INDIAN JOURNAL OF LEGAL AFFAIRS AND RESEARCH

Peer-reviewed, open-access, refereed journal

IJLAR

+91 70421 48991
editor@ijlar.com
www.ijlar.com

DISCLAIMER

The views and opinions expressed in the articles published in the Indian Journal of Legal Affairs and Research are those of the respective authors and do not necessarily reflect the official policy or position of the IJLAR, its editorial board, or its affiliated institutions. The IJLAR assumes no responsibility for any errors or omissions in the content of the journal. The information provided in this journal is for general informational purposes only and should not be construed as legal advice. Readers are encouraged to seek professional legal counsel for specific legal issues. The IJLAR and its affiliates shall not be liable for any loss or damage arising from the use of the information contained in this journal.

IJLAR

Introduction

Welcome to the Indian Journal of Legal Affairs and Research (IJLAR), a distinguished platform dedicated to the dissemination of comprehensive legal scholarship and academic research. Our mission is to foster an environment where legal professionals, academics, and students can collaborate and contribute to the evolving discourse in the field of law. We strive to publish high-quality, peer-reviewed articles that provide insightful analysis, innovative perspectives, and practical solutions to contemporary legal challenges. The IJLAR is committed to advancing legal knowledge and practice by bridging the gap between theory and practice.

IJLAR

Preface

The Indian Journal of Legal Affairs and Research is a testament to our unwavering commitment to excellence in legal scholarship. This volume presents a curated selection of articles that reflect the diverse and dynamic nature of legal studies today. Our contributors, ranging from esteemed legal scholars to emerging academics, bring forward a rich tapestry of insights that address critical legal issues and offer novel contributions to the field. We are grateful to our editorial board, reviewers, and authors for their dedication and hard work, which have made this publication possible. It is our hope that this journal will serve as a valuable resource for researchers, practitioners, and policymakers, and will inspire further inquiry and debate within the legal community.

IJLAR

Description

The Indian Journal of Legal Affairs and Research is an academic journal that publishes peer-reviewed articles on a wide range of legal topics. Each issue is designed to provide a platform for legal scholars, practitioners, and students to share their research findings, theoretical explorations, and practical insights. Our journal covers various branches of law, including but not limited to constitutional law, international law, criminal law, commercial law, human rights, and environmental law. We are dedicated to ensuring that the articles published in our journal adhere to the highest standards of academic rigor and contribute meaningfully to the understanding and development of legal theories and practices.

IJLAR

DIGITAL LENDING IN INDIA: REGULATORY ACCOUNTABILITY AND BORROWER DATA PROTECTION UNDER THE RBI DIGITAL LENDING DIRECTIONS, 2025 AND THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023

AUTHORED BY - ANEESHA BISWAS & KATRIONA SEN
Student, Amity Law School, Kolkata

Abstract

India's digital lending market has widened access to credit through mobile applications and third-party platforms, but has also exposed borrowers to opaque data collection, intrusive recovery and uncertainty over responsibility between lenders and technology intermediaries. The Reserve Bank of India (RBI) addresses sector-specific risks through the Reserve Bank of India (Digital Lending) Directions, 2025 (Digital Lending Directions), while the Digital Personal Data Protection Act, 2023 (DPDP Act) establishes a broader data-protection framework. This article examines accountability among regulated entities (REs), lending service providers (LSPs) and other data handlers. It argues that the RBI framework places primary supervisory responsibility on REs, while the DPDP Act follows the entity determining the purposes and means of processing. Their interaction raises questions about LSP status, consent, recovery-related processing, regulatory coordination and lending outside the RBI perimeter. The article proposes reforms that make accountability depend on actual conduct, not contractual labels.

Keywords: digital lending; RBI; DPDP Act; data fiduciary; lending service provider; borrower protection; regulatory accountability.

I. Introduction

Digital lending has shifted parts of the credit process from customer acquisition and credit assessment to disbursal, servicing and recovery from physical branches to digital platforms. This model can reduce transaction costs and widen access to credit. It can also create serious risks where borrowers do not know which entity is lending, what data is being collected, or

how that data will be used. The RBI's Working Group on Digital Lending identified concerns arising from unregulated applications, third-party outsourcing, data privacy, mis-selling and unethical recovery practices.[1]

The RBI issued Guidelines on Digital Lending in September 2022 and separate instructions on default loss guarantees in June 2023[2]. In May 2025, it consolidated earlier instructions and added measures for multi-lender arrangements and a public directory of digital lending apps[3]. The DPDP Act was enacted in 2023 and its Rules were notified on 13 November 2025. Because commencement is staggered, the applicable provisions must be identified by date.[4]

This article asks: who is accountable when personal data is misused during a digital loan transaction, and through which regulatory mechanism can the borrower obtain an effective remedy? It argues that the RBI framework and the DPDP Act are potentially complementary, but their effectiveness depends on identifying the real decision-maker behind data processing and coordinating sectoral supervision with data-protection enforcement. The analysis is doctrinal and states the legal position as at 3 November 2026.

