrower never consented to that transfer.

So the moment the data hits the RE's systems, the RE is processing it without a valid basis — non-compliant before it has even spoken to the borrower.



With a consent to transfer, the first fiduciary in the chain captures consent for the transfer up front, so the data arrives at the second fiduciary already covered.



In practice, a proper consent to transfer includes three stacked purposes:

1. **Normal consent:** the consent you would collect anyway, for your own processing of the borrower's data.
2. **Consent to transfer:** the explicit consent to allow the transfer of data to a named third party or class of third parties required under Clause 13(4) of RBI's Credit Facilities Directions
3. **Consent for the receiving fiduciary's purposes:** consent for what the RE will do with the data. This is not mandatory, but doing this avoids the customer having to undergo separate consent collection later, and reduces friction.

Frame consent around the purpose, not the vendor

Frame the second and third consents around the **purpose** rather than a named vendor where you can. If consent covers "transfer to your lending partner for credit assessment," you do not need fresh consent when that partner changes, as long as the purpose holds. If you tie it to one named entity, you will need to reobtain consent every time you change a vendor.

Is consent to transfer legal under the DPDP Act?

Yes. The Act does not stop fiduciaries from collecting consent on each other's behalf - it only requires valid consent for the transfer. Two provisions confirm it:

- **Section 4(a)** permits processing of personal data "for which the Data Principal has given her consent," without dictating who in the chain collects it.
- **Section 2(i)** defines a Data Fiduciary as one who determines the purpose and means of processing "alone or in conjunction with other persons."

Controlling consent from DSAs and channel partners

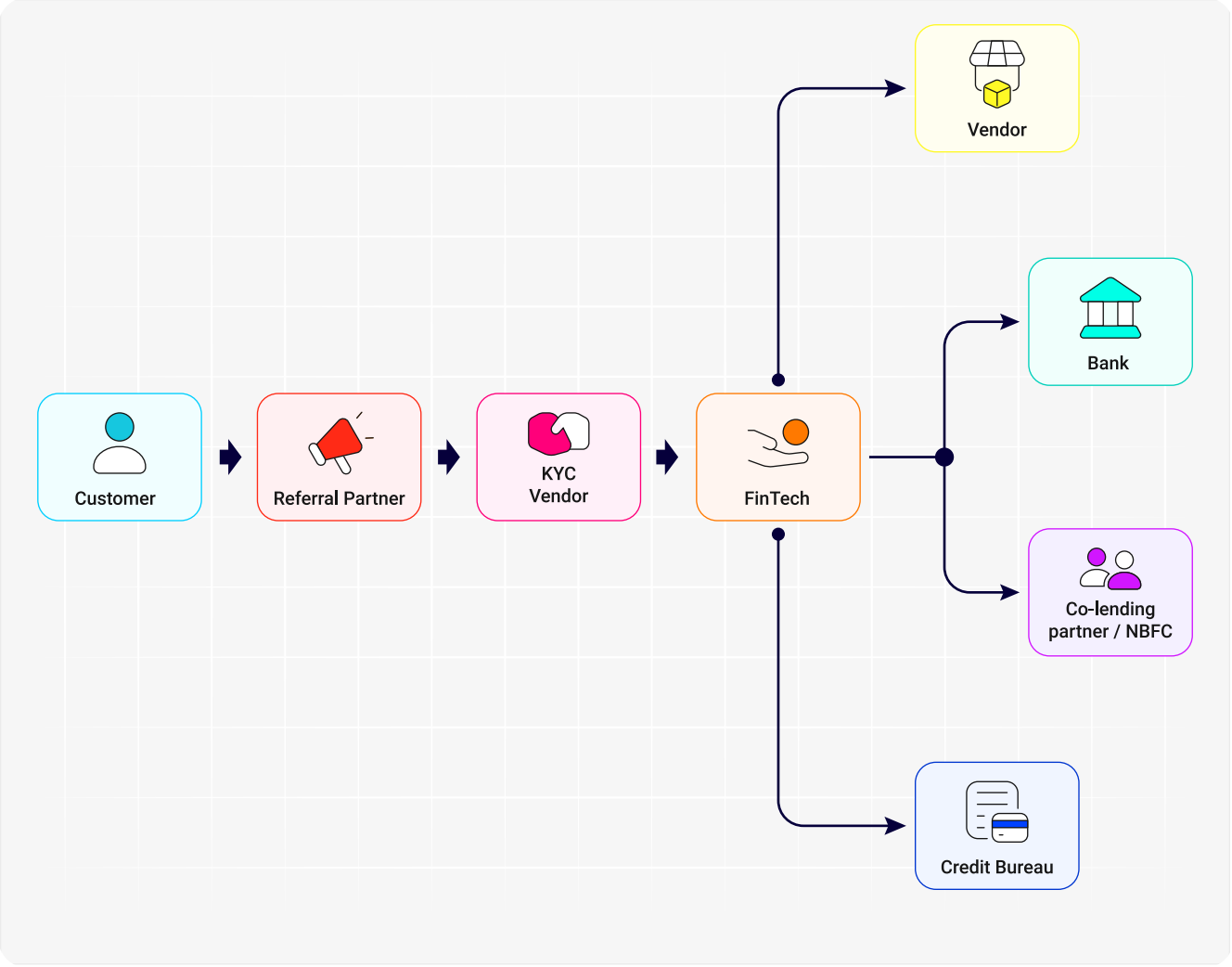
You remain answerable for how consent is collected, even when a partner collects consent. To ensure consents are actually collected, you can:

- Put a consent flag on every record at entry and don't allow records without a valid flag to move forward.
- Try to collect consents on your flow through a QR code, WhatsApp flow or IVR.
- If a partner collects consent in its own system, get the consent logs.

Understanding your Third Party Data Flows

Whether you are liable for a third party's actions depends on its role - a Data Processor (Section 2(k)) acts under your instruction, while an independent Data Fiduciary (Section 2(i)) decides its own purposes. Here is how the typical players in a lending flow fall:

Here is a typical digital lending data flow:



The table below breaks down the roles of each entity in a typical digital lending flow.

Entity	Role	Explanation
LSP / Fintech	Data Fiduciary	Determines how it processes and uses the borrower data it collects.
KYC Vendor	Data Processor	Verifies KYC solely on the RE's behalf, under its instructions.
Channel / Referral Partner	Data Processor/ or Data Fiduciary	Sourcing leads solely for you → Processor. Independently marketing or processing the data for its own or others' purposes → Fiduciary.
Regulated Entity (Bank)	Data Fiduciary	Independently determines how it processes the borrower data the fintech shares.
Co-lending partner (NBFC)	Data Fiduciary	Both lenders process the data for their own lending purpose; each determines its own use, so both are Fiduciaries.
Vendors	Data Processor	Process data solely under your instructions.
Group Companies	Data Processor/ or Data Fiduciary	Processing independently for their own purposes → Fiduciary. Under your instructions → Processor. Group entities are treated as separate third parties either way.
Credit Bureau	Data Fiduciary	Maintains its own database and processes for its own purposes; independently responsible for its own compliance.

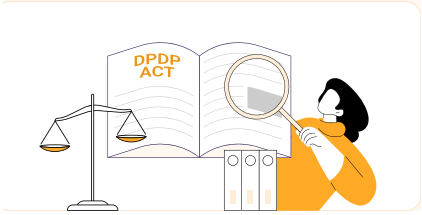
When the role is genuinely in doubt, assume you are a Data Fiduciary. For 90% of borderline cases, the safe and correct call is to treat yourself as a Data Fiduciary and prepare accordingly.

Minimising Third Party Risk

As a Data Fiduciary, you are responsible for all actions of third parties who are your Data Processors, including software vendors, LSPs, TechFins/FinTechs etc.

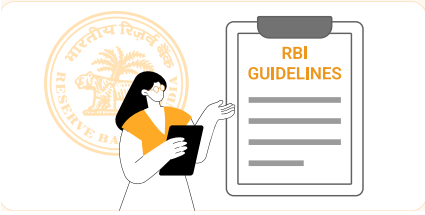
What does the law say about minimizing third party risk?

DPDP Act



- Make sure your vendors stop processing and erase data when consent is withdrawn or the purpose ends.
- Have a valid contract with each vendor.
- Ensure your vendors take reasonable security safeguards to prevent a personal data breach.

