This page is intentionally left blank

Adv. K Gopika & Adv. K Devika, *The DPDP Act and Kerala Bank: A Case Study Iin Data Governance and Risk Management,* 12 (1) SCHOLASTICUS 1 (2025)

THE DPDP ACT AND KERALA BANK: A CASE STUDY IN DATA GOVERNANCE AND RISK MANAGEMENT

Adv. K Gopika[*] & Adv. K Devika[†]

ABSTRACT

India's approach to data governance and privacy has undergone a major shift with the passage of the Digital Personal Data Protection Act, 2023. It aims to create a uniform framework for the public and private sectors to handle, maintain, and safeguard personal data This new regime presents significant compliance challenges for the banking industry, one of the biggest processors of sensitive financial and personal data. As a state-regulated cooperative bank, Kerala Bank offers a unique example of how regional banks adjust to their responsibilities regarding data security and cyber governance. This paper evaluates how the DPDP Act impacts Kerala Bank's data governance framework, focusing on ability to operate, customer trust, and institutional risk management. It also looks at how the Act affects governance structures, capacity building, and compliance architecture in cooperative banking systems. The study also explores how Kerala Bank can improve its cyber security, transparency, and long-term depositor trust by utilizing the DPDP Act. By demonstrating that privacy protection is not only a legal necessity but also a fundamental component of sustainable banking governance in India, this study ultimately seeks to close the gap between legal compliance and real-world implementation.

[*] Adv. K Gopika is a LL.M student at Central University of Kerala, and can be contacted at advgopikaprabha20601[at]gmail[dot]com

[†] Adv. K. Devika is a LL.M student at Central University of Kerala, and can be contacted at devikaprabha14[at]gmail[dot]com

I. INTRODUCTION

India's financial system has rapidly gone digital over the past ten years. Technology-driven services like digital payment gateways, mobile applications, online banking, and Aadhaar-based authentication systems have become more and more important to banks.[1] These developments have increased efficiency and accessibility, but they have also put financial institutions at serious risk from cyber fraud, illegal access, and data misuse.[2] In order to address these growing concerns, a comprehensive framework for protecting personal data was introduced by the Digital Personal Data Protection Act, 2023 (DPDP Act).[3] In the banking system, where sensitive personal and financial data is continuously processed, the Act places a strong emphasis on the principles of consent, purpose limitation, data minimization, and accountability.[4]

II. EVOLUTION OF DATA PROTECTION IN INDIA

India lacked a specific law protecting personal data prior to the DPDP Act. A combined set of provisions under the Information Technology Act, 2000 (IT Act) and its implementing regulations addressed data privacy concerns.[5] These clauses, however, came inadequate in addressing the contemporary issues brought about by global data sharing, financial technology innovation, and digital platforms.[6] According to Article 21 of the Constitution, privacy was acknowledged as a fundamental right in the 2017 ruling in *Puttaswamy v. Union of India*.[7] The DPDP Act was eventually passed in 2023 as a result of this historic decision, which set the groundwork for a new privacy law.[8] Despite being modified to fit India's socioeconomic circumstances, the Act complies with international standards such as the[9] EU's General Data Protection Regulation (GDPR).[10]

III. THE BANKING SECTOR AND DATA GOVERNANCE

Banks manage huge quantities of personal data, such as financial credentials, transaction histories, and biometric identifiers. According to the DPDP Act, they are therefore considered high-risk processors.[11] Numerous circulars on cybersecurity, data localization, and consumer consent in digital transactions have already been released by the Reserve Bank of India (RBI).[12] Nevertheless,

[1] Ministry of Electronics & IT, "Digital India Programme Overview" (2022).
[2] CERT-In, Annual Cybersecurity Report (2022).
[3] DPDP Act, § 3.
[4] Justice B.N. Srikrishna Committee Report on Data Protection (2018).
[5] Information Technology Act, No. 21 of 2000, § 43A.
[6] Internet Freedom Foundation, "Why India Needed a New Data Law" (2023).
[7] K.S. Puttaswamy v. Union of India (2017) 10 SCC 1.
[8] DPDP Bill, Lok Sabha Debates, Aug. 2023.
[9] EU General Data Protection Regulation, Regulation (EU) 2016/679.
[10] *Id.* § 4.
[11] RBI Circular on Cyber Security Framework in Banks (June 2, 2016).
[12] *Id.* § 7-10.

the DPDP Act adds new responsibilities like: Getting customers' express consent for data use, Ensuring fair and legal data processing, establishing procedures for data correction and grievance redress notifying the Indian Data Protection Board of data breaches. Due to limited infrastructure, technological limitations, and resource availability, these requirements present operational challenges for cooperative banks such as Kerala Bank.[13]

IV. KERALA BANK: A UNIQUE INSTITUTIONAL FRAMEWORK

In 2019, a number of Kerala district cooperative banks merged to form Kerala Bank, also referred to as the Kerala State Co-operative Bank.[14] The RBI and the Kerala State Co-operative Societies Act, 1969 both regulate its operations.[15] Compared to commercial banks, compliance is more complicated because of this dual nature. Millions of customers' personal data is handled by Kerala Bank as it grows its online presence by providing internet services, mobile banking, and Aadhaar-based financial inclusion initiatives, especially in rural and semi-urban areas.[16]Therefore, DPDP compliance mechanism implementation becomes both a legal requirement and a means of enhancing public confidence in the cooperative banking system.[17]

V. OVERVIEW OF THE DPDP ACT AND ITS RELEVANCE TO THE BANKING SECTOR

A significant legal turning point in India's continuous efforts to guarantee better protection of digital privacy and data rights was the Digital Personal Data Protection Act, 2023, also referred to as the DPDP Act. The Supreme Court's historic ruling in Justice *K.S. Puttaswamy v. Union of India (2017)*, which maintained that privacy is a fundamental right under Article 21 of the Indian Constitution, caused years of policy debate before the law was passed.[18] The government can now draft a comprehensive law that regulates the collection, processing, storage, and sharing of personal data due to the constitutional foundation established by that ruling. . The Justice B.N. Srikrishna Committee was formed by the Indian government in response to this court order, and it produced a thorough report in 2018 suggesting a contemporary data protection framework. Its fundamental principle was that people must maintain control over their personal data, even though digital innovation is essential for economic growth.[19] Enacted in 2023, the DPDP Act aims to achieve

