

Original Research Article

Data Privacy in Grassroots Banking - Assessing DPDP Act Readiness in Urban Cooperative Banks in the Era of AI

Mr. Nitin Janki Mamatu Pimparkar,¹ Dr. Ramraj T. Nadar^{2*}

¹Research Scholar – Guru Nanak College of Arts, Science and Commerce, University of Mumbai, 400037 Maharashtra, India

²Research Guide – Vice Principal & Head, Department of Commerce, Guru Nanak College of Arts, Science and Commerce, University of Mumbai, 400037 Maharashtra, India

Corresponding author E-mail: ramraj@gncasc.org

Received: 10 September, 2026 | Accepted: 23 September, 2026 | Published: 28 September, 2026

Abstract

The rapid digitisation of financial services has fundamentally transformed the operational framework of banking institutions in India. Urban Cooperative Banks (UCBs), which serve as vital grassroots financial institutions, play a crucial role in advancing financial inclusion by extending banking services to small businesses, middle-income groups, and underserved communities across urban and semi-urban regions. However, the accelerating adoption of digital banking platforms, artificial intelligence (AI), cloud computing, and data analytics has resulted in the extensive collection and processing of personal and financial information, thereby raising critical concerns related to data privacy, cybersecurity, and ethical governance. The Digital Personal Data Protection (DPDP) Act, 2023, enacted by the Government of India, introduces a comprehensive legal framework for safeguarding digital personal data by defining the obligations of data fiduciaries, establishing rights for data principals, and mandating accountability mechanisms for organisations processing personal data (Government of India, 2023). For UCBs, compliance with the DPDP Act is not merely a regulatory necessity but also a strategic opportunity to enhance

customer trust, strengthen cybersecurity practices, improve governance standards, and enable the responsible adoption of AI-driven banking solutions.

This research paper examines the readiness of Urban Cooperative Banks to implement the requirements of the DPDP Act, 2023, particularly in the context of AI-enabled banking operations. The study adopts a qualitative exploratory approach based on secondary data collected from regulatory reports, academic literature, government publications, Reserve Bank of India (RBI) guidelines, and industry studies. The analysis evaluates UCB preparedness across five key dimensions: legal compliance, governance capability, AI adoption, cybersecurity readiness, and ethical responsibility. The study identifies that while UCBs have made notable progress in digital transformation, significant challenges remain, including limited technological infrastructure, high compliance costs, a shortage of skilled professionals, dependence on legacy systems, and inadequate AI governance mechanisms. To address these issues, the paper proposes a DPDP compliance framework incorporating privacy-by-design principles, AI governance practices, cybersecurity enhancement, employee training, vendor management, and regulatory oversight. The research concludes that effective implementation of the DPDP Act, 2023 can enable Urban Cooperative Banks to achieve responsible digital transformation while protecting customer privacy, strengthening institutional resilience, and enhancing trust in India's cooperative banking ecosystem.

Keywords: Data Privacy, DPDP Act 2023, Urban Cooperative Banks, Artificial Intelligence, AI Governance, Banking Ethics, Cybersecurity, Data Protection, Digital Banking, Financial Inclusion.

1. Introduction

The Indian banking sector has undergone significant digital transformation in recent years, driven by technological advancements, government-led digital initiatives such as Digital India and the Pradhan Mantri Jan Dhan Yojana, and an increasing customer preference for digital financial services. Urban Cooperative Banks (UCBs), which have traditionally been established to support local communities, small enterprises, and financially underserved groups, have increasingly adopted digital platforms such as internet banking, mobile banking, Unified Payments Interface (UPI) payments, electronic Know Your Customer (e-KYC), and automated banking solutions. The Reserve Bank of India's Financial Inclusion Index, which rose to 67.0 in March 2025 from 64.2 in March 2024, reflects the growing penetration of digital financial services across all categories of banking institutions, including cooperative banks (Press Information Bureau, 2025).

While digital transformation has undeniably enhanced accessibility and operational efficiency, it has also significantly increased the volume of customer data collected and processed by financial institutions. Banking organisations now routinely handle sensitive information including identity details, transaction history, financial records, and behavioural data derived from digital interactions. The growing dependence on data-driven systems has created substantial concerns regarding privacy protection, cybersecurity, and responsible data usage. The increasing frequency and sophistication of cyberattacks targeting financial institutions globally, including those in India, have further underscored the urgency of establishing robust data protection mechanisms. The Picus Blue Report 2024 found that the financial services sector achieved only a 17% prevention rate against certain ransomware threats, with alert scores dropping sharply from 18% to 6%, leaving critical threats undetected (Picus Security, 2024).

The emergence of Artificial Intelligence (AI) has added a further layer of complexity to the banking landscape. AI applications such as fraud detection systems, automated credit assessment models, customer service chatbots, predictive analytics, and risk management systems provide significant operational benefits including improved accuracy, speed, and cost efficiency. However, AI-based banking also introduces challenges relating to transparency, explainability, automated decision-making, data minimisation, and ethical use of customer information. Scholars have highlighted that algorithmic bias and the lack of explainability in AI-driven financial decisions can disproportionately affect vulnerable populations, including those served by cooperative banks (Bank of England, 2023; Women's World Banking, 2024). The Bank of England has noted that beyond inherent issues with bias, fairness and ethics, AI may create or amplify financial stability and monetary stability risks (Bank of England, 2023). Similarly, Women's World Banking (2024) has documented how gender-related algorithmic bias in financial services can restrict women's access to credit and other financial products, with biases originating in prejudiced datasets.

