



Implementing user consent under India's Data Protection law

Case studies from the financial sector

March 2024

Koan Advisory Group

Implementing user consent under India's Data Protection law

Case studies from the financial sector



Koan Advisory Group is a New Delhi-based public policy consultancy. It specialises in policy and regulatory analysis in both traditional and emergent sectors and markets. For more information, please visit: www.koanadvisory.com

Author

Ateesh Nandi

Acknowledgement

The author thanks Rakesh Maheshwari and Srishti Joshi for their insight and support.

©2024 Koan Advisory Group

All rights reserved. No part of this publication may be reproduced or transmitted in any form or by any means without permission in writing from Koan Advisory Group

contactus@koanadvisory.com | www.koanadvisory.com

TABLE OF CONTENTS

List of Abbreviations	04
Introduction	06
Overview	07
Interplay between the Act and sectoral rules	08
Select case studies from the financial sector	09
4.1 UPI payments	09
4.2. Card payments (credit/debit cards)	10
4.3. Digital lending	10
4.4. KYC records management	12
4.5. Insolvency records management	13
4.6. Credit scoring	13
Application of the Act to regulated services	16
5.1. Responsibility and accountability	16
5.2. Explicit consent requirements	16
Exploring options within the framework of the Act	18
6.1. Way forward	18
Endnotes	19

Abbreviations

The Act	Digital Personal Data Protection Act, 2023
CERSAI	Central Registry of Securitisation Asset Reconstruction and Security Interest of India
CIC	Credit information company
CIC Act	Credit Information Companies Act, 2005
DLA	Digital lending app
IBC	Insolvency and Bankruptcy Code, 2016
IRDAI	Insurance Regulatory and Development Authority of India
KYC	Know your customer
LSP	Lending service provider
NBFC	Non-banking financial company
NeSL	National E-Governance Services Limited
NPCI	National Payments Corporation of India
PA/PGs	Payment aggregators / Payment gateways
PML Rules	Prevention of Money Laundering (Maintenance Of Records) Rules, 2005
PMLA	Prevention of Money Laundering Act
PSO	Payment system operator
RBI	Payment and Settlement Systems Act, 2007
RBI	Reserve Bank of India
SEBI	Securities and Exchange Board of India
TPAP	Third-party application provider
UPI	Unified Payments Interface
UPI PSP Bank	UPI payment service provider bank

Summary

The Digital Personal Data Protection Act, 2023 (the Act) requires that user consent be ‘free, specific, informed, unconditional, and unambiguous’, and be provided through a clear ‘affirmative action’. It clarifies that data fiduciaries can withhold services if user consent is refused or withdrawn. The Act also prescribes a set of carve outs and exceptions to the explicit user consent requirement.

In this paper, we examine potential conflicts between the Act and sectoral data protection requirements. We discuss three case studies from the financial sector where multiple stakeholders work in tandem to deliver services. We discuss another three case studies involving mandatory data exchange among regulated entities.

In the first set of cases, we look at value chains for digital payments and lending. Personal data is processed by multiple entities including banks, networks, fintech service providers etc., for service delivery. We note that consent to sharing of data for service delivery is implicit where the data principal consents to use a regulated service. If a user provides her phone number and bank details to a Unified Payments Interface (UPI) payment app, she needs to provide separately consent to have it shared with banks and the National Payments Corporation of India (NPCI) for making UPI payments.

In the second set, we look at mandatory data sharing frameworks established under the Credit Information Companies Act, 2005 (CIC Act), the Prevention of Money Laundering Act, 2002 (PMLA), and the Insolvency and Bankruptcy Code, 2016 (IBC). Mandatory data sharing under the PMLA and IBC fall within the carve outs and exceptions under the Act.

Central Registry of Securitisation Asset Reconstruction and Security Interest of India (CERSAI) serves as the central know-your-customer (KYC) records registry under the PMLA. As a public body, CERSAI can qualify as an ‘instrumentality of the state’ under Section 7(c) of the Act, and can lawfully process data under the PMLA without having to obtain explicit user consent. Similarly, the National E-Governance Services Limited (NeSL) manages data relating to insolvency claims under the IBC. Data processing by NeSL is specifically exempted from consent requirements under Section 17(1)(f) of the Act.

However, the same cannot be said for credit information companies (CICs), which are private entities that process personal data to prepare credit scores as per the CIC Act. Data processing by CICs does not fall within any of the contexts specified as ‘legitimate uses’ under Section 7 of the Act, nor is it exempted under Section 17. Financial sector entities are statutorily mandated to share data with CICs for credit scoring. The Act however makes this contingent on explicit user consent – which may create unintended challenges. Incomplete and inaccurate data may for instance create risks for lenders.

Mandatory data sharing frameworks should be included within the ‘legitimate uses’ of data. As such, Central Government may exercise its executive powers to exempt explicit consents for credit scoring under the CIC Act. Aside from the case studies discussed in this paper, there may be other sectors where the strict application of explicit consent may need to be revisited. These would need to be examined separately in due course.

Introduction

The Digital Personal Data Protection Act, 2023 (the Act) is India's first data protection law. It will come into effect when the Central Government issues an official notification.¹ At present, the bespoke data regulator is yet to be instituted and several aspects of the Act are yet to be crystallised.

The Central Government is expected to publish and notify the rules on various aspects of the Act in January, 2024,² an essential step to operationalise the Act and create a uniform data protection framework for private and public entities across sectors. This framework would however include regulated sectors where data protection standards are already in place. As overlaps and potential conflicts between the Act and sectoral data protection rules may impact regulatory predictability, they need to be addressed at the outset.

In this paper we discuss the interplay between the Act and existing sectoral data protection rules. We examine certain activities regulated by the Reserve Bank of India (RBI) as well as mandatory data exchange frameworks in the financial sector, as case studies.