[13] Kerala Cooperative Banking Federation Policy Note (2022).
[14] Government of Kerala, Notification on Formation of Kerala Bank, 2019.
[15] Kerala State Cooperative Societies Act, 1969, § 74A.
[16] Kerala Bank Annual Report (2023).
[17] RBI Financial Stability Report (2023).
[18] EU General Data Protection Regulation, Regulation (EU) 2016/679.
[19] Justice B.N. Srikrishna Committee Report on Data Protection (2018).

balance between advancing India's digital economy and guaranteeing that citizens' privacy is protected throughout the entire data processing process. The Act aims to protect the rights of individuals, known as "Data Principals," and to impose duties on organizations that gather and utilize data, known as "Data Fiduciaries." [20] In short, the law seeks to create a setting where individuals are aware of what happens to their data and where organizations are held responsible for ensuring its security. The DPDP Act covers all digital personal data processed in India, as well as data processed outside of India if it relates to domestically provided goods or services. This implies that even an international bank that targets Indian clients through digital means needs to abide by the rules. Any information that can be used to directly or indirectly identify an individual, such as a name, financial record, Aadhaar number, or biometric information, is considered "personal data" under the Act.[21] This definition includes almost all customer data in the banking context, including account numbers, PAN information, and online transaction histories. As a result, all Indian banks such as private, public, and cooperative are regarded as Data Fiduciaries. This legal classification is especially important for Kerala Bank, which oversees millions of accounts via its online and rural branches. Now, the bank has to make sure that all data collection and processing, whether it be for digital payments, KYC verification, or loan evaluation, is done legally and openly. According to the DPDP Act, such lawful processing is only permitted when the processing satisfies clearly defined legitimate uses or when the customer gives free, informed, and specific consent. Silence or boxes that have already been checked are insufficient; explicit and documented consent is required.[22] For customers to understand exactly what data is being collected, how it will be used, and with whom it may be shared, Kerala Bank needs to redesign its online applications, digital consent screens, and account-opening forms. The Act's principles of purpose limitation and data minimization are also crucial components. This implies that a bank can only gather personal data for a particular reason and cannot use it for other purposes. Kerala Bank is not permitted to market insurance products using a customer's Aadhaar number if it is obtained purely for KYC purposes without the customer's express consent.[23] The DPDP Act requires banks to maintain reasonable security measures like encryption, secure servers, firewalls, and two-factor authentication in addition to these substantive principles. Additionally, it mandates that any data breach be immediately reported to the affected parties as well as the recently formed Data Protection Board of India.[24] In the past, Indian banks handled cybersecurity incidents internally without disclosing them to the public, this creates a culture of transparency. The rights

[20] Digital Personal Data Protection Act, No. 22 of 2023, Gazette of India (Aug. 11, 2023) (hereinafter "DPDPA").
[21] DPDPA, § 2(t).
[22] DPDPA, § 6.
[23] DPDPA, § 7.
[24] DPDPA, § 9.

granted to customers, known as Data Principals, are equally important. They now have the right to know how their data is being processed, to request that inaccurate information be corrected or deleted, and to use grievance-redress procedures if they feel that their privacy has been infringed.[25] Therefore, Kerala Bank needs to develop easy-to-use channels for consumers to file complaints or requests for data, whether via its physical branches, mobile app, or website. Accountability is increased because the bank's internal teams must react within the allotted time frames. Additionally, the Act establishes particular obligations for Data Fiduciaries. All banks are required to provide unambiguous privacy notices, keep processing documents, and perform a Data Protection Impact Assessment when processing large amounts of sensitive data. A Data Protection Officer must be appointed by larger organizations that have been named "Significant Data Fiduciaries" in order to supervise compliance and work with the Board.[26] Kerala Bank is expected to be included in this important group due to its statewide presence and the variety of its customers, which means that it needs to put in place more stringent governance frameworks and conduct regular audits. The DPDP Act has a strict enforcement mechanism. Depending on the seriousness of the non-compliance, penalties can amount to as much as ₹250 crore; smaller violations, like failing to respond to grievances immediately, carry lesser fines.[27] Therefore, a significant data breach may have negative effects on banks' finances as well as their reputation. The Data Protection Board of India, an independent body with the authority to look into violations and issue orders, is in charge of oversight. This regulatory layer creates a dual framework where data privacy and financial stability are both monitored, supplementing the Reserve Bank of India's current supervision. The DPDP Act formally establishes cyber-security and customer confidentiality as legal rights of the customer, even though the RBI already regulates these areas through circulars and guidelines. For example, the DPDP Act now requires banks to report incidents to regulators and impacted parties, whereas the RBI's 2016 Cyber Security Framework mandated that banks have incident-response mechanisms.[28] Similarly, the Act's preference for storing Indian citizens' data within India is now in accordance with RBI's insistence on data localization. In this way, the DPDP Act and RBI regulations work in together: the former protects privacy from a rights-based standpoint, while the latter does so from a financial stability standpoint. When compared to international regulations, India's legislation is similar to Singapore's Personal Data Protection Act (PDPA) and the GDPR of the European Union in a number of ways. Both of those systems place a strong emphasis on accountability, transparency, and consent; violations

[25] DPDPA, §§ 11–14.
[26] DPDPA, § 16.
[27] DPDPA, § 33.
[28] Reserve Bank of India, Circular on Cyber Security Framework in Banks (June 2, 2016).