The Digital Personal Data Protection (DPDP) Act, 2023 provides India with its first dedicated legal framework for protecting digital personal data. The Act, which received the President's assent on 11 August 2023, places responsibility on organisations processing personal data—designated as Data Fiduciaries—and provides individuals, referred to as Data Principals, with greater control over their personal information (Government of India, 2023). The DPDP Rules, 2025, subsequently notified by the Ministry of Electronics and Information Technology (MeitY) on 14 November 2025 after nationwide consultations that received 6,915 inputs, provide detailed operational guidelines for implementation (MeitY, 2025). For UCBs, compliance with the DPDP Act requires comprehensive improvements in governance structures, technology infrastructure, employee awareness, vendor management, and AI oversight.

This study examines DPDP readiness among Urban Cooperative Banks and proposes a practical framework for implementing data privacy and responsible AI governance in grassroots banking institutions. The paper is organised as follows: Section 2 discusses the nature and importance of UCBs; Section 3 provides the background of the DPDP Act and AI in banking; Section 4 reviews the existing literature; Section 5 identifies the research gap; Section 6 outlines the objectives; Section 7 describes the methodology; Section 8 presents the conceptual framework; Sections 9 through 13 analyse the impact, readiness, challenges, and strategies; and Section 14 presents the conclusion and recommendations.

2. Urban Cooperative Banks (UCBs): Meaning, Operation and Importance

Urban Cooperative Banks (UCBs) are cooperative financial institutions that provide a wide range of banking services primarily to individuals, small businesses, traders, and local communities in urban and semi-urban areas across India. They operate on the cooperative principle of mutual assistance, where members have a meaningful role in ownership and governance, while their banking activities are regulated under the applicable banking and cooperative regulatory framework administered by the Reserve Bank of India (RBI) and the respective state registrars of cooperative societies. UCBs mobilise deposits from customers and deploy these funds to provide loans, advances, and other financial services to individuals, small enterprises, and local businesses, thereby contributing significantly to financial inclusion, local economic development, and access to formal banking services for populations that may otherwise remain outside the purview of the commercial banking system.

In the current banking landscape, UCBs are increasingly adopting digital banking channels, mobile applications, online transaction platforms, digital KYC verification systems, and data analytics tools, reflecting a broader trend of digital transformation observed across the Indian banking sector (IJNRD, 2024). As a result of this digital expansion, UCBs collect and process significant amounts of customers' personal and financial data, including identity documents, contact information, account details, transaction histories, and credit-related information. The growing use of Artificial Intelligence (AI) in areas such as credit scoring, fraud detection, risk management, and customer service further increases the scale and complexity of data processing activities undertaken by these institutions. This expanded data footprint creates greater concerns regarding data privacy, cybersecurity, unauthorised access, and potential misuse of personal information.

The RBI classifies UCBs into four regulatory tiers based on their deposit size and operational complexity, allowing the central bank to apply differentiated regulatory requirements appropriate to each tier's risk profile. According to the Reserve Bank of India (Urban Co-operative Banks – Licensing, Scheduling and Regulatory Classification) Guidelines, 2025, the four-tier framework comprises: Tier 1—all unit UCBs and salary earners' UCBs (irrespective of deposit size), and all other UCBs having deposits up to ₹100 crore; Tier 2—UCBs with deposits of more than ₹100 crore and up to ₹1000 crore; Tier 3—UCBs with deposits of more than ₹1000 crore and up to ₹10,000 crore; and Tier 4—UCBs with deposits of more than ₹10,000 crore (Reserve Bank of India, 2025). This tiered framework recognises the diversity in size, capacity, and sophistication among UCBs, ranging from large, multi-branch urban banks to smaller, community-focused institutions. The DPDP Act, 2023, and the DPDP Rules, 2025 provide an important overarching framework for protecting digital personal data in India, applicable to all entities processing personal data regardless of their size or sector. Therefore, assessing the readiness of UCBs across all tiers to meet DPDP requirements is critically important for strengthening data governance, protecting customer privacy, maintaining public trust, and ensuring the responsible adoption of digital technologies and AI in grassroots banking institutions.

3. Background of the DPDP Act and Artificial Intelligence in Banking

3.1. Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection (DPDP) Act, 2023, enacted as Act No. 37 of 2023, establishes a comprehensive set of principles for the lawful and responsible processing of digital personal data in India. The object of the Act is to provide for the processing of digital personal data in a manner that recognises both the right of individuals to protect their personal data and the need to process such personal data for lawful purposes (Government of India, 2023). The Act creates a regulatory architecture that defines the roles and obligations of Data Fiduciaries (organisations that determine the purpose and means of processing personal data) and Data Processors (entities that process data on behalf of Data Fiduciaries), while simultaneously establishing enforceable rights for Data Principals (the individuals to whom personal data relates).

The major requirements relevant to banking institutions include: lawful processing of personal data based on consent or legitimate uses; comprehensive consent management with provisions for withdrawal; purpose limitation ensuring data is used only for specified purposes; data minimisation requiring collection of only necessary information; implementation of reasonable security safeguards; mandatory personal data breach reporting to the prescribed authority; establishment of grievance redressal mechanisms; and overarching accountability of Data Fiduciaries for all processing activities undertaken on their behalf, including those carried out by third-party

vendors and service providers (Government of India, 2023). The law rests on seven core principles: consent and transparency, purpose limitation, data minimisation, accuracy, storage limitation, security safeguards and accountability, which guide every stage of data processing.