We note that rigorous enforcement, especially of the provisions pertaining to explicit user consent, may inadvertently create challenges in operationalising the Act. Therefore, we discuss ways for the Central Government to align and harmonise the proposed and existing legal frameworks for data protection.

Overview

In this section, we discuss concepts fundamental to the Act, in particular, how personal data is lawfully processed and who is responsible for it under the Act.

Centralised responsibility and liability. The Act assigns responsibility for the protection of personal data on the entity which determines the purpose and means of data processing – the data fiduciary. Data fiduciaries are wholly responsible for ensuring that data processors comply with provisions of the Act. They are responsible for compliance even when processing is undertaken on their behalf by a data processor.

Explicit consent, and various carve-outs. The Act prescribes a notice-consent framework for lawful data processing. A data fiduciary must provide an itemised notice specifying the data sought to be collected and the purpose of processing the data. The individual whose data is sought (the data principal) must then provide ‘free, specific, informed, unconditional, and unambiguous’ consent to the data fiduciary through ‘a clear affirmative action’.³

However, data fiduciaries can process data without explicit user consent in certain specified contexts. Defined in the law as ‘legitimate uses’, these contexts include data processing for delivering public services, complying with court orders, or responding to a pandemic.⁴ Notably, the explicit consent requirement, along with various other provisions,⁵ is also lifted in other specified cases – such as data processing for law enforcement, the performance of regulatory functions, or corporate restructuring.⁶

Interplay between the Act and sectoral rules

Before discussing case studies from the financial sector, we introduce the question of applicability and conflict of data protection requirements. We discuss whether the Act would supersede sectoral data protection requirements, and if so, to what extent.

Existing RBI rules are either activity-centric (such as rules for digital lending) or entity-centric (such as rules for payment aggregators and payment gateways: PA/PGs). These include bespoke data protection requirements in certain cases. For instance, regulated entities engaged in digital lending are subject to consent requirements and purpose limitations on how they collect, use, and store individuals' data, and whom they share it with.⁷ In co-branded card arrangements where a card issuer (such as a bank or an NBFC) ties up with a co-branding entity for marketing and distribution, the co-branding entity is prohibited from accessing information on transactions undertaken through the co-branded card.⁸ Similarly, merchants and PA/PGs are prohibited from storing un-tokenised (i.e. unmasked) card details,⁹ and UPI payment app providers are required to obtain informed user consent for sharing data with third-parties.¹⁰

The Act introduces uniform data protection requirements for data fiduciaries. Its objective is to establish a proportionate responsibility framework for data protection through 'general, and in certain cases, special obligations on entities that process personal data.'¹¹ Section 38 of the Act is meant to ensure consistency with other laws. In case of a conflict between a provision of the Act and any other law in force, the Act would prevail to the extent of such conflict.¹²

However, the provisions of the Act are enforceable in addition to, not in derogation of any existing law governing the processing of personal data.¹³ In other words, the Act does not override laws that prescribe stricter data protection standards than its own. This is evident in the case of data processing outside of India, where stricter localisation rules, such as for payment system data,¹⁴ override the Act.¹⁵

Sectoral requirements such as the data storage and access limitations on PA/PGs and co-branded partners, amount to a stricter data protection standard than the Act prescribes. On the other hand, the Act prescribes a stricter standard of user consent and accountability for data fiduciaries than existing laws.

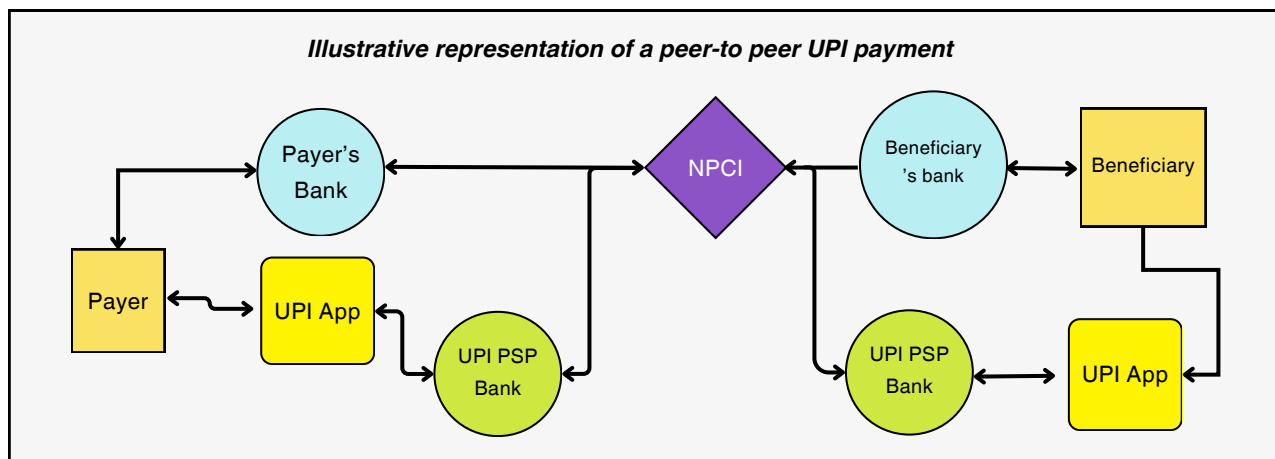
Select case studies from the financial sector





We examine a total of six regulated ‘value chains’ – that is, a network of entities that work in tandem to deliver a service or perform a commercial activity – and analyse how provisions of the Act would apply to them.

We first examine the value chains for digital payments and digital lending because multiple stakeholders are involved in transaction fulfilment. In digital payments for instance, personal and transaction data is shared amongst banks, networks, and fintech service providers. Similarly, in digital lending, fintech businesses that facilitate loans or credit products typically exchange personal data with the various lenders they have partnered with. Illustrations of these value chains are discussed below.

4.1 UPI payments

A peer-to-peer UPI payment is authorised by the payer on her UPI app, which triggers a series of data exchanges between the network of PSP banks on UPI and NPCI for payment fulfilment.