RBI Guidelines



- Make sure vendors notify you immediately of any security breach or leakage of customer data.
- Make sure you have audit rights over their operations.
- Ensure vendors do not combine or commingle your customer data with data of other clients.
- Ensure vendors maintain adequate security measures.
- Ensure vendors comply with data localisation requirements.
- Ensure vendors have business continuity and disaster recovery plans.

Contracts alone won't protect you because the penalties for violations can be far higher than the indemnity amount in your contract. To protect yourself:

- Conduct vendor due diligence before onboarding, and ask about subcontractors.
- Try to minimize and tokenise the data you share.
- Have vendors work inside your interface.

CHAPTER

07

Data Breach



What counts as a breach

Under Section 2(u), a personal data breach is defined broadly: any unauthorised processing, or accidental disclosure, loss, or alteration of personal data that compromises its confidentiality, integrity, or availability.

This is a wide definition — it covers far more than the cyberattacks that make the news. These would also constitute a breach:

- Emailing one customer's sanction letter or KYC documents to a different customer
- A field agent losing a phone with borrower records on it
- A misconfigured storage bucket exposing part of your loan book

This means that digital lenders will need to enforce strong security protocols to prevent breach.

Preventing a breach

Section 8(5) of the DPDP Act requires digital lenders to ensure reasonable security safeguards as defined in Rule 6 of the DPDP Rules.

What Rule 6 requires	What it looks like for a lender
Access controls	• Role-based access to the LOS (Loan Origination System)/LMS • Collections agents limited to their assigned accounts • KYC files restricted, not open across the org
Encryption, obfuscation or masking	• Mask Aadhaar, PAN and bank details on agent screens and in the CRM • Encrypt stored KYC documents
Logging and monitoring	• Log every pull of a borrower's bureau report or KYC file • Alert on bulk exports of the loan book
Backups and retention	• Keep the loan book and repayment records recoverable • Covers data RBI requires you to retain
Contracts with processors	• Bind KYC vendors, collections agencies, LSPs and cloud providers to the same standard

Responding to a breach

You become aware of the breach — clock starts.

24 Hours

48 Hours

72 Hours

Notify Affected Customers

Due: Without delay

Send a plain-language notice that includes:

- What happened (nature, extent, timing)
- The likely consequences for them
- The measures you're taking to limit the damage
- The steps they can take to protect themselves
- A contact for their queries

Notify Data Protection Board (Initial Intimation)

Due: Without delay

Send an initial intimation that includes:

- A description of the breach
- The likely impact of the breach

Notify Data Protection Board (Detailed Report)

Due: Within 72 hours

Send a detailed report within 72 hours that includes:

- A detailed report and root cause analysis
- Who or what caused it
- The remedial measures taken
- A record of the notifications sent to borrowers

What to do after a breach has happened?

When a breach happens, digital lenders must issue notifications to the Data Principals and Data Protection Board under Section 8(6) of the DPDP Act. The clock starts when you become **aware** of the breach — when investigation confirms it, not when you first suspect it.

Contain and recover

Alongside the notifications, take active measures to eliminate the breach:

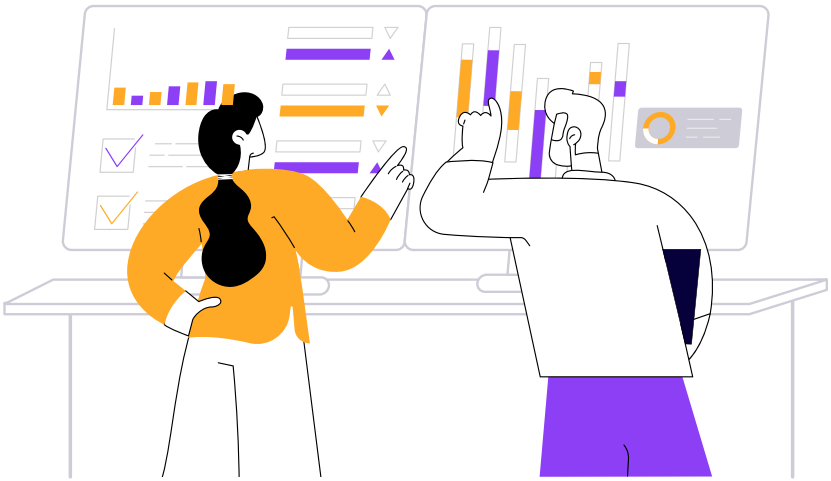
1. **Contain and secure:** Detect the source and scope. Disable compromised accounts, isolate affected systems, and stop further loss.
2. **Assess impact and fix the root cause:** Establish what data was affected and its impact on borrowers. Identify the root cause and remediate it, so the same gap can't reopen.
3. **Document everything:** Preserve logs, access records, forensic evidence, the notifications you sent, and the breach reports — this is the evidence you'll rely on in an audit or a Board inquiry.
4. **Review, learn, and strengthen:** Once the incident closes, review how it happened and how you handled it. Update the response plan, the processes, and the controls, and train teams on what you learned.