Given that banks process significant volumes of sensitive personal and financial information on a daily basis, effective compliance with the DPDP Act requires the establishment of strong data governance frameworks, robust security controls, clear accountability mechanisms, and systematic documentation of all data processing activities. The DPDP Act is complemented by the DPDP Rules, 2025, which provide detailed operational requirements including specifications for notice and transparency regarding data collection and processing, mechanisms for consent management and withdrawal, standards for security safeguards, timelines and procedures for breach reporting, protocols for handling Data Principal rights requests and grievances, and additional obligations for entities designated as Significant Data Fiduciaries (MeitY, 2025). The DPDP Act imposes substantial financial penalties for non-compliance by Data Fiduciaries, with the highest penalty up to ₹250 crore applying to failure to maintain reasonable security safeguards. Banks are expected to align DPDP Rule requirements with their existing RBI compliance systems rather than treating them as a separate or parallel regulatory framework.

3.2. Artificial Intelligence in Banking

Artificial Intelligence has become an increasingly important component of modern banking operations, transforming both customer-facing and back-office functions. UCBs are gradually adopting AI-enabled applications that span a range of operational areas, including fraud detection and transaction monitoring systems that analyse patterns in real-time to identify suspicious activities; customer support chatbots that handle routine queries and reduce response times; automated loan assessment models that evaluate creditworthiness using alternative data sources; customer segmentation tools that enable targeted product offerings; predictive analytics for cash flow forecasting and treasury management; and anti-money laundering (AML) monitoring systems that enhance regulatory compliance (National Institute of Standards and Technology, 2023).

Although AI improves operational efficiency and decision-making capabilities, it simultaneously creates significant privacy and ethical concerns because AI systems fundamentally depend on the analysis of extensive datasets. Issues such as algorithmic bias that may lead to discriminatory outcomes, lack of explainability in automated decisions, unauthorised profiling of individuals, and risks associated with third-party AI tools and vendor dependencies require effective governance frameworks. International standards such as the OECD Principles on Artificial Intelligence (OECD, 2019) and the NIST Artificial Intelligence Risk Management Framework (NIST, 2023) emphasise the importance of transparency, accountability, security, and human oversight in AI systems, providing valuable guidance for banking institutions seeking to adopt AI responsibly. The OECD AI Principles, adopted in May 2019, represent the first intergovernmental standard on AI, identifying principles for responsible stewardship of trustworthy AI (OECD, 2019). The NIST AI RMF 1.0, released in January 2023, provides a structured framework for managing risks associated with AI while fostering innovation and promoting trustworthiness (NIST, 2023).

3.3. RBI Regulatory Applicability

The DPDP framework operates alongside, rather than in place of, the existing RBI regulatory requirements governing customer data and financial information. For UCBs, several key regulatory frameworks are relevant and must be considered in an integrated compliance approach. The Master Direction on Know Your Customer (KYC)

Direction, 2016 governs customer identification procedures, KYC data collection, and record retention requirements (Reserve Bank of India, 2016). The Guidelines on Digital Lending, 2022 are applicable to UCBs undertaking digital lending activities and cover requirements for need-based data collection, customer consent, privacy protections, and the arrangements involving Lending Service Providers (LSPs) and Digital Lending Apps (DLAs) (Reserve Bank of India, 2022). The Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices, 2023 applies to all UCBs, with specific emphasis on Tier 3 and Tier 4 banks, and covers cloud computing, IT vendor management, security requirements, due diligence, and outsourcing risk management (Reserve Bank of India, 2023). Additionally, the RBI's Cybersecurity Framework provides a tiered approach to cybersecurity governance, prevention, detection, and incident response for urban cooperative banks. The payment and card-related directions are relevant where UCBs provide payment or card services to their customers.

4. Literature Review

Existing research on digital banking consistently highlights that technology adoption has improved financial inclusion, service efficiency, and customer convenience across diverse banking contexts. Studies examining the digital transformation of cooperative banks in India have noted that while these institutions have made progress in adopting core banking solutions, digital payment systems, and internet banking platforms, they continue to face infrastructure limitations, resource constraints, and capacity gaps that distinguish them from their commercial banking counterparts (IJNRD, 2024). However, increased digital dependence has simultaneously expanded cybersecurity and privacy risks, creating a dual challenge of leveraging technology for growth while managing its inherent risks.

Research on data protection frameworks emphasises that financial institutions require structured privacy governance, transparency, and accountability mechanisms to effectively protect customer data. The European Union's General Data Protection Regulation (GDPR), which came into effect in May 2018, has served as an influential model for data protection legislation worldwide, including India's DPDP Act. Scholars have noted that the GDPR's requirement for data protection by design and by default, enshrined in Article 25, represents a paradigm shift from reactive to proactive privacy management, requiring organisations to embed privacy considerations into the design of systems and processes from the outset (European Parliament and Council of the European Union, 2016). The DPDP Act reflects a similar philosophical orientation, although it is tailored to the Indian regulatory and business environment. The foundational concept of Privacy by Design, originally developed by Cavoukian (2011) and subsequently adopted in international standards such as ISO/IEC 27701:2019 for privacy information management (International Organization for Standardization, 2019), provides a principled approach that is directly relevant to banking institutions seeking to implement the DPDP Act's requirements. Cavoukian's seven foundational principles—proactive not reactive, privacy as the default setting, privacy embedded into design, full functionality, end-to-end security, visibility and transparency, and respect for user privacy—offer a comprehensive framework for embedding privacy into organisational processes and systems (Cavoukian, 2011).