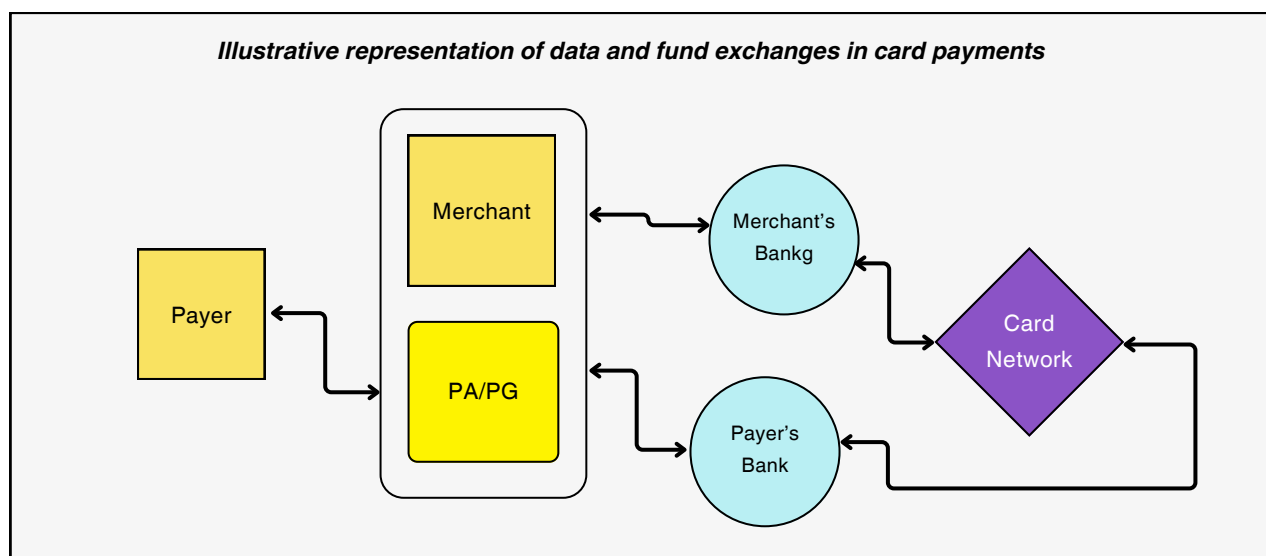






Symbol	Stakeholder	Comments
	UPI Third Party Application Provider (UPI app)	As the customer facing entity, these fintech businesses often serve as points of data collection.
	UPI Payment Service Provider (PSP) Bank	These entities link bank platforms to the UPI network and issue UPI IDs. UPI apps must link their systems with PSP banks to facilitate payments. ¹⁶
	Payer's bank / beneficiary's bank	Transaction amounts are debited / credited from these accounts.
	National Payments Corporation of India (NPCI)	NPCI is an RBI authorised payment system operator (PSO). All exchanges of messages (such as OTP authorisation requests or debit / credit alerts) and funds are routed through the NPCI.

Source: Author's own; RBI¹⁷

4.2 Card payments (credit/debit cards)

An online card payment (card-not-present transaction) typically involves a merchant on-boarded to a PA/PG for payment fulfilment. Once a user authorises payment, data exchanges occur amongst banks, PA/PGs and the payment network.

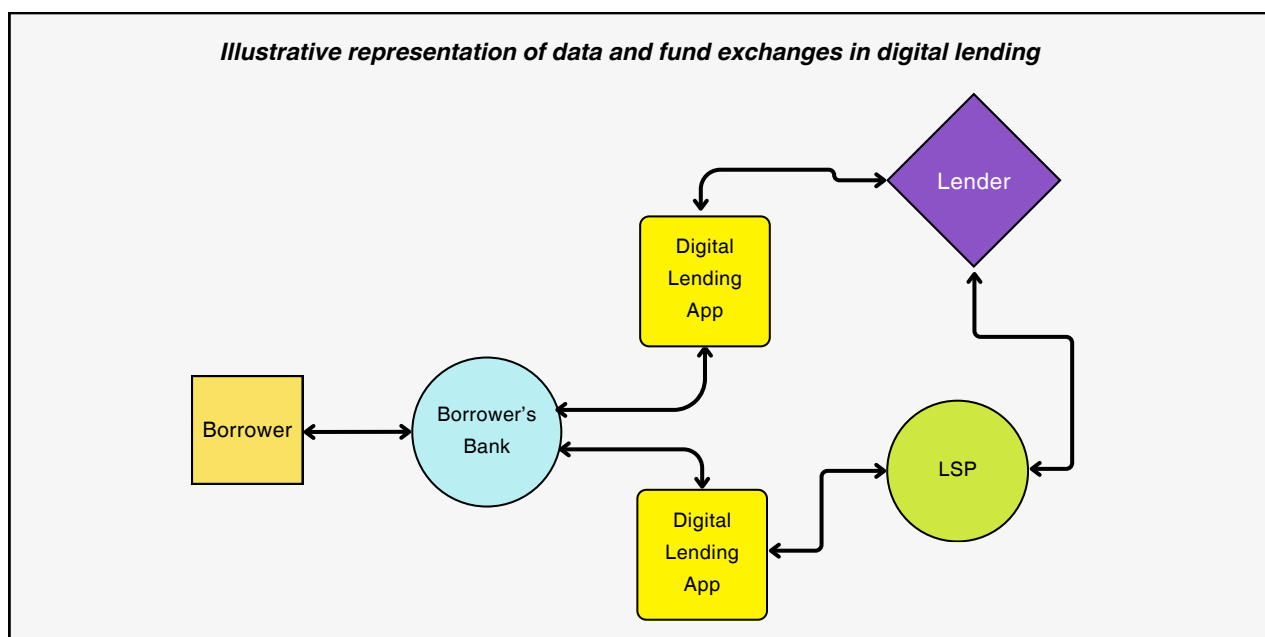






Symbol	Stakeholder	Comments
	Merchant	As the customer facing entity, merchants typically collect card details for transactions.
	UPI Payment Service Provider (PSP) Bank	PA/PGs either facilitate the transaction or provide only the technological interface for securely routing transactions. Many merchants outsource payment processing entirely to PAs.
	Payer's bank / merchant's bank	Transaction amounts are debited / credited from these accounts.
	Networks	Networks are PSOs. They include international card networks such as Visa, Mastercard etc., as well as the NPCI.