II. The Regulatory Architecture

A. RBI Digital Lending Directions: responsibility anchored in the regulated entity

The Digital Lending Directions apply to specified RBI-regulated entities, including commercial banks, co-operative banks, non-banking financial companies and all-India financial institutions. An LSP is defined as an agent of an RE that performs one or more digital-lending functions on the RE's behalf. The Directions do not create a general licensing regime for every technology platform that facilitates credit; instead, they regulate digital lending undertaken by REs and the arrangements through which those REs engage LSPs.[5]

The central accountability rule is explicit: outsourcing does not dilute or absolve the RE of its statutory or regulatory obligations, and the RE remains fully responsible and liable for the acts and omissions of its LSP. The RE must conduct enhanced due diligence, assess the LSP's

[1] Reserve Bank of India, Report of the Working Group on Digital Lending Including Lending Through Online Platforms and Mobile Apps (Nov. 2021).
[2] Reserve Bank of India, Guidelines on Digital Lending, RBI/2022-23/111, DOR.CRE.REC.66/21.07.001/2022-23 (Sept. 2, 2022); Reserve Bank of India, Guidelines on Default Loss Guarantee (DLG) in Digital Lending, RBI/2023-24/40, DOR.CRE.REC.21/21.07.001/2023-24 (June 8, 2023).
[3] Reserve Bank of India (Digital Lending) Directions, 2025, RBI/2025-26/36, DOR.STR.REC.19/21.07.001/2025-26 (May 8, 2025) [hereinafter Digital Lending Directions].
[4] Digital Personal Data Protection Act, No. 22 of 2023, Gazette of India, Extraordinary, pt. II, sec. 1 (Aug. 11, 2023) [hereinafter DPDP Act]; Digital Personal Data Protection Rules, 2025, G.S.R. 846(E), Gazette of India, Extraordinary, pt. II, sec. 3(i) (Nov. 13, 2025) [hereinafter DPDP Rules].
[5] Digital Lending Directions, supra note 3, paras. 2–4.

data-privacy policies and storage systems, enter into a contract defining the parties' roles, and periodically review the LSP's conduct. This is important because the borrower ordinarily experiences the app and its interface, not the internal contractual allocation between the lender and the service provider.[6]

The Directions also regulate the borrower-facing transaction. They require creditworthiness assessment and key disclosures, including the Key Fact Statement (KFS); regulate disbursal and repayment so that funds ordinarily move directly between the borrower and the RE; require a cooling-off period; and provide for grievance redressal. Where an LSP works with multiple REs, loan offers must be presented in an objective and comparable manner, and the interface must not use dark or deceptive patterns to push a particular lender's product.[7]

Data governance is addressed directly. Collection must be need-based and supported by prior, explicit consent, with an auditable trail. Borrowers must be able to deny consent for specific data uses and revoke consent where applicable. The Directions restrict access to mobile-phone resources such as contact lists and call logs, regulate access to device functions for limited purposes, require a comprehensive privacy policy, and prescribe storage requirements for data collected in the digital-lending process. These sector-specific requirements apply to REs and the LSPs engaged by them.[8]

The RBI has also operationalised reporting of RE-deployed digital lending apps through its Centralised Information Management System (CIMS), with a public directory intended to help customers verify an app's claimed association with an RE. The directory is not an RBI endorsement or a guarantee of an app's conduct; the RBI has stated that the information is based on RE submissions. It is therefore a useful verification tool, but not a substitute for supervisory validation or borrower due diligence.[9]

B. DPDP Act: accountability based on the function performed

The DPDP Act distinguishes a Data Principal, a Data Fiduciary (the person determining the purposes and means of processing) and a Data Processor (a person processing data on behalf of a fiduciary). An LSP's status therefore cannot be settled merely by describing it as an 'agent'

[6] Id. para. 5(i)–(vii).
[7] Id. paras. 6–11.
[8] Id. paras. 12–15.
[9] Reserve Bank of India, Press Release, Reserve Bank of India (Digital Lending) Directions, 2025 (May 8, 2025); Ministry of Finance, Government and RBI Strengthen Digital Lending Ecosystem Through New Regulatory Framework, Digital Lending App Directory and Enhanced Customer Safeguards, Press Information Bureau (July 21, 2026).