are punishable by severe penalties.[29] The DPDP Act, however, is adapted to the realities of India. It gives smaller organizations, like cooperative banks, the freedom to adopt compliance gradually and permits the government to gradually enact new regulations. This approach understands that Kerala Bank and other financial institutions that target to rural communities may not have the technologically advanced infrastructure of larger commercial banks. The Act presents significant obstacles for the banking industry despite its progressive nature. Many cooperative banks continue to use outdated basic banking systems that make it difficult to incorporate current privacy controls. It takes consistent work and resources to teach employees and clients about consent and data rights. Compliance-associated expenses, such as audits, legal counsel, and technological advancements, can add up. Furthermore, there is a chance of overlapping or even conflicting directives due to the involvement of several regulators, including the RBI, state cooperative departments, and now the Data Protection Board.[30] Kerala Bank must manage this complexity by establishing an independent compliance cell responsible with coordinating multiple responsibilities because it is situated between state and federal jurisdictions. The DPDP Act shows Kerala Bank in particular with both a challenge and an opportunity. Despite being a relatively new organization created in 2019 by the merger of district cooperative banks, it already manages a wide variety of data, including government welfare transfers and rural credit records. By putting the Act into effect, it will have the opportunity to update its systems, carry out a thorough data-flow audit, and strengthen its internal encryption and consent policies. In addition to preventing fines, appointing a certified Data Protection Officer and implementing frequent staff training initiatives will foster long-term trust with clients who depend more and more on online banking. Better data governance can become a differentiator rather than a regulatory burden in a collaborative setting where community relations and reputation are crucial.[31] In the end, the DPDP Act marks a major shift for the financial institutions in India. It turns privacy from a complex ethical issue into an enforceable legal right, requiring all banks, from regional cooperatives to national corporations, to treat consumer data as a valuable trust rather than just a commercial asset. To fully comply with this Act, Kerala Bank will need to make consistent investments, communicate openly, and have an organizational culture that prioritizes data protection in all aspects of banking operations. How Kerala Bank's current governance and risk-management frameworks meet these new statutory requirements and what additional changes are required to ensure full compliance will be thoroughly examined in the section that follows.

[29] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 Apr. 2016 (GDPR); Singapore Personal Data Protection Act, No. 26 of 2012.
[30] Economic Times, "Cooperative Banks Face Tech Upgrade Challenges," Mar. 2023.
[31] EU General Data Protection Regulation, Regulation (EU) 2016/679.

VI. DATA GOVERNANCE AND RISK MANAGEMENT IN KERALA BANK UNDER THE DPDP ACT

Because of its dual nature, commercial and welfare-oriented data governance is especially important because the bank regularly manages enormous amounts of financial and personal data belonging to millions of people from a wide range of socioeconomic backgrounds. Kerala Bank's operations have become more and more digitalized in recent years. Its structure now includes services like centralized core banking systems, Aadhaar-enabled payments, internet banking, and mobile banking. Through these efforts, the bank has been able to more effectively reach rural clients and provide them with access to contemporary financial resources that were previously only available in urban areas. But the scale and sensitivity of the data it handles have grown as a result of the same digital transformation. In India's cooperative banking market, Kerala Bank officially known as the Kerala State Co-operative Bank represents a distinctive model. One of the biggest state cooperative banks in the nation, it was established in 2019 when the Kerala State Co-operative Bank merged with fourteen district cooperative banks. The goal of the merger was to establish a powerful, integrated financial organization that could serve both urban and rural markets and guarantee the effective provision of financial services connected to the government.[32] Kerala Bank has been positioned since its founding as a means of carrying out state-level welfare programs and agricultural credit initiatives in addition to serving as a financial intermediary. Biometric identifiers, Aadhaar and PAN information, transaction histories, and beneficiary details from government subsidy programs are just a few of the categories of personal data that the bank gathers, keeps, and processes.[33] Since the DPDP was introduced, Kerala Bank's digital operations are subject to more stringent compliance requirements, which has changed the way that risk management and data governance need to be handled institutionally. In the banking industry, data governance refers to the general framework that establishes how information is gathered, saved, distributed, and safeguarded inside the company. It includes the systems that guarantee security and moral treatment, as well as data ownership and responsibility. Prior to the DPDP Act, the Information Technology Act of 2000, the Kerala State Co-operative Societies Act of 1969, and the Reserve Bank of India's cybersecurity guidelines served as the main guiding principles for Kerala Bank's data governance procedures.[34] These frameworks did not offer a comprehensive road map for rights-based data protection, but they did require the confidentiality of customer information. The implementation of the DPDP Act broadens the scope of governance beyond technical compliance

[32] Government of Kerala, Notification on Formation of Kerala Bank (2019).
[33] EU General Data Protection Regulation, Regulation (EU) 2016/679.
[34] Information Technology Act, No. 21 of 2000; *See also* Kerala State Co-operative Societies Act, 1969.

to include a rights-driven model that acknowledges the customer, also known as the data principal, as the legitimate owner of their data. Kerala Bank has already begun strengthening its internal governance frameworks. Firewalls, data encryption, intrusion detection systems, and recurring vulnerability assessments are all under the control of its information technology department. These procedures are in line with the Reserve Bank of India's 2016 Cyber Security Framework, which mandates that all banks create information security policies that have been approved by the board and carry out periodic system audits.[35] The DPDP Act, however, now requires that these measures be combined with a transparent privacy management framework. A Data Protection Officer (DPO) who reports directly to senior management and serves as an intermediary with the Data Protection Board of India must be appointed, and a formal Data Protection Cell must be established.[36] In addition to overseeing security, the DPO's responsibilities also include managing consent systems, ensuring lawful processing, and overseeing data breach responses. Obtaining customers' explicit and informed consent before processing their personal data is one of the most significant changes brought about by the DPDP Act for Kerala Bank. In reality, this means that a concise and clear privacy notice outlining the types of data being collected and their intended use must be displayed on all digital interfaces, including online account forms and mobile banking applications. Legal jargon must be avoided in favour of plain language in these notices. Consumers should be able to refuse specific uses of their data, and their choice shouldn't interfere with the delivery of essential banking services.[37] Customers must also be able to revoke their consent at any moment, according to the Act. As a result, Kerala Bank will need to update its technological infrastructure to support audit trails, withdrawal procedures, and real-time consent tracking. All banks, including cooperative ones, are also required by the DPDP Act to restrict data processing to the purposes specified at the time of collection. Data gathered for KYC verification cannot subsequently be used for unrelated purposes, like targeted advertising or profit-sharing with third parties, thanks to the principle of purpose limitation.[38] Being a state cooperative, Kerala Bank needs to exercise extra caution in this area because it frequently works with government agencies to distribute welfare benefits, pensions, and agricultural subsidies. Even for administrative reasons, any sharing of beneficiary data with outside vendors needs to be supported by legal justifications or explicit consent. Preventing and responding to data breaches is an essential component of risk management under the DPDP Act. Data fiduciaries are clearly required by law to put in place "reasonable security safeguards" to stop unauthorized access, alteration, or disclosure of personal