Source: Author's own; RBI¹⁸

4.3 Digital lending

A data principal accesses digital lending services from a digital lending app. Data is exchanged between fintech lending service providers, the lender, and banks. However, fund transfers (loan disbursement, interest payments etc.) take place directly between the borrower and the lender, and not via the fintech service provider's account.



Symbol	Stakeholder	Comments
	Digital Lending App (DLA)	Authorised lenders can disburse loans and credit products directly from their own DLAs, or indirectly via the DLAs of the LSPs they partner with.
	Lending Service Provider (LSP)	LSPs facilitate loans on behalf of authorised lenders. They play a key role in customer acquisition, loan servicing and account management.
	Borrower's bank	The loan amount is credited and interest payments are debited from this account.
	Authorised lender	Authorised lenders include commercial and cooperative banks and NBFCs. ¹⁹

Source: Author's own; RBI²⁰

Stakeholders in the value chains for UPI payments, card payments and digital lending interact with each other at the instance of the user. As the first touchpoint for the data principal, the customer facing entity typically obtains the user consents for data processing. Currently, these entities obtain user consents at the time of sign-up or account opening for a variety of purposes. Consent notices for users' personal data such as phone numbers and bank details typically specify the purpose of collection using broad phrases like 'provision of services' or 'compliance with law'. We will discuss how the Act may impact this practice in section 5 of the paper.

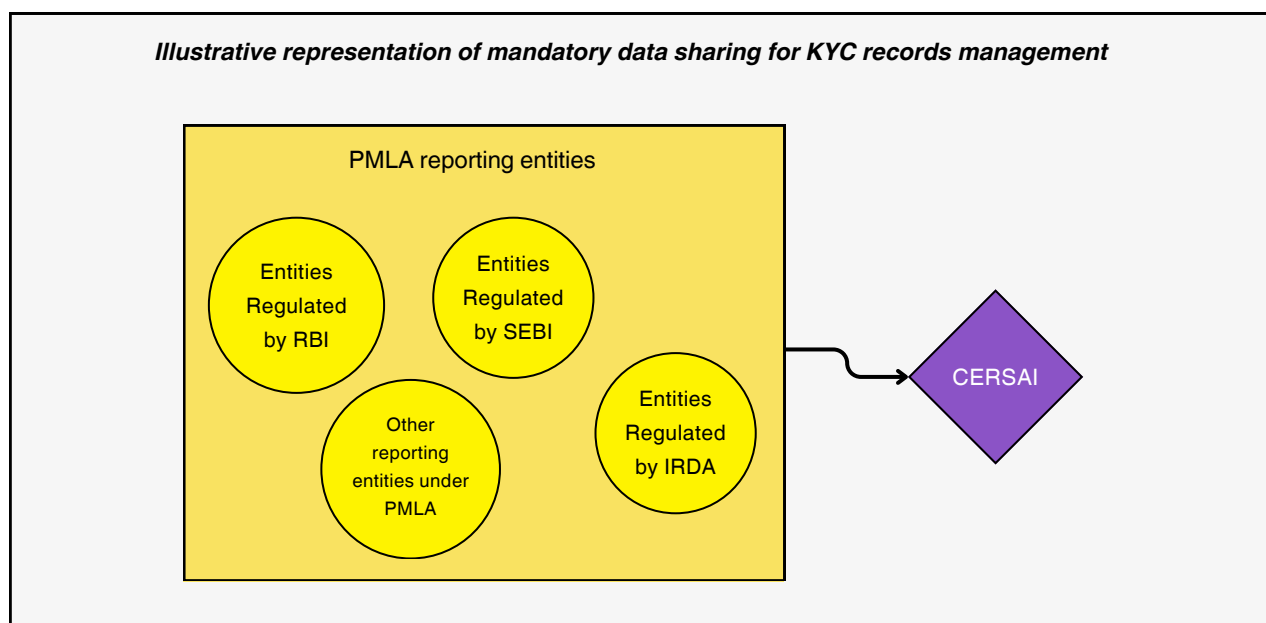
Next, we take up three cases involving mandatory data exchange. These include the statutory frameworks for:



1. KYC records management under the Prevention of Money Laundering Act, 2002 (PMLA),
2. Insolvency records management under the Insolvency and Bankruptcy Code, 2016 (IBC), and
3. Credit scoring under the Credit Information Companies Act, 2005 (CIC Act).

Data sharing in these cases does not occur at the instance of a user seeking services, but rather due to the requirements of a law. In each of these frameworks, entities such as banks or financial institutions are required to share the personal data of their clients with certain designated entities. Illustrations of these value chains are discussed below.

