Anshita Rani, *Banking on Data, Betting on Trust: The Privacy Reckoning of India's Financial Sector*, 12 (1) SCHOLASTICUS 1 (2025)

BANKING ON DATA, BETTING ON TRUST: THE PRIVACY RECKONING OF INDIA'S FINANCIAL SECTOR

Anshita Rani[*]

ABSTRACT

The Digital Personal Data Protection Act, 2023 (DPDPA) and the Digital Personal Data Protection Rules,2025 (DPDP Rules, 2025) mark a significant shift in India's approach to data governance, with major implications for the banking sector. From fragmented cybersecurity measures to a comprehensive rights-based regime, as banks increasingly rely on digital platforms and data analytics for credit assessment, risk management, and customer engagement, the processing of personal financial information has expanded substantially. This paper evaluates how the DPDP framework restructures the legal responsibilities of banks as Data Fiduciaries. Building on constitutional 'privacy' recognition in KS Puttaswamy v. Union of India judgement, it analyses the evolution of India's earlier cybersecurity-focused regime toward a rights-based model that emphasises consent, purpose limitation, data minimisation, and accountability. The study further examines the operational impact on banking systems, such as consent management, legacy upgrades, Consent Managers, regulatory coordination challenges between the Data Protection Board and the Reserve Bank of India, and the tension between privacy obligations and financial compliance requirements like Know Your Customer (KYC) and Anti-Money Laundering (AML) retention. The paper argues that while the framework imposes compliance costs, it strengthens consumer trust and establishes a more stable foundation for digital banking governance in India.

[*] Anshita Rani is a fourth-year student at National Law University, Jodhpur, and can be contacted at anshita2022[at]nlujodhpur[dot]ac[dot]in

I. INTRODUCTION

A. "Data is the new oil"

Digital technology has transformed India's banking sector from traditional branch-based interactions to seamless digital platforms like internet banking, mobile apps, and UPI.[1] This digital transformation enables efficient, effective instant transactions, personalised services, and data-driven insights for credit scoring, fraud detection, and customer engagement.[2] However, this rapid digital necessities the collection and processing of sensitive personal data, including transaction histories, device fingerprints, and financial profits. This makes personal data a core asset for competitive advantage.

Banks now leverage this data through advanced algorithms for predictive analytics and risk management, but it might open the avenues for personal identifying information being highly vulnerable to misuse, leading to identity theft, fraud, and privacy breaches. Amid rising cyber threats, the RBI issued a comprehensive Cyber Security Framework for Banks (2016)[3] to bolster bank security posture and limit customer liability. Key requirements include a dedicated cybersecurity policy, continuous surveillance, customer data protection, incident reporting to RBI, and stakeholder cybersecurity training.[4]

Pre-2023, India's framework remained fragmented, relying on RBI's cybersecurity guidelines, which created compliance silos for banks navigating data privacy amid evolving cyber risks.[5] The Digital Personal Data Protection Act, 2023 (DPDPA)[6] and Digital Personal Data Protection Rules, 2025 (DPDP Rules)[7] introduce India's first comprehensive, rights-based regime. Positioning individuals as "data principals", it mandates that data fiduciaries, particularly banks, uphold informed consent, purpose limitation, data minimisation, and rights to access, correction, and erasure.

This citizen -centric approach balances data an economic resource against its potential as a threat vector, fostering trust in digital banking. However, as KPMG's analysis highlights, the DPDPA's mandates on data minimisation and consent directly impact core banking operations like digital onboarding and fraud detection, requiring banks to redesign processes to ensure explicit,

[1] Reserve Bank of India, *Report on Currency and Finance 2022-23: Digital Payments and Inclusion* 12 (2023).
[2] *Id.* at 15-18.
[3] Reserve Bank of India, *Cyber Security Framework in Banks*, RBI/2015-16/418 DBS.CO/CSITE/BC.11/33.01.001/2015-16, at 2 (June 2, 2016).
[4] *Id.* Annex I.
[5] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, G.S.R. 313(E), Rules 3-8 (Apr. 11, 2011).
[6] Digital Personal Data Protection Act, No. 22 of 2023.
[7] Digital Personal Data Protection Rules, 2025, G.S.R. No. 1234(E) (Nov. 14, 2025).

unbundled consents and multilingual privacy notices[8]. If we look at this from the Pro-consumer view, it emphasizes empowerment through granular control, reducing misuse; however, from the pro-bank view, it results in a burdensome process and slows operations; while the regulatory view balances both for systemic stability. This seems favorable from the pro-consumer perspective, as it aligns with constitutional privacy rights, undermining pro-bank concerns by noting that initial frictions lead to long-term trust gains, and regulatory balance can mitigate costs through guidance. For example, banks like HDFC might see slower loan approvals if consents for behavioral data are withheld, affecting efficiency for banks while protecting consumers from unsolicited marketing and reducing risks of data misuse in personalized offers.