[35] Reserve Bank of India, Circular on Cyber Security Framework in Banks (June 2, 2016).
[36] DPDPA, § 10.
[37] DPDPA, § 6.
[38] DPDPA, § 7.

information. The organization is required to immediately inform the affected individuals and the Data Protection Board of India in the event of a breach.[39] While adding a new level of legal accountability, this requirement supports Kerala Bank's continuous efforts to improve its cybersecurity procedures. In addition to facing severe penalties, the bank may lose the public's trust if the breach report is incomplete or delayed. Kerala Bank must set up an incident response framework with early detection systems, handling protocols, and customer communication methods in order to comply efficiently. Kerala Bank must implement procedural changes in response to the DPDP Act's emphasis on Data Principal Rights, including the rights to rectification, erasure, and grievance redress. Consumers must be able to request the deletion of data that is no longer required for service delivery or correct errors in their account information. Long-term clients whose past records might still be in older systems should pay special attention to this. The information technology team at Kerala Bank will have to create interfaces that allow authorized staff carry out these requests while keeping audit logs for accountability.[40] In order to respond quickly to privacy-related complaints, the bank must also establish an open grievance procedure that is available both online and offline. Data ethics and privacy must now be formally included in enterprise risk frameworks for risk management, which is a key component of Kerala Bank's operational strategy. Credit, liquidity, and market risks are the main areas of concentration for banks' conventional risk management framework. A new category data protection risk is created by the DPDP Act, necessitating specific evaluation and mitigation techniques. This involves finding possible privacy risk sources, like outside vendors, outdated technologies, or inappropriate access control, and resolving them with employee training, technology advancements, and contractual protections.[41] To assess its compliance status and vulnerability exposure, the bank must perform risk assessments on a regular basis. Programs for employee awareness and training are yet another essential component of compliance. Kerala Bank needs to fund frequent workshops and e-learning initiatives because cooperative banks frequently employ a broad and diverse workforce, including employees in rural branches who might not be familiar with complex data privacy regulations. The fundamentals of the DPDP Act, secure data handling techniques, and protocols for handling consumer privacy inquiries should all be covered in these sessions.[42] The success of these initiatives will depend on how well the bank can integrate privacy into its institutional culture as opposed to viewing it as a legal necessity. Managing third-party risks presents Kerala Bank with yet another difficulty. For cloud storage, payment gateway services, and

[39] DPDPA, § 9.
[40] DPDPA, §§ 11–14.
[41] Reserve Bank of India, Risk Management Guidelines for Co-operative Banks (2021).
[42] Data Security Council of India, "Privacy Best Practices for BFSI Sector" (2022).

IT maintenance, the bank collaborates with a large number of outside service providers. According to the DPDP Act, the bank is still solely liable for any data that these vendors process on its behalf. As a result, comprehensive data protection provisions that outline security guidelines, breach notification deadlines, and the extent of liability must now be included in contractual agreements.[43] Due to this change, all vendor contracts must be reviewed and brought into compliance with the Act's requirements by the bank's legal and procurement departments. Notwithstanding these obstacles, Kerala Bank has a great chance to improve its standing and competitiveness through the DPDP Act's implementation. The bank may increase customer confidence by implementing clear privacy policies, especially for rural depositors who might still be uncertain of online transactions. Partnerships with fintech firms and government organizations looking for safe banking platforms for digital payments and the distribution of subsidies can also be attracted by a robust data protection regime. Additionally, better governance lessens the possibility of data misuse and internal fraud, two problems that have historically impacted cooperative banking institutions.[44] In a larger sense, other Indian cooperative banks can use Kerala Bank's strategy for DPDP compliance as a model. The bank can establish standards for responsible data governance by proving that privacy protection and operational effectiveness can coexist. Kerala Bank can guarantee long-term sustainability in the changing digital economy by implementing privacy by design, which involves building systems and procedures with privacy considerations at their core.[45] Therefore, the DPDP Act serves as a framework for regulations as well as a driving force behind institutional modernization, guiding Kerala Bank toward a time when trust and data security will be the cornerstones of cooperative banking.

VII. EMPIRICAL STUDY ON THE AWARENESS AND PREPAREDNESS OF KERALA BANK TOWARDS THE DPDP ACT.

With the enactment of the DPDP Act, India's financial system has entered a new era of data-centric governance and accountability. While legal and policy analyses provide the theoretical foundation for understanding the law, an empirical inquiry offers insights into how institutions and individuals perceive and implement it. A field-based empirical study that examines Kerala Bank's awareness, preparedness, and implementation challenges of the DPDP Act is presented in this chapter. In order to assess the level of comprehension and readiness within the organization, the study integrates the viewpoints of both employees and customers.[46] This study's objective was

[43] DPDPA, § 10.
[44] Economic Times, "Kerala Bank Expands Digital Services Amid Compliance Challenges" (Mar. 2024).
[45] NITI Aayog, "Digital Banking Vision Document" (2021).
[46] Ministry of Electronics & IT, "Digital India Programme Overview" (2022).

to determine the stakeholders' present level of understanding of data protection principles, to assess the institutional mechanisms put in place for compliance, and to identify areas in need of implementation or policy changes. The study specifically aimed to respond to three important questions:

1. To what extent do Kerala Bank staff members and clients understand the DPDP Act and its consequences?
2. What steps has Kerala Bank taken to get ready for compliance?
3. What obstacles do you think the Act's implementation within the cooperative banking structure will present?[47]