Research on AI in banking identifies significant benefits such as improved fraud detection accuracy, faster credit decision-making, enhanced customer personalisation, and more efficient regulatory compliance monitoring. However, scholars and practitioners have highlighted serious concerns regarding algorithmic fairness, transparency, explainability of automated decisions, and responsible data usage. The Bank of England's analysis of ethical dimensions in AI has noted that algorithmic bias can perpetuate or amplify existing inequalities in financial

services, particularly affecting marginalised communities (Bank of England, 2023). Similarly, Women's World Banking (2024) has documented how gender-related algorithmic bias in financial services can restrict women's access to credit and other financial products. International frameworks such as the OECD AI Principles (OECD, 2019), the NIST AI Risk Management Framework (NIST, 2023), and ISO/IEC 42001:2023 for AI management systems (International Organization for Standardization, 2023) emphasise responsible AI practices grounded in the principles of transparency, accountability, security, and human oversight, providing a normative foundation for AI governance in banking.

A critical observation emerging from the literature review is that existing studies predominantly focus on commercial banks and fintech organisations, with limited academic research addressing the specific data protection challenges and AI governance needs of Urban Cooperative Banks. This gap is significant because UCBs differ from commercial banks in their governance structures, resource availability, technological maturity, and the socio-economic profiles of their customer base. This literature gap highlights the need for a focused analytical framework that addresses the specific limitations, requirements, and developmental trajectories of UCBs in the context of the DPDP Act and responsible AI adoption.

5. Research Gap

A systematic review of the existing body of literature reveals several significant gaps that this study seeks to address. First, there is a notable scarcity of academic research specifically examining DPDP readiness among Urban Cooperative Banks, with the majority of data protection studies focusing on large commercial banks, multinational financial institutions, or fintech companies. Second, there is an insufficient understanding of AI-related privacy risks in the cooperative banking sector, where the unique intersection of limited technological resources, growing AI adoption, and a customer base that may be particularly vulnerable to privacy violations creates a distinctive risk profile that has not been adequately explored. Third, the academic literature lacks structured models or assessment frameworks for evaluating the privacy maturity of grassroots banking institutions, which operate under fundamentally different constraints compared to their commercial counterparts. Fourth, there is limited research integrating DPDP compliance, cybersecurity preparedness, and responsible AI governance into a unified analytical framework applicable to cooperative banks. Fifth, there is an inadequate understanding of the specific technological, financial, organisational, and human-resource challenges faced by smaller banking institutions in implementing comprehensive data protection regimes. This study attempts to address these identified gaps by developing a phased DPDP readiness assessment framework specifically tailored to the context, capabilities, and constraints of Urban Cooperative Banks.

6. Objectives of the Study

The objectives of this study are as follows:

- a) To examine the impact of the Digital Personal Data Protection (DPDP) Act, 2023 on data privacy practices in Urban Cooperative Banks (UCBs).
- b) To assess the readiness of Urban Cooperative Banks for implementing the requirements of the DPDP Act, particularly in the context of AI-enabled banking operations.
- c) To evaluate the role of the DPDP Act in shaping data processing and privacy management practices within Urban Cooperative Banks.

- d) To identify the key challenges faced by Urban Cooperative Banks in ensuring DPDP compliance in the era of AI.
- e) To recommend practical strategies for strengthening data privacy governance and responsible AI adoption in Urban Cooperative Banks.

7. Research Methodology

This study adopts a descriptive and analytical research approach, relying exclusively on secondary data sources. The primary sources of data include: the Digital Personal Data Protection (DPDP) Act, 2023 and the DPDP Rules, 2025, along with related government notifications and publications issued by the Ministry of Electronics and Information Technology; publications, circulars, reports, and guidelines issued by the Reserve Bank of India (RBI), including master directions on IT governance, KYC, digital lending, and IT outsourcing; government notifications and policy documents pertaining to data protection and cooperative banking; peer-reviewed research journals and academic publications addressing data privacy, AI governance, and cooperative banking; industry reports on cybersecurity trends and banking sector vulnerabilities; and published literature on cooperative banking, digital governance, and financial inclusion. The analytical framework evaluates UCB readiness across five dimensions: legal compliance, governance capability, AI adoption maturity, cybersecurity preparedness, and ethical responsibility. Given the secondary data approach, the findings are necessarily interpretive and should be validated through future primary research involving surveys, interviews, or case studies of individual UCBs.

8. Conceptual Framework

The conceptual framework of this study is built upon the recognition that Urban Cooperative Banks primarily cater to middle-income groups, small businesses, self-employed individuals, and local communities who may have limited awareness of data privacy rights and limited ability to exercise control over their personal information. The increasing dependence of these institutions on digital platforms for service delivery has correspondingly increased their exposure to cybersecurity risks and data privacy concerns. The DPDP Act establishes a comprehensive set of obligations for organisations processing personal data, requiring them to: obtain informed and meaningful consent from data principals before processing their personal data; process data only for lawful, specified purposes that have been clearly communicated; maintain reasonable technical and organisational security safeguards to protect personal data against unauthorised access, disclosure, modification, or loss; report personal data breaches to the prescribed authority within the timelines specified under the DPDP Rules; protect and facilitate the exercise of rights of data principals, including the right to access, correct, and erase personal data; and ensure accountability for all data processing activities, including those carried out by third-party service providers and vendors on their behalf (Government of India, 2023; MeitY, 2025). This framework integrates the DPDP Act's requirements with the principles of Privacy by Design (Cavoukian, 2011), the AI governance guidelines from NIST (2023) and OECD (2019), and the RBI's existing regulatory framework for cooperative banks.