or 'processor' in a contract; its actual conduct must be examined.[10]

Once the relevant substantive provisions commence, the Act will require processing to be for a lawful purpose and on the basis of consent or a specified legitimate use. It sets requirements for notice and consent, imposes general obligations on Data Fiduciaries including security safeguards and breach notification and gives Data Principals rights relating to access, correction, erasure and grievance redressal. The Schedule permits a penalty of up to ₹250 crore for failure to take reasonable security safeguards. These obligations should not, however, be described as fully operative before their notified commencement date.[11]

The constitutional context is the Supreme Court's recognition in K.S. Puttaswamy that privacy is a fundamental right. That decision supplies an important constitutional foundation for evaluating state and private interference with personal information, although the precise statutory obligations applicable to a lender must still be traced to the relevant legislation and regulations.[12]

A limited comparison with the European Union's General Data Protection Regulation (GDPR) is instructive. The GDPR expressly structures controller–processor responsibility, requires risk-based impact assessments in specified high-risk processing, and regulates certain solely automated decisions. India's DPDP Act similarly distinguishes fiduciaries and processors, but does not create an equivalent general right to an explanation of automated credit decisions. The comparison supports targeted Indian guidance on algorithmic lending, without assuming that the two statutes are identical.[13]

IJLAR

C. Staggered commencement: the importance of timing

The commencement notification dated 13 November 2025 brought the DPDP Act's institutional provisions including the establishment and functioning provisions concerning the Data Protection Board into force on publication. Section 6(9), concerning registration of Consent Managers, is scheduled to commence one year after publication, on 13 November 2026. The principal processing obligations and Data Principal rights in sections 3 to 17, together with the corresponding substantive Rules, are scheduled to commence eighteen months after publication, on 13 May 2027. Accordingly, as at 3 November 2026, the principal

[10] DPDP Act, supra note 4, § 2(i), (k).
[11] Id. §§ 4–15, 33 & sched.
[12] K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1 (India).
[13] Regulation (EU) 2016/679, arts. 5, 6, 22, 28, 35, 2016 O.J. (L 119) 1.

substantive duties in those provisions have not yet commenced.[14]

This distinction is central to the article. The RBI Digital Lending Directions already impose sector-specific obligations on REs and their LSPs. The DPDP Act's substantive framework is prospective until 13 May 2027, even though the institutional provisions have commenced. It is therefore inaccurate to state that all DPDP rights, consent duties, breach-notification duties or penalties are presently enforceable. The transition also requires careful treatment of the Information Technology Act, 2000 and the rules made under it, to the extent those provisions remain applicable before the relevant DPDP provisions commence.

III. Key Accountability Problems

A. The RE–LSP relationship: contractual labels versus actual control

The RBI Directions make the RE responsible for the acts and omissions of its LSP. The DPDP Act, by contrast, asks who determines the purpose and means of processing. Where an LSP merely processes borrower information on the RE's documented instructions, it is likely to fall within the Data Processor category; the RE remains the Data Fiduciary and cannot contract out of its statutory responsibility. If, however, an LSP independently decides to use borrower data for its own purposes for example, to build a separate customer profile, cross-sell unrelated products or create proprietary datasets, it may itself qualify as a Data Fiduciary for that processing.[15]

This creates layered accountability. RBI supervises the RE and its regulated activities, while the DPDP framework may apply directly to any entity qualifying as a Data Fiduciary. REs should map each LSP's actual data activities and determine whether it acts only on instructions or independently decides processing purposes. Contracts should reflect, not replace, that assessment.

The RBI's DLA directory improves transparency but has limits. Because the directory is based on information supplied by REs and does not amount to RBI certification, it cannot by itself establish that every app is safe or compliant. Effective accountability requires audit trails, periodic verification and a clear route for borrowers to report an app that misrepresents its association with a regulated lender.

[14] Notification No. G.S.R. 843(E), Gazette of India, Extraordinary, pt. II, sec. 3(i) (Nov. 13, 2025); DPDP Rules, supra note 4, r. 1(2)–(4).
[15] DPDP Act, supra note 4, §§ 2(i), (k), 8(1)–(2).