Penalties for Breach and Failure to Prevent Breach:

- **Up to ₹250 crore** for failing to maintain reasonable security safeguards (Section 8(5)).
- **Up to ₹200 crore** for failing to notify affected borrowers or the Board (Section 8(6)).

08

Data Visibility and Proof



You are collecting consent, enabling user rights and deleting or retaining data as required. But if a dispute arises tomorrow, how do you prove that you complied?

The DPDP Act places the **burden of proof** on the Data Fiduciary so the Data Fiduciary has to prove that:

- A valid notice was given
- Consent was properly obtained
- Requests were handled correctly
- Deletion or retention decisions were lawfully executed

> Your ROPA serves as a critical piece of this puzzle. In case of an audit or investigation, a well-maintained ROPA is your first line of defence — it documents every data flow, every purpose, and every processing activity across your organisation.

To do this, you need logs as they are your primary evidence. Logs create an auditable trail of exactly what happened, when, and who was involved - so that you can show compliance before a court or before the Data Protection Board.

How to maintain logs?

The DPDP Act does not prescribe a specific format of logging yet. But to safeguard yourself, you should ideally log the following:

- Date and time
- How the Notice was shared
- Any query/request received from the Data Principal
- Responses to the Data Principals
- Deletion
- Traffic Data

Even with these reasonable safeguards, breaches can happen.

What is a Consent Artefact?

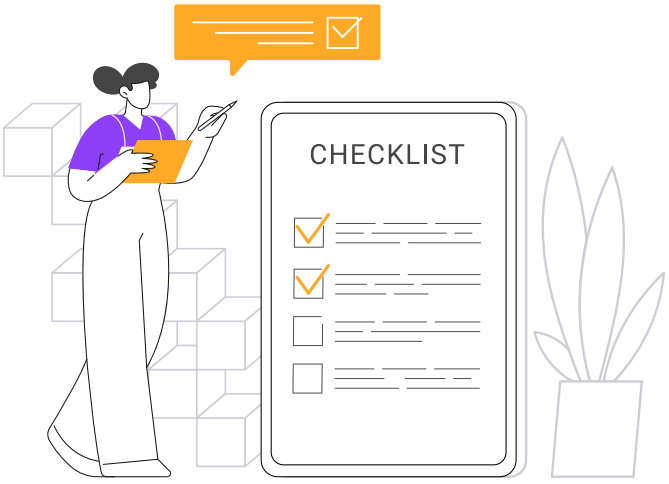
The Consent Artefact is a verifiable, tamper-proof proof of consent. MeitY (Ministry of Electronics and Information Technology) Electronic Consent Framework - a non-binding guide/advisory - recommends a consent artefact for recording of consent. A Consent Artefact is a machine-readable electronic document that captures what a user has consented to in any data sharing transaction and must contain the following:

- **Details of all entities involved**
- **Details of data:** The type of data being accessed, access permissions, date range, storage duration, and frequency of access
- **Purpose of data access**
- **Logs of data flows**
- **Digital Signature:** every Consent Artefact must be digitally signed to be valid

CHAPTER

09

Responsible Business Conduct Amendments



RBI's RBC Amendments further enshrine consent

RBI recently issued an amendment to its Responsible Business Conduct Directions which enshrine consent further in the sale of loan and financial products.

The deadline for the RBC is earlier than the DPDP Act - 1st January 2027.