9. Impact of DPDP on Data Privacy Practices in UCBs

The DPDP framework is expected to strengthen existing data privacy practices of UCBs across multiple dimensions. Purpose limitation requires that UCBs use customer data only for the purposes that have been clearly specified and communicated at the time of collection, preventing the repurposing of data for unrelated activities. Data minimisation mandates that UCBs collect only the personal data that is strictly necessary for the specified purpose, reducing the volume of sensitive information at risk. Transparency obligations require UCBs to provide

clear, accessible, and comprehensive privacy notices to customers, informing them about the types of data collected, the purposes of processing, the third parties with whom data may be shared, and their rights as data principals. Consent management necessitates the establishment of appropriate mechanisms for obtaining, recording, and managing customer consent, as well as facilitating the withdrawal of consent when requested. Data accuracy requirements compel UCBs to maintain reliable and up-to-date customer information, regularly reviewing and correcting records as necessary.

Furthermore, security obligations require UCBs to strengthen both technical safeguards (such as encryption, access controls, and intrusion detection systems) and organisational measures (such as policies, training, and incident response procedures) to protect personal data. Retention limitation principles require UCBs to avoid the unnecessary retention of personal data beyond the period required for the specified purpose or as mandated by applicable regulations. Data Principal rights provisions require UCBs to establish appropriate mechanisms for receiving, processing, and responding to customer requests and grievances related to their personal data. Accountability obligations require UCBs to maintain comprehensive responsibility for all data processed through third parties, including vendors, service providers, and cloud computing platforms. Finally, breach management obligations require UCBs to integrate DPDP breach reporting requirements with their existing RBI cybersecurity and incident-response mechanisms, ensuring timely detection, reporting, and remediation of data breaches in accordance with both regulatory frameworks.

10. DPDP Readiness of Urban Cooperative Banks: Three-Phase Assessment

10.1. Phase I – Pre-DPDP Phase (2023–2024): Awareness and Gap Assessment

The enactment of the DPDP Act in August 2023 created initial awareness regarding data privacy responsibilities among financial institutions across India. However, during this phase, most Urban Cooperative Banks were still governed primarily by the RBI's cybersecurity directions and internal banking policies, with limited specific attention to the requirements of the new data protection legislation. The major activities undertaken or initiated during this phase included the creation of data inventories to catalogue the types and volumes of personal data held by UCBs; customer data flow mapping to understand how personal data moves through organisational systems and to third parties; review of existing IT policies and data management practices against DPDP requirements; identification of AI applications and their data processing implications; and preliminary privacy risk assessments to identify the most critical gaps and vulnerabilities.

The key challenges during this phase included limited in-house expertise in data protection and privacy law, dependence on legacy banking systems that may not support modern data governance requirements, generally low levels of privacy awareness among staff and management, and budget constraints that limited investment in compliance infrastructure. The expected outcomes of this phase were the creation of foundational awareness about DPDP obligations and the development of preliminary compliance roadmaps. The overall readiness level during this phase is assessed as Low, reflecting the early stage of institutional engagement with the new regulatory requirements.

10.2 Phase II – Transition Phase (2025–2026): Compliance Preparation

During the transition phase, the notification of the DPDP Rules, 2025 by MeitY on 14 November 2025 provided detailed operational guidelines that shaped institutional compliance efforts and enabled UCBs to move from awareness toward structured implementation (MeitY, 2025). UCBs are expected to undertake comprehensive

privacy policy revision to align with DPDP requirements; implementation of consent management systems and processes; development of data retention frameworks that comply with both DPDP and RBI requirements; enhancement of cybersecurity infrastructure and practices; deployment of employee training programmes on data protection and privacy; development of AI governance policies addressing the specific risks of algorithmic decision-making; and assessment of vendor and third-party data processing arrangements.

AI-related activities during this phase include creating comprehensive inventories of AI applications deployed across banking operations; conducting AI risk assessments to identify potential privacy, bias, and fairness issues; establishing human oversight mechanisms for AI-driven decisions that affect customers; and implementing model monitoring systems to detect and address performance degradation or biased outcomes over time. The expected outcomes of this phase include the establishment of a structured compliance framework, improved cyber resilience, and the foundation for responsible AI adoption. The overall readiness level during this phase is assessed as Moderate, reflecting the transition from awareness to active implementation.

10.3 Phase III – Full Compliance Phase (May 2027 Onwards): Continuous Governance

From May 2027 onwards, organisations are expected to operate under complete regulatory oversight with formal enforcement of DPDP obligations. The MeitY has notified three sets of dates—14 November 2025, 14 November 2026, and 14 May 2027—for the enforcement of provisions of the DPDP Act (MeitY, 2025). During this phase, compliance becomes a continuous governance function rather than a one-time project or exercise. The major activities include conducting regular privacy audits to assess ongoing compliance; implementing continuous data governance monitoring across all systems and processes; performing AI impact assessments to evaluate the privacy and fairness implications of AI systems before and during deployment; adopting explainable AI practices that enable customers and regulators to understand how AI-driven decisions are made; maintaining continuous cybersecurity monitoring aligned with both DPDP and RBI requirements; and establishing systematic regulatory reporting mechanisms.