B. Consent in loan journeys: necessity, bundling and interface design

Digital credit requires some personal information to assess identity, income and creditworthiness. The legal issue is not whether a lender may collect any data, but whether each category of data is necessary for a specified lending purpose and whether the borrower is given a meaningful choice about additional uses. The DPDP Act's consent standard free, specific, informed, unconditional and unambiguous must be read with its requirement that consent be limited to personal data necessary for the specified purpose. In the lending context, this supports a distinction between data reasonably required to assess or service a loan and data sought for unrelated marketing, profiling or cross-selling.[16]

Consent can nevertheless become formal rather than meaningful when it is embedded in lengthy loan terms, presented through confusing screens or made a practical condition of receiving credit even for optional processing. The KFS addresses loan pricing and key contractual information, but it cannot alone cure a misleading data-permission interface. Research on privacy self-management and mandated disclosure cautions that individuals may not be able to assess the cumulative consequences of repeated consent decisions.[17]

A related concern is the use of interface design to steer borrowers. The RBI Directions' express prohibition on dark or deceptive patterns in multi-lender digital views is significant, but further guidance could clarify how similar practices are to be assessed across the wider loan journey. Regulators should consider whether optional data permissions are separated from essential permissions, whether 'decline' is as accessible as 'accept', and whether the borrower can understand the consequence of refusing a non-essential permission.[18]

The DPDP Rules also provide for registered Consent Managers. India's Account Aggregator framework separately enables consent-based sharing of financial information. The two systems serve related but not identical functions. Regulatory guidance should clarify their respective roles and whether a single consent artefact can meet the requirements of both frameworks without creating duplicate or confusing consent journeys.[19]

[16] Id. §§ 4, 6(1); Digital Lending Directions, supra note 3, para. 12.
[17] Daniel J. Solove, Privacy Self-Management and the Consent Dilemma, 126 Harv. L. Rev. 1880 (2013); Omri Ben-Shahar & Carl E. Schneider, The Failure of Mandated Disclosure, 159 U. Pa. L. Rev. 647 (2011).
[18] Digital Lending Directions, supra note 3, para. 6(iii); Ryan Calo, Digital Market Manipulation, 82 Geo. Wash. L. Rev. 995 (2014).
[19] DPDP Act, supra note 4, § 6(7)–(9); Reserve Bank of India, Master Direction—Non-Banking Financial Company—Account Aggregator (Reserve Bank) Directions, 2016 (Sept. 2, 2016).

C. Two regulatory frameworks, one lending transaction

The DPDP Act operates in addition to other laws and prevails to the extent of inconsistency. It also preserves another Indian law that provides greater protection or restriction on cross-border transfers. RBI data-storage requirements should therefore be analysed as sector-specific obligations, not assumed to be displaced by the DPDP Act.[20]

A single incident may engage both regulators. An LSP's unauthorised use of borrower information may raise questions about the RE's due diligence under the RBI Directions and, once the relevant DPDP provisions commence, the responsibilities of the RE or an independent Data Fiduciary. The Supreme Court has recognised the breadth of the RBI's regulatory role, but parallel powers make coordination important.[21]

The DPDP Act describes the Board as an independent body, although its members are appointed by the Central Government and their service conditions are prescribed by it. This may prompt debate about practical independence. The Justice B.N. Srikrishna Committee had recommended a more independent data-protection authority; the issue is best framed as one of institutional safeguards, not legal status.[22]

D. Default-related processing: a carefully bounded exemption

A significant qualification arises under section 17(1)(f) of the DPDP Act. It exempts specified processing undertaken to ascertain the financial information, assets and liabilities of a person who has defaulted on a loan or advance from a financial institution, subject to compliance with disclosure requirements under other applicable law. The exemption is purpose-specific. It should not be described as a general exemption for all debt recovery, all collection activity or any use of a borrower's data after default.[23]

Section 17(1) excludes most of Chapter II, Chapter III and section 16 for the specified exempt processing, while expressly retaining sections 8(1) and 8(5). The retained provisions include the Data Fiduciary's responsibility for processing carried out by it or on its behalf and the duty to take reasonable security safeguards. The provision does not retain every obligation in section 8: in particular, the breach-notification duty in section 8(6) is not among the retained provisions for processing covered by section 17(1). This is a material limitation and should be

[20] DPDP Act, supra note 4, §§ 16, 38; Digital Lending Directions, supra note 3, para. 13.
[21] Internet & Mobile Ass'n of India v. Reserve Bank of India, (2020) 10 S.C.C. 274 (India).
[22] DPDP Act, supra note 4, §§ 18–20, 28, 36; Committee of Experts Under the Chairmanship of Justice B.N. Srikrishna, A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians (Ministry of Electronics & Information Technology 2018).
[23] DPDP Act, supra note 4, § 17(1)(f).

acknowledged rather than suggesting that all DPDP borrower protections continue to apply to exempt processing.