4.4 KYC records management

Reporting entities under the PMLA are required to furnish KYC records of their clients to the Central KYC Records Registry under the PMLA.²¹

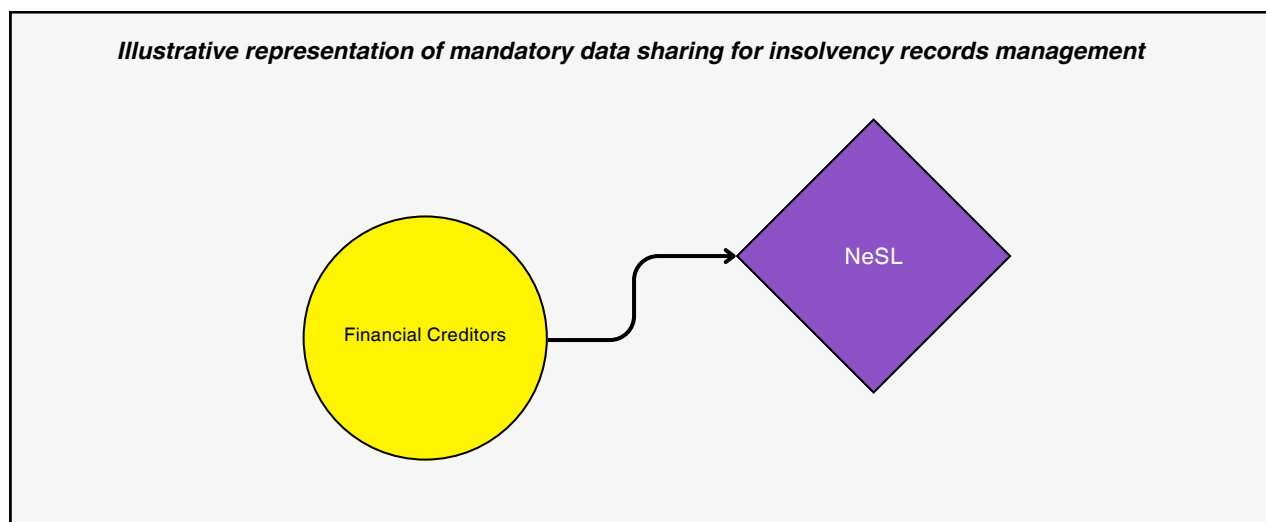




Symbol	Stakeholder	Comments
	Central Registry of Securitisation Asset Reconstruction and Security Interest of India (CERSAI)	<p>The Central Government authorised CERSAI to perform the functions of the Central KYC Records Registry under the PMLA vide Gazette Notification No. S.O. 3183(E) dated November 26, 2015.</p> <p>A Central KYC Records Registry is defined as a public entity authorised to safeguard and retrieve the KYC records of persons who undertake any financial transaction or activity with a designated reporting entity under PMLA.²²</p>
	Reporting entities under PMLA	<p>Every 'reporting entity' under the PMLA is required to share a digital copy of their client's KYC records to the CERSAI upon commencing an account-based relationship with a client.</p> <p>Reporting entities include entities regulated by the RBI,²³ SEBI,²⁴ IRDAI,²⁵ and any notified person performing a 'designated business or profession' under the PMLA, such as virtual asset service providers.²⁶</p>

Source: Author's own; RBI

4.5 Insolvency records management

'Information utilities' set up under the IBC receive, verify and authenticate data on 'financial debts' from various financial institutions.