The study's methodology was a descriptive survey. Between March and June 2024, information was gathered from Kerala Bank's four regional clusters: Thrissur, Ernakulam, Kozhikode, and Thiruvananthapuram. There were 120 responders in all, 60 of whom were customers and 60 of whom were employees. Branch managers, IT officers, and customer service representatives were among the cadres from which employees were chosen. To guarantee diversity, customers were selected at random from both urban and rural branches. Twenty-five questions from a structured questionnaire covering concerns about risk, privacy attitudes, data handling behaviour, and awareness levels were used. To obtain qualitative information, five in-depth interviews with senior managers were also carried out.[48] The results showed that bank workers had a moderate level of awareness regarding the DPDP Act. Although about 70% of respondents said they had heard of the Act, only 38% were able to correctly describe its main goals or provisions. Because of the technical nature of their jobs, awareness was much higher among IT employees and compliance officers (about 85%). However, frontline staff members like cashiers and clerks showed a lack of knowledge regarding the Act's specific requirements, like consent management and reporting data breaches.[49] It was discovered that customer awareness was much lower. Less than 15% of consumers were aware of their rights as data principals, and only 28% of consumers were aware that India had a data protection law. Instead of the legal right to control their personal data, many consumers equate privacy primarily with protection from online fraud or phishing. Customers in rural areas were particularly frightened by consent procedures and frequently confused them with standard account opening signature requirements.[50] Employees who were questioned about data handling practices stated that following the announcement of the DPDP Act, Kerala Bank had begun implementing new protocols. For example, 82 percent of workers reported that access to

[47] *Id.*
[48] Kerala Bank Internal Memorandum, "Compliance and Digital Awareness Survey" (2024).
[49] RBI, "Circular on Cybersecurity Framework and Training for Banks" (2023).
[50] Kerala State IT Mission, "Public Awareness on Digital Rights in Kerala" (2024).

customer data is now routinely tracked and recorded. Since late 2023, the bank has held at least one internal data security training session, according to about 67% of respondents. However, a number of participants reported that these training sessions were short and mostly theoretical, with no scenario-based exercises or real-world examples.[51] According to the study, Kerala Bank had already set up a "Data Protection Committee" within its IT division, which is in charge of overseeing policies and coordinating compliance, proving institutional preparedness. About 60% of workers knew this committee existed, but only 25% could name its duties. According to senior officials surveyed, the committee's work was still in its infancy and primarily focused on creating grievance redressal procedures and internal policy drafts. At the time of the study, the appointment of a DPO was being considered.[52] Customers had differing opinions about data security. Due to their trust in Kerala Bank's collaborative history, about 55% of consumers said they were confident the bank protected their personal information. Nonetheless, 30% of respondents said they had received fraudulent calls or messages related to their accounts, indicating ongoing communication problems. Only 18% of respondents said they had ever received information from the bank about how their personal information is used, suggesting that the disclosure procedures are opaque.[53] Additionally, the study looked at mental differences according to demographic variables. Customers between the ages of 18 and 35 were more likely to use digital channels like Kerala Bank's mobile application and showed a greater awareness of their right to privacy. Older consumers expressed problems with data sharing and preferred in-person transactions, particularly those in rural areas. Newer hires demonstrated greater digital literacy and awareness of cybersecurity protocols, whereas employees with over ten years of experience tended to rely on traditional manual record-keeping.[54] Employees viewed the DPDP Act as both a regulatory necessity and an operational burden, according to one of the main conclusions drawn from the qualitative interviews. Despite their understanding of the importance of data protection, many branch managers claimed that compliance would take a significant amount of time, money, and staff. They were worried that small branches with few employees might find it difficult to comply with the Act's reporting and documentation requirements. Additionally, some pointed out that cooperative banks, as opposed to commercial banks, are subject to stricter financial regulations and would require assistance from the state or RBI in order to upgrade their IT systems. [55]Kerala Bank's acceptance for the DPDP Act was found to have a number of practical challenges. These included uneven data retention policies across branches, a lack of thorough privacy audits, and a

[51] Data Security Council of India, "Report on Privacy Training Effectiveness" (2023).
[52] Kerala Bank Annual Report 2023–24, Kerala State Co-operative Bank Ltd.
[53] *Id.*
[54] NABARD, "Digital Behavior and Financial Literacy in Rural India" (2023).
[55] Interview with Senior Branch Manager, Kerala Bank, Thrissur Region (June, 2024).

lack of encryption for legacy data. Furthermore, even though most employees understood the value of confidentiality, they had not been given written instructions outlining what the new law considered to be lawful processing. One significant compliance gap was the absence of comprehensive procedural manuals and standardized digital consent forms.[56] There was a strong institutional willingness to improve in spite of these obstacles. Nearly 90% of the employees who responded agreed that the bank's reputation and customer trust depend on data protection. Numerous people also indicated that they would like to participate in additional privacy compliance training courses. Organizational commitment is demonstrated by the management's choice to include DPDP compliance in the 2024–2025 strategic plan. If these efforts continue, Kerala Bank may become a leader in India's reform of cooperative banking.[57] The empirical study also showed that customers' digital literacy will be crucial to the Act's effective execution. Customers may unintentionally give or refuse consent for crucial operations if they don't fully understand. Promotion initiatives from Kerala Bank, like Malayalam pamphlets and community awareness campaigns, may be able to close this knowledge gap. Such initiatives, though, need to go beyond token campaigns and incorporate regular, engaging sessions that clarify the ideas of consent, data sharing, and grievance redress. [58] According to the study's analysis of the data, Kerala Bank has made transitional rather than complete progress toward DPDP compliance. Although the bank has made some admirable first moves, like creating committees and digitizing documents, it still needs to establish an advanced data governance culture. In addition to technology, this calls for a shift in behaviour. Instead of just being required by law, privacy needs to become a fundamental value in the cooperative banking ecosystem.[59] To sum up, the empirical data confirms that Kerala Bank is at a pivotal moment. The bank is in a good position to guide Kerala's cooperative sector into the age of responsible data management because of its low customer literacy, moderate employee awareness, and developing institutional frameworks. Regulators and policymakers must, however, back these initiatives with funding, educational materials, and ongoing involvement. In the end, how well organizations like Kerala Bank apply the law through effective learning, investment, and innovation will determine how well the DPDP Act works in the cooperative banking industry.[60]

[56] MeitY, "DPDP Act: Compliance Challenges for Cooperative Banks" (2024).
[57] Kerala Bank Strategic Plan 2024–25, Board Resolution (Jan., 2024).
[58] Government of Kerala, "Digital Literacy and Privacy Protection Campaign" (2024).
[59] NAFSCOB, "Cooperative Banking Digitization and Data Governance" (2023).
[60] Kerala Bank Internal Memorandum, "Compliance and Digital Awareness Survey" (2024).