The expected outcomes of this phase include mature privacy governance that is embedded in organisational culture and operations, increased customer trust resulting from demonstrable data protection practices, and a sustainable digital banking ecosystem that balances innovation with privacy protection. The overall readiness level during this phase is assessed as High or Mature, reflecting the attainment of a comprehensive and sustainable data protection posture.

10.4 Comparative Analysis of DPDP Readiness

Phase	Focus Area	Readiness Level	Major Activities
Pre-DPDP (2023–2024)	Awareness	Low	Gap analysis, data mapping, awareness creation
Transition (2025–2026)	Compliance Preparation	Moderate	Policy development, training, technology upgrades
Full Compliance (May 2027 onwards)	Enforcement	High	Continuous monitoring, audits, regulatory compliance

11. Evaluation of the Role of the DPDP Act

The study evaluates the role of the Digital Personal Data Protection (DPDP) Act, 2023 in data processing and privacy management within Urban Cooperative Banks. Since UCBs process substantial amounts of customers' personal and financial data through their banking operations, effective data protection and privacy practices are essential not only for regulatory compliance but also for maintaining the trust and confidence of the communities they serve. The evaluation focuses specifically on the following eight aspects.

First, regarding data processing practices, the assessment examines whether UCBs collect, process, store, and share personal data for legitimate and specified purposes as required under the DPDP Act. Second, concerning consent and transparency, the study examines the mechanisms used by UCBs for obtaining meaningful customer consent and providing clear, accessible information regarding the collection, use, and sharing of personal data. Third, the data security dimension evaluates the technical and organisational safeguards adopted by UCBs to prevent unauthorised access, disclosure, loss, or misuse of customer data, including encryption, access controls, and network security measures. Fourth, the privacy management assessment evaluates the effectiveness of privacy policies, data retention practices, access controls, and grievance redressal mechanisms in ensuring comprehensive privacy governance.

Fifth, the employee awareness dimension determines the level of understanding and training among bank employees regarding their DPDP-related data protection responsibilities, recognising that human factors represent a critical element in any data protection framework. Sixth, the data breach management assessment evaluates the preparedness of UCBs to identify, manage, contain, and respond to personal data breaches in accordance with the timelines and procedures specified under the DPDP Rules, 2025. Seventh, the third-party data processing dimension examines the controls maintained by UCBs when customer data is shared with external service providers, technology vendors, cloud platforms, and other third parties, an area of particular concern given the increasing reliance of UCBs on outsourced IT services. Eighth, the implementation challenges dimension identifies the major technological, financial, organisational, and human-resource challenges faced by UCBs in implementing the comprehensive requirements of the DPDP Act.

12. Challenges in DPDP Compliance in the Era of AI

Urban Cooperative Banks face a constellation of interconnected challenges in achieving and sustaining DPDP compliance, particularly as they navigate the integration of AI technologies into their operations. Limited financial resources represent perhaps the most fundamental constraint, as many UCBs, particularly those in the lower regulatory tiers, operate with modest capital bases and limited surplus available for investment in data protection infrastructure, technology upgrades, and specialist personnel. This financial constraint is compounded by the dependence on legacy IT infrastructure, which may not support modern data governance requirements such as granular access controls, encryption at rest and in transit, audit logging, and real-time data flow monitoring. The cost of modernising these systems while simultaneously maintaining day-to-day banking operations represents a significant challenge for smaller UCBs.

A persistent shortage of professionals with specialised expertise in data privacy, cybersecurity, and AI governance further constrains the ability of UCBs to implement effective compliance programmes. Unlike large commercial banks that can attract and retain dedicated data protection officers, privacy engineers, and AI ethics specialists, UCBs often rely on a small number of IT staff who must manage a broad range of responsibilities.

Inadequate employee awareness about data protection obligations, privacy best practices, and the specific requirements of the DPDP Act represents an additional challenge, as even well-designed technical controls can be rendered ineffective by human error or lack of understanding. Complex regulatory requirements arising from the need to comply simultaneously with the DPDP Act, the DPDP Rules, RBI master directions on IT governance, KYC, digital lending, and IT outsourcing, as well as cooperative society regulations, create a demanding multi-regulatory compliance environment that can overwhelm the limited governance capacity of smaller institutions.

Vendor and outsourcing risks are particularly acute for UCBs that increasingly depend on third-party technology providers for core banking solutions, digital banking platforms, AI tools, and cloud services. The DPDP Act's accountability provisions make UCBs responsible for data processing carried out by their vendors, requiring robust contractual safeguards, due diligence processes, and ongoing monitoring capabilities that many UCBs currently lack. The increasing sophistication of cybersecurity threats targeting financial institutions, including ransomware, phishing, and supply chain attacks, adds urgency to the need for enhanced security measures. The Picus Blue Report 2024 found that ransomware remains a major concern as it is costly and complex to detect, with BlackByte ransomware achieving only a 17% prevention rate (Picus Security, 2024). AI-specific challenges include the difficulty of implementing data minimisation principles in AI systems that typically require large and diverse datasets for training and operation; the risk of algorithmic bias producing unfair or discriminatory outcomes, particularly in credit scoring and loan approval processes; potential data leakage through AI model outputs, adversarial attacks, or unintended information disclosure; and the fundamental difficulty of balancing the imperative for AI-driven innovation with the equally important imperative for privacy protection.