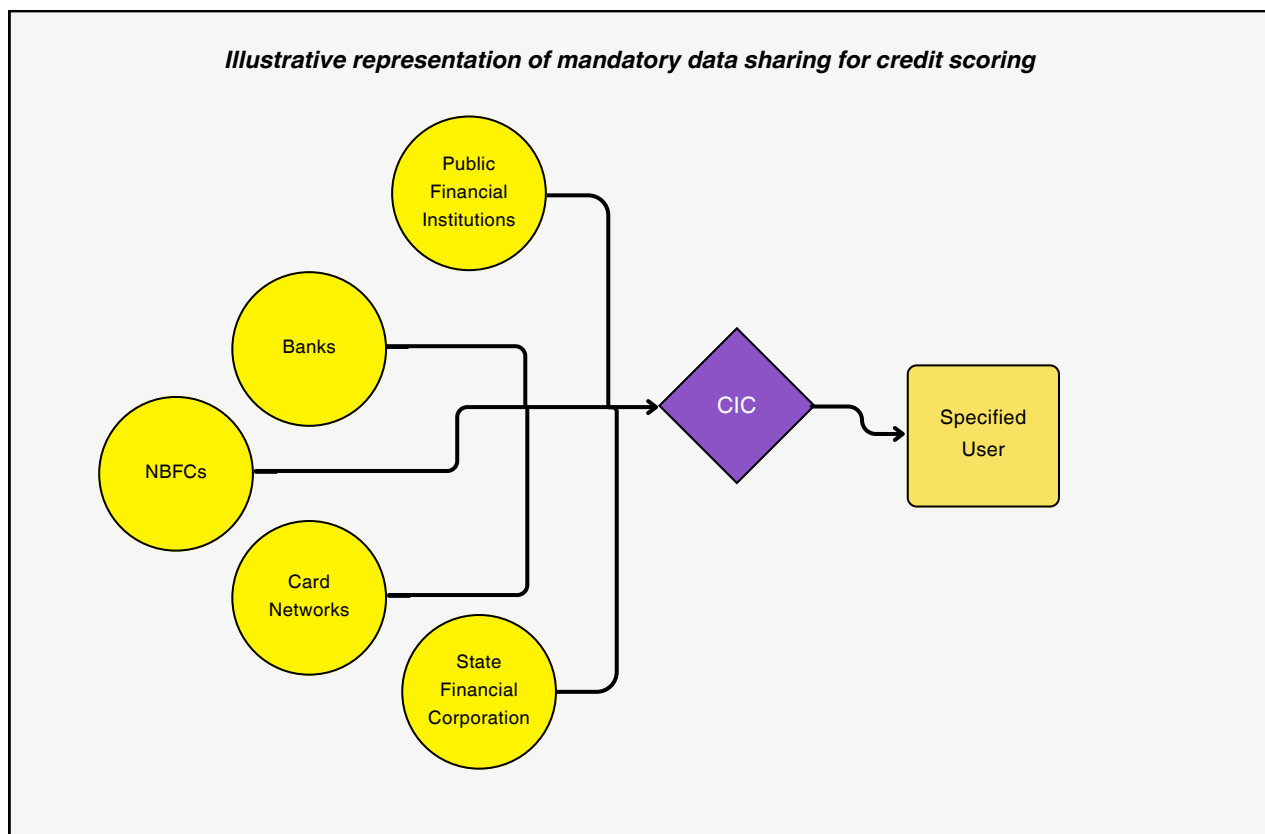





Symbol	Stakeholder	Comments
	National E-Governance Services Limited (NeSL)	<p>NeSL is currently the only authorised information utility under the IBC. The IBC authorises it to verify financial information for the determination of insolvency proceedings.</p> <p>The term 'financial information' includes details of a person's indebtedness, assets, liabilities, etc.²⁷</p>
	Financial creditors	<p>The IBC mandates financial creditors to submit information relating to financial debts to the NeSL²⁸ as per the Insolvency and Bankruptcy Board of India (Information Utilities) Regulations, 2017.</p> <p>A financial creditor is any person or entity to whom a 'financial debt' is owed. A financial debt is one that includes interest as consideration for the time-value of money. It covers all forms of borrowing, any liability under a lease or hire purchase agreement, indemnity bonds, etc.²⁹</p>

Source: Author's own; RBI

4.6 Credit scoring

Credit scoring takes place by credit information companies (CICs) who process the data shared by financial institutions to prepare credit reports.



Symbol	Stakeholder	Comments
	Credit Information Company (CIC)	CICs are entities authorised by the RBI to conduct the 'business of credit information' as per the CIC Act.
	Credit Institution	<p>Credit institutions such as banks, NBFCs, etc. are required to become members of at least one CIC and share 'credit information' for the purpose of credit scoring.³⁰</p> <p>The CIC Act defines 'credit information' to include data on the quantum and nature of loans sanctioned or disbursed, on the borrower's repayment history, on assets furnished as collateral or security, and on defaults, penal interest levies etc.³¹</p>
	Specified user	<p>A specified user under the CIC Act is an entity allowed to process credit information from CICs within the purpose limitations set out in the Credit Information Companies Regulations, 2006.</p> <p>'Specified users' include regulators such as the SEBI and IRDAI, all credit institutions and CICs, insurance companies, telecom service providers, NeSL, SEBI-registered stockbrokers, and others. Fintech businesses that process data to support CICs and that meet the RBI's eight-point eligibility criteria also qualify as specified users.³²</p>

Source: Author's own; RBI

Entities such as CERSAI and NeSL are subject to 'financial, administrative, or functional control over by the state'.³³ They also perform functions bearing a close nexus to 'governmental functions of public importance', and enjoy a monopoly status in the market that is conferred or protected by the state.³⁴ As such, they can qualify as 'instrumentalities of the state' – with significant implications for compliance under the Act. Data processing by the state or any of its instrumentalities for the performance of legally mandated functions amounts to a 'legitimate use' of data,³⁵ and falls outside the consent framework of the Act.³⁶

The functions discharged by NeSL are specifically exempt from various provisions of the Act – including explicit consents – under Section 17(1)(f) of the Act. NeSL, the only authorised 'information utility' under the IBC, processes data for the purpose of 'ascertaining the financial information and assets and liabilities of any person who has defaulted' on their loan payments.³⁷ For this reason, it is exempt from most of the obligations applicable to ordinary data fiduciaries. Moreover, the rights available to data principals, such as the right to have their personal data erased, are not enforceable against NeSL.³⁸

Application of the Act to regulated services

In this section, we discuss how provisions of the Act on accountability and user consent apply to the identified value chains. We first discuss which entities would be treated as data fiduciaries and data processors in regulated sectors. We then discuss how explicit user consent requirements would affect the identified value chains.

5.1 Responsibility and accountability

Each entity covered in this paper – whether a bank, financial institution, fintech service provider, or a CIC, CERSAI or NeSL – is responsible for determining the manner and purpose of data processing. It may process personal data either to provide core services, or for promotions and service optimisation. For instance, PhonePe, a popular UPI TPAP, collects user data such as mobile number, device identifiers, gender, and income for purposes such as KYC verification, marketing, and compliance with the law.³⁹ In this case the sharing of certain user data is necessary for service delivery. Similarly, the business of digital lending is predicated on the exchange of user data on income and indebtedness, for instance, between financial institutions and fintech service providers. Because these entities determine the purpose and means of processing data for their own ends, and not on behalf of another person under a principal-agent relationship, they should be treated as data fiduciaries under the Act.

On the other hand, service providers in outsourcing arrangements should be treated as data processors under the Act. Regulated entities in the financial sector often outsource non-core activities to third-party service providers,⁴⁰ which process personal data on behalf of another entity as their agents, and thus should be considered data processors. They must nonetheless be asked to provide specific representations, warranties, and indemnities in respect of compliance with various requirements of the Act, and thus be contractually accountable to their data fiduciaries for data breaches and other non-compliances.

5.2 Explicit consent requirements

The Act requires that notices for data collection be specified in granular detail, and user consent be purpose-limited and obtained through a clear affirmative action. Strict application of these requirements may affect the operation of certain essential services in the financial sector.

In the first three cases, users agree to share data along the value chain so as to receive services. No one stakeholder in the value chain can deliver services on its own.

Under the framework of the Act, however, a user or data principal may want to use UPI but refuse consent for data sharing with the NPCI, for instance. In such a case, the UPI payment app would be unable to provide the payment service, and may refuse service delivery. Section 6(5) of the Act allows a data fiduciary to stop providing services if the data principal withdraws or withholds their consent. The provision however applies only if user consents for necessary purposes are not provided or are withdrawn.

In practice, this means the notices issued by the consumer-facing entity will include a list of other entities that must receive personal data for service delivery. For instance, UPI payment apps would need to specify that

they will share user data with the NPCI and with UPI PSP banks to fulfil transactions. Similarly, lending apps would need to specify which banks and NBFCs will process the borrower's application.