The exemption does not authorise harassment, public shaming or indiscriminate access to contact lists. RBI instructions separately prohibit intimidation and privacy intrusions by recovery agents, including inappropriate contact with family or friends and persistent calls at prohibited hours. The law must distinguish legitimate ascertainment of a defaulter's financial position from abusive collection or unrelated exploitation of data.[24]

E. Lending outside the regulated perimeter and algorithmic opacity

The RBI framework is strongest where a regulated entity is involved. An unauthorised app operating wholly outside that perimeter may not be directly supervised as an RE or LSP under the Digital Lending Directions. The DPDP Act may apply to a person processing digital personal data within its scope once its substantive provisions commence, but data-protection compliance is not a substitute for a law governing the business of lending itself. The 2024 draft Banning of Unregulated Lending Activities Bill was not enacted as a central statute. In February 2026, the Supreme Court recorded that a draft was in circulation among States and Union Territories and called for appropriate legislation to check unauthorised money lending.[25]

Digital lenders may use alternative data and automated tools to assess creditworthiness. The DPDP Act's Significant Data Fiduciary framework may require impact assessments and audits where an entity is so designated. However, the Act does not create a general right to an explanation of every automated credit decision. RBI should clarify expectations for model governance, validation, bias testing and human review.[26]

IV. Recommendations

First, the RBI and the Data Protection Board should adopt a coordination protocol covering referrals, information-sharing, preservation of evidence and sequencing of enforcement. Such a protocol should respect each authority's statutory mandate while reducing the risk of inconsistent findings or duplicated proceedings.

Second, REs should be required to maintain a data-processing responsibility map for each

[24] Id. § 17(1) (excluding Chapter II except §§ 8(1), 8(5), Chapter III and § 16); id. § 8(6).
[25] Reserve Bank of India, Outsourcing of Financial Services—Responsibilities of Regulated Entities Employing Recovery Agents, RBI/2022-23/108, DOR.ORG.REC.65/21.04.158/2022-23 (Aug. 12, 2022); Digital Lending Directions, supra note 3, para. 5(v).
[26] Department of Economic Affairs, Ministry of Finance, Draft Banning of Unregulated Lending Activities Bill, 2024 (Consultation Draft, Dec. 2024); Order, SLP (Crl.) No. 5485 of 2024 (Sup. Ct. India Feb. 16, 2026).

LSP. The map should identify the data collected, purposes, retention periods, onward disclosures, subcontractors and whether the LSP acts as a processor or an independent fiduciary for particular activities. Contractual descriptions should be tested against actual practice.

Third, RBI and the Ministry of Electronics and Information Technology should issue joint guidance on consent architecture for digital loans, including the relationship between Consent Managers and Account Aggregators. Borrowers should receive short, purpose-specific notices and be able to refuse optional processing without losing access to data that is genuinely necessary for underwriting or servicing.

Fourth, the RBI should develop practical interface standards for digital loan journeys. These could include equal prominence for acceptance and refusal of optional permissions, prohibition of pre-ticked optional consents, clear explanations of data use, and periodic testing for dark patterns. This would complement the existing KFS rather than duplicate it.

Fifth, guidance should clarify the narrow scope of section 17(1)(f). It should state that the exemption is not permission to access contact lists, disclose a borrower's default to unrelated persons, or use financial information for unrelated marketing. Recovery agents and LSPs should remain subject to applicable RBI conduct requirements.

Sixth, the Union and State Governments should address the unregulated-lending perimeter through coordinated legislation and enforcement, consistent with the Supreme Court's February 2026 observations. The framework should distinguish genuine credit facilitation from unauthorised lending and provide accessible complaint and takedown mechanisms for fraudulent applications.

Finally, RBI should strengthen expectations for algorithmic credit governance, including documentation of material models, periodic validation, testing for discriminatory outcomes, clear allocation of responsibility between REs and vendors, and human review mechanisms for material adverse decisions.

V. Conclusion

India's framework combines sectoral supervision of REs with the DPDP Act's functional approach to data-processing responsibility. Their interaction can strengthen borrower protection, but only if the real actors are identified and the limits created by phased commencement and statutory exemptions are recognised.

The most significant unresolved issue is fragmented accountability. A borrower may interact with an app, contract with a regulated lender and have data processed by one or more

service providers. The law must make it possible to identify who is responsible, which authority can act and what remedy is available. Clearer LSP classification, coordinated enforcement, meaningful consent design, proportionate recovery safeguards and oversight of algorithmic lending would help ensure that digital innovation does not dilute the legal responsibilities owed to borrowers.