13. Strategies for Strengthening Data Privacy Governance and Responsible AI Adoption

Based on the analysis presented in the preceding sections, this study recommends a comprehensive set of strategies for strengthening data privacy governance and enabling responsible AI adoption in Urban Cooperative Banks. These strategies are designed to be practical, phased, and proportionate to the varying capacities and resources of UCBs across different regulatory tiers. UCBs should develop an integrated data governance framework that aligns DPDP requirements with existing RBI compliance obligations, creating a unified compliance architecture rather than treating data protection as a separate regulatory burden. The implementation of privacy-by-design principles in all digital and AI applications is essential, ensuring that privacy considerations are embedded into system design from the outset rather than retrofitted after deployment (Cavoukian, 2011).

UCBs should strengthen their technical and organisational safeguards, including consent management mechanisms, role-based access controls, end-to-end encryption, and comprehensive breach response procedures. Regular privacy impact assessments, cybersecurity audits, and AI risk assessments should be conducted to identify and address emerging vulnerabilities proactively. The establishment of formal AI governance frameworks, including human oversight mechanisms for automated decisions, model documentation requirements, and bias monitoring protocols, should be prioritised. These AI governance practices should be aligned with international guidance from the NIST AI Risk Management Framework (NIST, 2023), the OECD AI Principles (OECD, 2019), and the requirements of ISO/IEC 42001:2023 (International Organization for Standardization, 2023).

Capacity-building programmes for employees at all levels are critical, covering data protection responsibilities, privacy best practices, AI literacy, and incident response protocols. Customer privacy awareness initiatives should be developed to inform UCB customers about their rights under the DPDP Act and empower

them to make informed decisions about their personal data. Third-party and vendor due diligence processes should be significantly strengthened, including comprehensive data processing agreements, regular vendor audits, and clear accountability frameworks that reflect the DPDP Act's requirements. Continuous privacy and AI monitoring systems should be established to ensure ongoing compliance and enable timely detection and response to emerging risks. Finally, UCBs should actively collaborate with regulators, industry associations, and peer institutions to share best practices, develop common compliance tools and templates, and contribute to the collective advancement of data protection standards in the cooperative banking sector.

14. Scope and Limitations of the Study

This study focuses on Urban Cooperative Banks in India as grassroots banking institutions, examining their preparedness to implement the DPDP Act, 2023 and exploring the opportunities and challenges associated with AI-driven banking technologies. The scope encompasses the analysis of the DPDP Act's requirements, the RBI's regulatory framework applicable to UCBs, international standards for data protection and AI governance, and the specific challenges faced by UCBs in achieving compliance. The research is limited to information available through secondary sources, including legislative texts, regulatory publications, academic literature, and industry reports, and does not include empirical validation through primary data collection such as surveys, interviews, or case studies of individual UCBs. The findings and recommendations are therefore interpretive and should be validated through future primary research. The rapidly evolving nature of AI technologies, data protection regulations, and cybersecurity threats may also influence the continued relevance and applicability of the study's findings and recommendations.

15. Expected Outcomes of the Study

This study is expected to provide a comprehensive assessment of the readiness of Urban Cooperative Banks (UCBs) to comply with the provisions of the Digital Personal Data Protection (DPDP) Act, 2023 in the era of Artificial Intelligence. It identifies the current status of data privacy practices, evaluates organisational and technological preparedness, and examines the role of AI in customer data processing and privacy management within grassroots banking institutions. The research highlights key challenges related to DPDP compliance, AI adoption, data governance, cybersecurity, and regulatory implementation, and identifies gaps in existing privacy frameworks. Based on the findings, the study proposes practical strategies and a phased compliance framework for strengthening data privacy governance, improving AI governance, enhancing regulatory compliance, and building institutional capacity. The recommendations are expected to assist policymakers, regulators, and Urban Cooperative Banks in developing a secure, transparent, and privacy-centric banking ecosystem that promotes responsible AI adoption while safeguarding customer data and strengthening public trust in grassroots banking.

16. Recommendations

Based on the analytical findings of this study, the following recommendations are proposed for Urban Cooperative Banks to strengthen their data privacy governance and ensure responsible AI adoption in the context of the DPDP Act, 2023. UCBs should develop a comprehensive data governance framework that integrates DPDP requirements with existing RBI compliance obligations. They should conduct periodic privacy audits to assess and improve their data protection posture. Legacy banking systems should be modernised to support modern data governance requirements, including encryption, access controls, and audit logging. Cybersecurity infrastructure should be

strengthened in accordance with the RBI's tiered cybersecurity framework and the DPDP Act's security safeguard requirements.

UCBs should establish AI risk assessment mechanisms to evaluate the privacy, fairness, and security implications of AI systems before and during deployment. Comprehensive employee capacity-building programmes should be implemented to develop data protection competencies across all levels of the organisation. UCBs should appoint Data Protection Officers or designated compliance officers with clear responsibility for DPDP compliance. Continuous monitoring systems should be established for AI applications to ensure fairness, transparency, and accountability in algorithmic decision-making. Customer awareness programmes should be developed to inform customers about their privacy rights under the DPDP Act. Third-party vendor governance should be enhanced through comprehensive due diligence, data processing agreements, and regular audits. Finally, UCBs should actively collaborate with regulators and industry bodies to share best practices and contribute to the development of sector-specific data protection guidance.

17. Conclusion

The Digital Personal Data Protection (DPDP) Act, 2023 represents a significant and long-anticipated step towards strengthening data protection in India's rapidly growing digital economy. For Urban Cooperative Banks, which occupy a unique and vital position in India's financial inclusion architecture, compliance with the DPDP Act should be viewed not merely as a regulatory burden but as a strategic opportunity to improve governance standards, strengthen customer confidence, and support sustainable digital transformation. The Act's requirements for consent management, purpose limitation, data minimisation, security safeguards, and accountability provide a comprehensive framework that, if implemented effectively, can significantly enhance the data protection posture of UCBs and the broader cooperative banking sector.