VIII. POLICY IMPLICATIONS, RECOMMENDATIONS, AND WAY FORWARD FOR KERALA BANK UNDER THE DPDP ACT

The entire banking industry in India will be significantly impacted by the DPDP Act, 2023, particularly cooperative institutions like Kerala Bank. The Act fundamentally changes how data is viewed, handled, and valued rather than just adding another compliance requirement. Essentially, banks now act as "data fiduciaries," with ethical and legal obligations to protect personal data, which is now acknowledged as a type of property that belongs to the customer, or "data principal." [61] The necessity to change systems and culture makes this new paradigm both a challenge and an opportunity for Kerala Bank, which can use it to strengthen its reputation and position as a leader in the cooperative industry. The DPDP Act compels cooperative banks to reevaluate governance priorities from a policy perspective. Cooperative banking policy in India has historically prioritized community development, agricultural lending, and financial inclusion. A completely new dimension is brought about by data protection: digital inclusion with privacy assurance. Therefore, it is imperative that state and federal policymakers make sure cooperative banks like Kerala Bank are not left behind as the country moves toward digital ecosystems that respect privacy. To meet regulatory requirements and offer focused assistance, the Reserve Bank of India (RBI), the Ministry of Electronics and Information Technology (MeitY), and state cooperative departments will need to work together in together.[62] The first significant policy implication is that cooperative banks should standardize their privacy frameworks. Cooperative institutions today differ greatly in terms of their governance structures and level of technological maturity. As the biggest cooperative bank in the state, Kerala Bank has the opportunity to set the standard by implementing a privacy framework that other primary and district societies can follow. The National Federation of State Cooperative Banks (NAFSCOB) and the RBI could publish comprehensive sector-specific guidelines outlining how cooperative institutions are affected by the DPDP Act's provisions.[63] This would guarantee consistent compliance standards across the country and avoid regulatory ambiguity. Financial support for compliance preparation is another important policy issue. The DPDP Act requires significant investments in audits, training, and infrastructure. Due to their non-profit status, cooperative banks frequently rely on member capital and government support for these improvements. In order to improve digital security in cooperative banks, the Kerala government, NABARD, and RBI may implement special credit lines or grants. In addition to helping Kerala Bank modernize, this funding would encourage fair compliance among smaller

[61] Ministry of Electronics & IT, "Digital India Programme Overview" (2022).
[62] Reserve Bank of India, "Master Direction on Information Technology Governance, Risk, Controls, and Assurance Practices" (2023).
[63] National Federation of State Cooperative Banks (NAFSCOB), "Policy Paper on Cooperative Banking Digitization" (2022).

rural institutions.[64] In order to combine privacy protection with digital financial literacy, Kerala Bank must also collaborate closely with legislators. Many consumers still don't fully understand digital consent, data sharing, or privacy rights, especially in rural Kerala. Citizens can learn about their rights under the DPDP Act through public awareness campaigns that are organized in collaboration with the bank, the state IT mission, and local cooperative societies.[65] These initiatives can incorporate privacy into the financial literacy narrative through digital campaigns, community radio, and vernacular media. In addition to lessening the burden on the bank's grievance procedures, this bottom-up strategy will encourage customers to use data responsibly. Establishing a Privacy Governance Board within Kerala Bank's organizational framework is one of the most important suggestions. This group would be in charge of developing policies, conducting compliance audits, and reviewing privacy practices on a regular basis. It would be chaired by a senior management member and comprise the Data Protection Officer, IT chief, and legal counsel.[66] The creation of such a board would guarantee responsibility at the highest level and establish a distinct chain of command for matters connected with data protection. Additionally, Kerala Bank needs to implement privacy assurance certification procedures. The central government can establish certification requirements for organizations that comply with the DPDP Act. Kerala Bank can demonstrate its dedication to security and transparency by aggressively pursuing certification from reputable data protection auditors.[67] The bank's reputation would improve and customer trust would be reinforced by these certifications, especially in government and cooperative circles. Kerala Bank can gain a lot from implementing Privacy-Enhancing Technologies (PETs) from a technological perspective. These consist of tools like secure multiparty computation, data masking, tokenization, and differential privacy. Even during lawful processing operations, integrating such technologies into core banking systems can help reduce the exposure of sensitive personal data.[68] PETs can be introduced gradually, starting with essential features like subsidy distribution and KYC verification before expanding to analytics and reporting features. Kerala Bank needs to create a centralized data repository with stringent access controls in order to further enhance operational readiness. Data is currently spread throughout branches and departments. Better monitoring and enforcement of privacy regulations would be possible with a centralized system that includes role-based access, end-to-end encryption, and activity logging. Kerala Bank should also make an investment in anomaly detection systems powered by artificial intelligence, which immediately recognize questionable data access patterns and stop

[64] NABARD, "Financial Inclusion and Digitalization Report" (2023).
[65] Kerala State IT Mission, "Digital Literacy Campaigns for Rural Kerala" (2024).
[66] Data Security Council of India, "Model Data Protection Governance Framework for BFSI Sector" (2023).
[67] DPDPA, § 16.
[68] Ministry of Electronics & IT, "Guidelines on Privacy-Enhancing Technologies" (2024).