The user consent these customer facing apps collect for service delivery should automatically include consent for necessary data sharing along the value chain. That said, explicit consents must separately be obtained for data sharing with third parties for services not necessary to the core service offering – such as marketing, app-optimisation etc.

Applying explicit consent requirements becomes more challenging in the last three cases where the exchange of data is mandated by law. In these cases, the data principal does not initiate the data sharing.

Mandatory data exchange frameworks typically correspond to a larger public interest objective. For instance, centralised KYC records helps law enforcement authorities monitor the risk of money laundering or terror financing. Similarly, an information utility under the IBC verifies and authenticates financial data to ensure the integrity of corporate insolvency resolution proceedings. Equally, credit scores help financial institutions determine the terms of their loans and assess the size of capital buffers required.⁴¹

These legitimate objectives may be disrupted if data sharing always requires explicit user consent. Not all data fiduciaries are equally impacted by this, however. Public bodies like CERSAI or NeSL can qualify as an 'instrumentality of the state' for the purposes of Section 7(c) of the Act and can lawfully process data without explicit user consent.⁴² In any case, data processing by NeSL is specifically included in the exemptions to the Act.

CICs do not qualify as instrumentalities of the state, nor is processing for credit scoring exempt under Section 17 of the Act. Credit institutions (such as banks and NBFCs) are required to furnish historical financial data of borrowers, such as defaults on loans, payment behaviour, etc., to CICs.⁴³ This information is not shared at the instance of a data principal. CICs issue notices to credit institutions to share financial data as per the CIC Act. They also leverage data and insights from non-traditional or alternative data such as utility bill payments, e-commerce transactions and phone-related location data to compute credit scores.⁴⁴ CICs are notably subject to data protection principles such as purpose limitation, data minimisation and data accuracy.⁴⁵

Under the framework of the Act, credit institutions would need explicit consents from users for sharing data with CICs. If a data principal declines to provide consent, the credit institution would be stuck between upholding their right of refusal under the Act, and complying with the data sharing mandate under the CIC Act.

A potential incongruity therefore arises between data sharing mandates over private entities and the explicit consent requirements under the Act. We discuss possible ways for the Central Government to address the same in the concluding section.

Exploring options within the framework of the Act

Management of KYC records helps law enforcement authorities monitor money laundering and terror financing risks. Insolvency records management helps ensure the integrity of corporate insolvency resolution processes. Equally, access to accurate and complete data mitigates credit risks for lenders and liquidity risks in the macro economy. Upholding explicit consent requirements for the purpose of credit scoring may impact the accuracy of credit reports, and erode value from India's fintech sector.

Mandatory data sharing frameworks should in general be treated as 'legitimate uses' so long as data sharing takes place in accordance with the applicable regulatory standards and procedural guidelines. The existence of regulatory licensing and supervision can justify the dilution of the affirmative consent requirement in these cases.

The Central Government has residuary rulemaking powers under Section 40(z) of the Act and the power to remove difficulties in giving effect to any provision of the Act under Section 43. It also has the power to exempt application of the law over specified data fiduciaries for a specified period under Section 17(5) of the Act. It may exercise any of these powers to classify the operation of mandatory data sharing frameworks involving private entities as 'legitimate uses.'

6.1 Way forward

Our analysis suggests that affirmative user consents have the potential to disrupt the operation of regulated value chains. Two key takeaways from the above discussion are:

1. Consent for necessary data sharing among stakeholders in a value chain should be implicit when a user signs up to a regulated service.
2. Mandatory data sharing frameworks involving private entities should not be contingent on explicit user consent, and be included instead within the 'legitimate uses' of data.

Accordingly, the Central Government may classify the operation of mandatory data sharing frameworks as 'legitimate uses' of processing by issuing an order under Section 40(z) or Section 43. These exemptions should apply only over data sharing that takes place according to applicable regulatory standards and procedural guidelines. In the alternate, the Central Government may exempt explicit consent requirements over mandatory data exchanges. It may bring regulated entities such as CICs within the exemptions under Section 17(1)(b) of the Act. The RBI has wide powers under the CIC Act to issue directions, and determine the policies and functioning of CICs. Credit scoring under the CIC Act framework is arguably a part of its supervisory functions to mitigate macro financial risks.

Aside from credit scoring, moreover, there may be other value chains that are impacted by the requirement of affirmative user consent. These need to be examined. For instance, value chains regulated by SEBI, IRDAI and PFRDA involve coordination amongst multiple stakeholders for service delivery. They also include mandatory data exchange, where the strict application of explicit user consents may need to be revisited. A similar exploration may be conducted also in the case of activities outside direct regulatory oversight – such as domain name registration, public directory services etc.