AI adoption in banking provides significant opportunities for improving operational efficiency, enhancing customer experience, and enabling data-driven decision-making. However, as this study has examined, it also introduces new categories of privacy and ethical challenges that require careful governance. The risks of algorithmic bias, lack of explainability, unauthorised profiling, and data leakage through AI systems demand that UCBs integrate responsible AI practices with DPDP compliance through effective governance structures, robust cybersecurity controls, systematic employee capability development, and continuous monitoring and improvement. The international guidance provided by the OECD AI Principles (OECD, 2019), the NIST AI Risk Management Framework (NIST, 2023), and ISO/IEC 42001:2023 (International Organization for Standardization, 2023) offers valuable normative frameworks that UCBs can adapt to their specific contexts and capabilities.

The three-phase DPDP readiness framework proposed in this study—progressing from awareness and gap assessment through transition and compliance preparation to full compliance and continuous governance—provides a practical and phased roadmap for UCBs to transition from their current state to a mature privacy governance posture. By adopting proactive data protection strategies, investing in technology and human capital, and embracing a culture of privacy and ethical responsibility, Urban Cooperative Banks can continue their indispensable role as trusted grassroots financial institutions while embracing the benefits of digital innovation responsibly and sustainably.

References

- Bank of England. (2023, October 11). *Bias, fairness, and other ethical dimensions in artificial intelligence*. Bank Underground. <https://bankunderground.co.uk/2023/10/11/bias-fairness-and-other-ethical-dimensions-in-artificial-intelligence>
- Cavoukian, A. (2011). *Privacy by Design: The 7 Foundational Principles*. Information and Privacy Commissioner of Ontario, Canada. <https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples>.
- European Parliament and Council of the European Union. (2016). Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data (General Data Protection Regulation). *Official Journal of the European Union*, L 119, 1–88.
- Government of India. (2023). *The Digital Personal Data Protection Act, 2023* (Act No. 37 of 2023). Ministry of Electronics and Information Technology. [https://www.meity.gov.in/content/digital-personal-data-protection-act-2023\[reference:44\]](https://www.meity.gov.in/content/digital-personal-data-protection-act-2023[reference:44])
- International Journal of Novel Research and Development (IJNRD). (2024). Digital transformation in India's cooperative bank. *International Journal of Novel Research and Development*, 9(5). <https://www.ijnrd.org/papers/IJNRD2405601>.
- International Organization for Standardization. (2019). *ISO/IEC 27701:2019 – Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management*. ISO. <https://www.iso.org/standard/71670.html>
- International Organization for Standardization. (2023). *ISO/IEC 42001:2023 – Information technology – Artificial intelligence – Management system*. ISO. <https://www.iso.org/standard/81230.html>
- Ministry of Electronics and Information Technology (MeitY). (2025). *The Digital Personal Data Protection Rules, 2025*. Government of India. <https://www.meity.gov.in/documents/act-and-policies/digital-personal-data-protection-rules-2025>
- National Institute of Standards and Technology. (2023). *Artificial Intelligence Risk Management Framework (AI RMF 1.0)* (NIST AI 100-1). U.S. Department of Commerce. <https://www.nist.gov/itl/ai-risk-management-framework>
- OECD. (2019). *Recommendation of the Council on Artificial Intelligence* (OECD/LEGAL/0449). OECD Publishing. <https://legalinstruments.oecd.org/en/instruments/oecd-legal-0449>
- Picus Security. (2024). *Financial Services Cybersecurity: 2024 Performance in Banking, Financial Services, and Insurance (BFSI)*. Picus Security Research. <https://www.picussecurity.com/resource/blog/financial-services-cybersecurity-performance-2024>
- Press Information Bureau, Government of India. (2025, August 6). *RBI's Financial Inclusion Index rises to 67 in 2025*. <https://www.pib.gov.in/PressNoteDetails.aspx?NoteId=154980&ModuleId=3®=3&lang=2>
- Reserve Bank of India. (2016). *Master Direction – Know Your Customer (KYC) Direction, 2016* (Updated as on August 14, 2025). RBI. <https://www.rbi.org.in/commonman/english/scripts/notification.aspx?id=2607>

Reserve Bank of India. (2022). *Guidelines on Digital Lending* (RBI/2022-23/111 DOR.CRE.REC.66/21.07.001/2022-23, September 02, 2022). RBI. <https://website.rbi.org.in/web/rbi/-/notifications/guidelines-on-digital-lending-12382>

Reserve Bank of India. (2023). *Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices* (RBI/DoS/2023-24/107, November 7, 2023).
RBI. [https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=12562\[reference:54\]](https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=12562[reference:54])

Reserve Bank of India. (2025). *Reserve Bank of India (Urban Co-operative Banks – Licensing, Scheduling and Regulatory Classification) Guidelines, 2025* (RBI/DOR/2025-26/269, December 04, 2025).
RBI. https://www.rbi.org.in/scriptS/BS_ViewMasDirections.aspx?id=13203

Women's World Banking. (2024). *Algorithmic bias, financial inclusion, and gender: A primer*. Women's World Banking. https://www.womensworldbanking.org/wp-content/uploads/2024/03/Algorithmic_Bias_Primer.