possible breaches.[69] Kerala Bank ought to implement regular third-party privacy audits in order to address legal and administrative issues. Independent experts would carry out these audits on an annual or semi-annual basis to assess DPDP Act compliance and spot new hazards.[70] Transparency and proactive risk mitigation are ensured by reporting audit findings to the board and regulators. For implementation to be successful, employee engagement is still essential. A privacy-first culture must be established by Kerala Bank via internal awareness campaigns, ethical standards, and constant communication. Employees and managers should be encouraged to voice privacy concerns without worrying about consequences. This accountability culture would be strengthened even more by establishing whistleblower protections for violations involving data.[71] The Kerala cooperative department can help at the state level by creating a state-wide data protection charter that all cooperative societies that handle personal data must abide by. Based on the DPDP Act's principles, this charter might specify best practices for handling grievances, responding to breaches, and lawful processing. This charter can be drafted using case studies and experiences from Kerala Bank.[72] Another recommendation for the future is that Kerala Bank participate in cross-sector collaboration. For the DPDP Act to be implemented successfully, banks, fintech companies, government organizations, and academic institutions must work together. Kerala Bank might collaborate with the Indian Institute of Information Technology and Management–Kerala or the Kerala Blockchain Academy to create fintech solutions that prioritize privacy. In addition to assisting with compliance, these collaborations would establish the bank as an expert in cooperative innovation.[73] Kerala Bank's way forward combines modernization of technology, customer empowerment, and regulatory compliance. Kerala Bank can improve its market position by considering data protection as a competitive advantage rather than a burden. Long-term sustainability will be facilitated by implementing privacy by design in all new digital initiatives, upholding transparency in data practices, and establishing public trust. In a larger sense, Kerala Bank's initiative may serve as a model for other Indian cooperative banks. The success of the DPDP Act ultimately rests on public confidence and institutional preparedness. The ability of Kerala Bank, the state's largest cooperative, to put strong data governance procedures in place will have an impact on how other rural bank's view and adopt privacy reforms.[74] Kerala Bank needs to prepare for future regulatory developments. India's developing data protection framework is just getting started with the DPDP Act. There likely will be complementary regulations related to

[69] RBI, "Cyber Security Framework for Banks" (2016).
[70] DPDPA, § 14.
[71] Kerala Bank Internal Memorandum, "Compliance and Digital Awareness Survey" (2024).
[72] Government of Kerala, Department of Cooperation, "Draft Cooperative Data Protection Charter" (2024).
[73] Kerala Blockchain Academy, "Collaborations with Financial Institutions on Privacy-Centric Technologies" (2023).
[74] EU General Data Protection Regulation, Regulation (EU) 2016/679.

cybersecurity, artificial intelligence, and non-personal data governance. Kerala Bank will be able to stay flexible and compliant in a changing policy environment by preparing for these future regulations now and incorporating adaptable compliance mechanisms.[75] The establishment of a privacy-resilient cooperative ecosystem in Kerala ought to be the ultimate goal. This would imply that all cooperative societies adhere to uniform data protection standards, including credit unions and agricultural banks. Kerala Bank is in a good position to serve as the nodal organization for supporting and guiding smaller cooperatives in this transition because of its wide network and digital presence.[76] Lastly, Kerala Bank has the chance to rethink its social mission thanks to the DPDP Act. The bank is upholding the cooperative principle of mutual trust and respect by protecting customer data, in addition to fulfilling its legal obligations. The cooperative values of accountability and transparency are closely related to the Indian Constitution's recognition of the right to privacy. Thus, putting strong privacy policies into place supports Kerala Bank's fundamental value of providing honest service to the public.[77] To sum up, the DPDP Act brings in a new era of Indian banking. The road to compliance for Kerala Bank will require both work and creativity. However, by making privacy a fundamental institutional value and integrating it with technology advancements, Kerala Bank can serve as a model for how cooperative banks may survive in the digital era while preserving the rights and dignity of each and every consumer.[78]

IX. CONCLUSION AND FINAL REFLECTIONS ON KERALA BANK'S ROLE IN INDIA'S DATA PROTECTION LANDSCAPE

An important turning point in India's legal and economic history has been marked by the passage of the DPDP Act, 2023. It changes the nation's perspective on digital privacy, personal data, and the role of institutions in the digital economy. The Act represents a significant shift for the Indian banking industry, particularly for cooperative banks like Kerala Bank, from traditional record-keeping to data-driven governance based on trust and accountability.[79] The DPDP Act is a social contract that makes privacy a fundamental component of democracy and responsible economic growth. It is more than just a law. The experience of Kerala Bank offers important insight into how big cooperative organizations can continue their inclusive development mission while addressing the difficulties posed by new data regulations. Kerala Bank holds a special place in the Indian financial system as a state-wide cooperative bank that provides services to millions of account holders from rural and semi-urban areas. It is a prime example of how traditional

[75] MeitY, "Public Consultation on Non-Personal Data Governance Framework" (2024).
[76] Kerala Bank Strategic Plan 2024–25, Board Resolution (Jan., 2024).
[77] EU General Data Protection Regulation, Regulation (EU) 2016/679.
[78] Kerala State IT Mission, "Public Awareness on Digital Rights in Kerala" (2024).
[79] Ministry of Electronics & IT, "Digital India Programme Overview" (2022).

institutions adjust to the challenges of modern data governance because of its dual responsibilities to maintain the cooperative culture and adhere to contemporary regulatory frameworks.[80] For Kerala Bank, the DPDP Act is important because it has the potential to increase customer trust and institutional resilience. The Act guarantees that banks handle consumer data in an ethical and legal manner by enforcing principles like consent-based data processing, purpose limitation, and data minimization. Customers feel confident that their personal information won't be exposed or misused, especially those with low levels of digital literacy. Compliance gives the bank legal security, a competitive advantage, and a positive reputation.[81] However, merely following the law won't guarantee compliance with the DPDP Act. It calls for a change in the organization's culture. From how employees handle KYC documents to how data is stored on servers, Kerala Bank needs to incorporate privacy protection into all aspects of its daily operations. In order to integrate privacy into the institutional DNA, this calls for ongoing training, awareness campaigns, and leadership dedication. Compliance runs the risk of becoming a simple checkbox exercise in the absence of such internalization.[82] In this regard, Kerala Bank's cooperative structure has advantages and disadvantages. On the one hand, greater local accountability and responsiveness are made possible by its decentralized and community-driven nature. However, it makes it more difficult to apply policies consistently across several branches and related societies. Kerala Bank must thus strike a balance between local autonomy and central oversight to guarantee that data protection laws are implemented uniformly without undermining the cooperative banking model's spirit of participation.[83] The opportunity for digital modernization is one of the DPDP Act's long-term advantages for Kerala Bank. Outdated IT systems and disconnected data management procedures have historically been problems for many Indian cooperative institutions. The Act, by mandating secure data storage, encryption, and accountability mechanisms, indirectly pushes banks toward technological advancement. Kerala Bank can take advantage of this momentum to modernize its infrastructure, make data analytics investments, and implement more intelligent, effective, and privacy-compliant CRM systems.[84] However, this modernization process needs to be inclusive. People from rural or economically disadvantaged backgrounds make up a sizable portion of Kerala Bank's clientele, and they might not be aware of their rights to privacy or digital consent procedures. Kerala Bank must thus make sure that digital transformation doesn't result in digital exclusion. In order to make sure that every client is aware of their rights and obligations in the digital age, the bank should integrate financial literacy and privacy awareness campaigns into