Endnotes

- 1 Section 1 (2) of the Act.
- 2 Staff report, *DPDP rules to be out by January-end, says MoS IT Rajeew Chandrasekhar*, Business Standard, January 16, 2024, Available at: https://www.business-standard.com/india-news/dpdp-rules-expected-to-be-released-by-end-of-the-month-mos-chandrasekhar-124011600679_1.html
- 3 Section 6(1) of the Act.
- 4 Section 7 of the Act.
- 5 The provisions of Chapter III (Rights and duties of data principal) and most provisions of Chapter II (Obligations of Data Fiduciary) do not apply in the cases covered in Section 17(1).
- 6 Section 17(1) of the Act.
- 7 Annexure 1, Paragraph 10, 11 and 12, RBI Guidelines of Digital lending dated September 02, 2022, Available at: <https://rbidocs.rbi.org.in/rdocs/notification/PDFs/GUIDELINESDIGITALLENDINGD5C35A71D8124A0E92AEB940A7D25BB3.PDF>.
- 8 Paragraph 21 (b), RBI Master Direction – Credit Card and Debit Card – Issuance and Conduct Directions, 2022, dated April 21, 2022, Available at: https://rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=12300.
- 9 See Tokenisation – Card Transactions: Permitting Card-on-File Tokenisation (CoFT) Services, dated September 07, 2021. Available at: <https://rbi.org.in/Scripts/NotificationUser.aspx?Id=12159&Mode=0>; Guidelines on Regulation of Payment Aggregators (PAs) and Payment Gateways dated 17 March 2020. Available at: <https://rbi.org.in/Scripts/NotificationUser.aspx?Id=11822&Mode=0>
- 10 See NPCI UPI Procedural Guidelines Version 1.7, October 2019, Available at: <https://www.scribd.com/document/497710607/UPI-Procedural-Guidelines-pdf-26112019-OnwebsiteLIVE-0>.
- 11 Paragraph 4(c), Statement of objects and reasons, the Digital Personal Data Protection Bill, 2023. Available at: https://prsindia.org/files/bills_acts/bills_parliament/2023/Digital%20Personal%20Data%20Protection%20Bill,%202023.pdf
- 12 Section 38 (2) of the Act.
- 13 Section 38 (1) of the Act.
- 14 See RBI FAQs on Storage of Payment System Data, June 26, 2019, Available at: <https://www.rbi.org.in/commonperson/English/Scripts/FAQs.aspx?Id=2995>
- 15 Section 16(2) of the Act.
- 16 See NPCI list of TPAPs and partner PSP banks. Available at: <https://www.npci.org.in/what-we-do/upi/3rd-party-apps>
- 17 See RBI, Discussion Paper on Charges in Payment Systems. Available at: <https://rbidocs.rbi.org.in/rdocs/Publications/PDFs/DPSSDISCUSSIONPAPER5E016622B2D3444A9F294D07234059AA.PDF>
- 18 *Ibid*
- 19 Section 1, RBI Guidelines on Digital Lending, September 1, 2022. Available at: <https://rbidocs.rbi.org.in/rdocs/notification/PDFs/GUIDELINESDIGITALLENDINGD5C35A71D8124A0E92AEB940A7D25BB3.PDF>
- 20 RBI Guidelines on Digital lending, September 1, 2022. Available at: <https://rbidocs.rbi.org.in/rdocs/notification/PDFs/GUIDELINESDIGITALLENDINGD5C35A71D8124A0E92AEB940A7D25BB3.PDF>
- 21 <https://www.ckycindia.in/ckyc/?r=faq>
- 22 Prevention of Money Laundering (Maintenance Of Records) Rules, 2005, (PML Rules)
- 23 RBI Master Direction - Know Your Customer (KYC) Direction, 2016 (Updated as on October 17, 2023). Available at: https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=11566
- 24 SEBI Circular, Operationalisation of Central KYC Records Registry (CKYCR), July 21, 2016. Available at: https://www.sebi.gov.in/legal/circulars/jul-2016/operationalisation-of-central-kyc-records-registry-ckycr-_32870.html?QUERY
- 25 IRDAI Circular, Operationalisation of Central KYC Records Registry (CKYCR), July 13, 2016. Available at: <https://irdai.gov.in/document-detail?documentId=382568>
- 26 See Financial Intelligence Unit – India, AML & CFT Guidelines for Reporting Entities providing services related to Virtual Digital Assets, 2023. Available at: https://fiuindia.gov.in/pdfs/AML_legislation/AMLCFTguidelines10032023.pdf.
- 27 Section 3 (13), IBC.
- 28 Section 215, IBC.
- 29 Section 5(8), IBC.

Endnotes

- 30 See Section 15 and 16 of the CIC Act.
- 31 Section 2(d), CIC Act.
- 32 RBI, Eligibility criteria for entities to be categorised as Specified User under clause (j) of Regulation 3 of the Credit Information Companies (Amendment) Regulations, 2021. Available at: <https://rbidocs.rbi.org.in/rdocs/content/pdfs/Eligibility05012022.pdf>
- 33 Zee Telefilms Ltd. & Anr. v. Union Of India & Ors., AIR 2005 SC 2677.
- 34 Sukhdev Singh & Ors., v. Bhagatram Sardar Singh Raghuvanshi, (1975) 1 SCC 421.
- 35 Section 7(c) of the Act.
- 36 Section 4(1) of the Act.
- 37 See Section 17(1)(f) of the Act.
- 38 Chapter II except sub-sections (1) and (5) of section 8, and Chapter III are not covered in exemptions.
- 39 See PhonePe Privacy Policy. Available at: <https://www.phonepe.com/privacy-policy#information-collection>.
- 40 See RBI Framework for Outsourcing of Payment and Settlement-related Activities by Payment System Operators, August 3, 2021. Available at: <https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=12136&Mode=0>. See also, SEBI Guidelines on Outsourcing of Activities by Intermediaries, December 15, 2011. Available at: https://www.sebi.gov.in/legal/circulars/dec-2011/guidelines-on-outsourcing-of-activities-by-intermediaries_21752.html
- 41 BIS working papers How do credit ratings affect bank lending under capital constraints, September 2018. Available at: <https://www.bis.org/publ/work747.pdf>
- 42 As per Section 7(c), data processing *'for the performance by the State or any of its instrumentalities of any function under any law for the time being in force in India or in the interest of sovereignty and integrity of India or security of the State'* is a legitimate use.
- 43 See Sections 15, 16 and 17 of the CIC Act.
- 44 Shehnaz Ahmed, Alternative Credit Scoring – A Double Edged Sword, Vidhi Centre for Legal Policy, December 8, 2020. Available at: <https://vidhilegalpolicy.in/research/alternative-credit-scoring-a-double-edged-sword/>
- 45 See Chapter VI, CIC Act read with the Credit Information Companies Rules, 2006.



©2024 Koan Advisory Group

All rights reserved. No part of this publication may be reproduced or transmitted in any form or by any means without permission in writing from Koan Advisory Group

contactus@koanadvisory.com | www.koanadvisory.com