Here's what the new amendments say about consent:

- **Bundled consents are effectively dead.** Gone are the days when your loan product sneaked in a bundled third party insurance product too. Under the RBC Amendments, the customer needs to specifically opt in to any insurance product. This also means that they can reject the one you suggest and choose their own.
- **Pre-ticked consent boxes are disallowed.** The amendment requires that the default option for any digital consent flow shall be 'No' / 'I do not agree'.
- **Dark patterns face a direct regulatory challenge.** The amendment prohibits the following dark patterns:
  - **Interface interference:** pre-ticked consent boxes, or having "delete my data" and "close account" options deep in the interface.
  - **Basket sneaking:** adding insurance or fraud protection by default at checkout.
  - **Confirm shaming:** guilt-laden unsubscribe flows ("No, I prefer to stay uninformed").
  - **Forced action:** requiring access to contacts, camera, or location to complete registration, unless genuinely required by regulation and transparently disclosed.
  - **Trick wording:** double negatives like "Uncheck this box if you do not want offers."
  - **False urgency, drip pricing, bait and switch:** countdown timers, undisclosed processing fees, advertised rates that change at application.
- **Language translation.** Just like the DPDP Act requires consent notices in the customer's language, the RBC Directions require all sale documents, including terms and conditions, to be available in a local language.
- **Promotional communication.** Promotional alerts may only go to customers who have given explicit consent to receive them, and unsubscribing must be easy and simple. DSAs (Direct Selling Agents), DMAs (Direct Marketing Agents) must also respect "Do not disturb" flags.

CHAPTER

10

Legal Provisions



01. Section 2, Digital Personal Data Protection Act, 2023

02. Section 4, Digital Personal Data Protection Act, 2023

03. Section 5, Digital Personal Data Protection Act, 2023

04. Section 6, Digital Personal Data Protection Act, 2023

05. Section 7, Digital Personal Data Protection Act, 2023

06. Section 8, Digital Personal Data Protection Act, 2023

07. Section 10, Digital Personal Data Protection Act, 2023

08. Section 11, Digital Personal Data Protection Act, 2023

09. Section 12, Digital Personal Data Protection Act, 2023

10. Section 13, Digital Personal Data Protection Act, 2023

11. Section 14, Digital Personal Data Protection Act, 2023

12. Section 17, Digital Personal Data Protection Act, 2023

13. Chapter IV, Digital Personal Data Protection Act, 2023

14. Rule 6, Digital Personal Data Protection Rules, 2025

15. Rule 7, Digital Personal Data Protection Rules, 2025

16. Rule 14, Digital Personal Data Protection Rules, 2025

17. Section 13, RBI (Commercial Banks – Credit Facilities) Directions, 2025

18. Section 13, RBI (NBFCs – Credit Facilities) Directions, 2025

19. Reserve Bank of India (Commercial Banks – Know Your Customer) Directions, 2025

20. Reserve Bank of India (Non-Banking Financial Company – Know Your Customer) Directions, 2025

21. RBI's Responsible Business Conduct (RBC) Directions — Amendments

Consentin by Leegality

Consentin is an all-in-one DPDP compliance platform for all your privacy compliance needs.

Consent Collect

Collect consent with minimal drop-offs across various channels.

Cookie Consent

Manage cookie consent without slowing down website performance.

Consentin Lens

Discover and map personal data across structured and unstructured systems.

Privacy Centre

Allow customers to manage consent and raise grievances on your platform.

Rights Management

Log, assign, and track every rights request against its SLA.

Retention & Deletion

Automate retention and deletion across internal systems and third-party vendors.

Assessments

Conduct DPIA, PIA and third-party assessments and automate risk management.

Breach Notification

Manage breach response workflows and send breach notifications.

Built with 10+ years of Leegality's experience

Privacy-first companies have already started using Consentin:

Union Bank of India · YES BANK · SBI card · Coca-Cola Hindustan Coca-Cola Beverages · Chola Enter a better life

5paisa · PAYMENTZ · IIFL CAPITAL · IIFL HOME LOAN · IIFL FINANCE

Payswiff A subsidiary of Chola · ORIX · Livlong 365 · Chola Securities Enter a better life · Flipkart Finance Private Limited