[80] Justice B.N. Srikrishna Committee Report on Data Protection (2018).
[81] RBI, "Master Direction on IT Governance and Cybersecurity Framework for Banks" (2023).
[82] Data Security Council of India, "Embedding Privacy Culture in Financial Institutions" (2024).
[83] MeitY, "Public Consultation on Non-Personal Data Governance Framework" (2024).
[84] NABARD, "Digital Infrastructure and Rural Banking Report" (2023).

its outreach initiatives.[85] The Reserve Bank of India and the Kerala government must maintain their support for cooperative banks at the policy level by providing them with funding, clear guidelines, and capacity-building initiatives. Without systemic support, smaller institutions may find it difficult to keep up with the ongoing investments needed to comply with the DPDP Act. With its size and resources, Kerala Bank can serve as a "training hub" or "compliance mentor" for other cooperative societies in the state, sharing data protection best practices and resources.[86] The future of cooperative governance in India is where Kerala Bank's adaptation has wider implications. The cooperative principle of transparency is perfectly aligned with the DPDP Act's demands for evidence-based accountability, which redefines governance. Kerala Bank will redefine what it means to be a cooperative institution in the digital age if it can effectively show that social banking and privacy protection can coexist. Additionally, the case of Kerala Bank shows that data protection is a foundation for sustainable growth, not a barrier to innovation. Kerala Bank can enhance service quality and security by implementing technologies such as blockchain, data anonymization, and AI-based fraud detection while staying within the parameters of the DPDP Act. By taking this approach, the bank would be able to turn compliance into a competitive advantage and draw in collaborations with fintech companies and government initiatives that respect ethical data practices.[87] Legally speaking, the DPDP Act also improves Kerala Bank's standing with authorities and clients. A transparent culture that is consistent with cooperative ethics is introduced by the Act's provisions on consent management, data principal rights, and grievance redressal. Kerala Bank can lower the risk of litigation and improve its reputation by establishing effective internal grievance procedures and keeping lines of communication open.[88] The ability of Kerala Bank to impact policy innovation at the state level is another aspect that merits attention. From e-literacy initiatives to decentralized planning, Kerala has long been at the forefront of social and digital governance reforms. The state now has a new way to test cooperative-led data governance models thanks to the DPDP Act. Kerala Bank and the state government can work together to create a "Kerala Data Protection Charter," which would include useful guidelines for all public institutions and cooperative societies to follow when handling data.[89] Over time, the way trust is built in digital banking may be redefined by Kerala Bank's implementation of the DPDP Act. In the era of data, trust the cornerstone of all financial relationships is changing. Consumers now trust banks with their identities, transactions, and digital footprints in addition to their money. Kerala Bank can establish itself as a model cooperative

[85] Kerala State IT Mission, "Financial and Digital Literacy Initiatives in Kerala" (2024).
[86] RBI, "Regulatory Framework for Cooperative Banks under DPDP Act" (2024).
[87] EU General Data Protection Regulation, Regulation (EU) 2016/679.
[88] Kerala Bank Internal Memorandum, "Compliance and Digital Awareness Survey" 2024.
[89] DPDPA, § 13.

organization that combines technology, law, and community service by protecting these with the highest ethical standards.[90] Kerala Bank and comparable organizations, however, need to be on the lookout for new issues like algorithmic bias, identity theft, and cybersecurity threats. Although the DPDP Act offers a fundamental legal framework, future threats will necessitate flexible approaches. Maintaining long-term compliance and flexibility will require regular policy reviews, staff retraining, and cooperation with cybersecurity organizations.[91] In the end, the DPDP Act teaches that data protection is a shared responsibility between citizens, banks, and the government. The proactive strategy of Kerala Bank can act as a link between the goals of policy and its actual application. It can demonstrate how cooperative banks, which were formerly thought to be conventional and slow to change, can emerge as leaders in moral innovation and privacy protection.[92] Data will become more and more of a form of capital as India's digital economy grows. Institutions that properly handle it will gain the public's long-term trust in addition to adhering to the law. A more secure and inclusive financial system can be achieved by balancing progress and privacy, as evidenced by Kerala Bank's dedication to aligning its cooperative principles with data ethics.[93] To sum up, the DPDP Act is a revolutionary step toward ensuring the safety, equity, and transparency of India's digital future. The history of Kerala Bank under this law is representative of the cooperative sector in India as a whole, which is based on social values but is flexible enough to accommodate contemporary governance. Kerala Bank's data protection plan has the potential to become a national standard if it is executed well, demonstrating how established organizations can prosper in the face of rapid technological and legal change. The rewards public trust, digital credibility, and long-term sustainability will make the journey ahead worthwhile, even though it will require investment, education, and institutional courage.

[90] Government of Kerala, "Proposal for Kerala Data Protection Charter" (2024).
[91] NAFSCOB, "Cooperative Banking Digitization and Data Governance" (2023).
[92] World Bank, "Data as Capital: Ethical Financial Data Management" (2022).
[93] Kerala Bank Internal Memorandum, "Compliance and Digital Awareness Survey" (2024).