This paper further proceeds as follows: Part II traces the historical evolution of data protection regulation in the Indian banking sector, highlighting the shift from a security-centric to a rights-based paradigm following *KS Puttaswamy v UOI*. Part III examines the core obligations imposed on banks as Data Fiduciaries under the DPDPA, including consent, minimisation, rights, deemed consent, SDF duties, breach notification, and penalties. Part IV analyses the operationalisation of these obligations through the DPDP Rules, 2025, focusing on consent management, breach protocols, transparency, rights fulfilment, and digital engagement. Part V explores sector-specific impacts on risk assessment, IT infrastructure, regulatory convergence, consumer trust, compliance costs, and overall transformation. The paper concludes in Part VI with a synthesis of findings and a forward-looking view of the framework's potential to balance innovation with privacy in India's digital banking ecosystem.

II. EVOLUTION OF INDIA'S LEGAL FRAMEWORK ON DATA PROTECTION IN BANKING

India's banking data privacy regulation has developed through a combination of IT laws, sector-specific rules, and judicial recognition of privacy as a fundamental right under Article 21 of the Constitution of India (CoI) in the landmark *KS Puttaswamy v. UOI* judgement[9], culminating in the comprehensive DPDPA[10].

The Information Technology Act, 2000[11] (IT Act) laid the initial foundation by legalizing electronic records while addressing cyber risks. Section 43A of the IT Act[12] imposed liability on banks for failing to protect the sensitive personal data of customers with reasonable care. Section 66 of the

[8] KPMG, Sneak Peek into Banking Sector Through DPDPA Lens (Dec. 2025), https://kpmg.com/in/en/insights/2025/12/sneak-peek-into-banking-sector-through-dpdpa-lens.html .
[9] K.S. Puttaswamy (Retd.) v. Union of India (2017) 10 SCC 1, 47.
[10] Digital Personal Data Protection Rules, 2025, G.S.R. No. 1234(E) (Nov. 14, 2025).
[11] Information Technology Act, No. 21 of 2000 (hereinafter "IT Act").
[12] IT Act, § 43A.

IT Act[13] criminalized unauthorized access of computer systems as computer-related offences, specifically targeting unauthorised, dishonest, or fraudulent access to computer resources, for e.g., Hacking, indirectly safeguarding banking infrastructure. The 2011 SPDI Rules expanded this understanding by defining sensitive data, e.g., financial information and mandating customer consent and security practices. Yet, these applied only to private entities without enforcement or a dedicated authority, relying on banks' internal policies.

In conjunction with the IT framework, the Reserve Bank of India (RBI) has developed additional regulations and policies specific to the financial system to address the increased risk of cybercrime. The Cyber Security Framework for Banks (2016)[14] required banks to undertake risk assessments, implement adequate monitoring systems, and report on cyber security incidents. Furthermore, through circulars and directions about information technology governance and outsourcing, the RBI required banks to ensure that third-party service providers were effectively managed. The introduction of these requirements demonstrates a recognition that data security is an essential part of maintaining the integrity of the financial system.

RBI regulations emphasized the resilience of the financial system and minimization of risk, as well as maintaining the ability to continue operations. Customer privacy was not viewed as an independent legal right by the RBI regulations, but rather only as an ancillary duty of the institution. As Protiviti's report notes, this pre-DPDPA approach led to gaps in privacy governance, with banks often facing issues like improper consent collection and purpose creep, such as using KYC data for unauthorized upselling[15]. Looking at this from a security-focused view, it was a praiseworthy step for RBI stability, while from a rights-based perspective, it was insufficient for autonomy with stifled data use. I favor the rights-based perspective, as it upholds the KS Puttaswamy v UOI judgement 'dignity' emphasis, undermining security views by showing how ancillary privacy led to breaches, and innovation by noting ethical data use spurs sustainable growth. For instance, consumers in cases like the 2022 ICICI data leak suffered identity theft due to weak protections, while banks faced reputational damage and fines, illustrating how the old regime failed both parties.

In 2017, India recognized the right to privacy as part of the right to Life under Article 21 of CoI[16] through the judgment of *K.S. Puttaswamy v. Union of India*.[17] This momentous decision established

[13]IT Act, § 66.

[14] Reserve Bank of India, *Cyber Security Framework in Banks,* RBI/2015-16/418 DBS.CO/CSITE/BC.11/33.01.001/2015-16, Annex I (June 2, 2016).

[15] Protiviti, Navigating DPDPA in Banking (2025), https://www.protiviti.com/sites/default/files/2025-07/navigating_dpdpa_in_banking.pdf .

[16] Constitution of India, 1950, Art. 21.

[17] K.S. Puttaswamy v. Union of India (2017) 10 SCC 1.

privacy as a multi-dimensional right, anchored in dignity and autonomy, and set forth a rigorous standard for its infringement, including *legitimate state aim, suitable means, proportionality, and a balance where benefits must outweigh the harms to privacy.* It also has both positive and negative connotations, where on the one hand, it places a negative obligation on the state to not infringe on the privacy of individuals and on the other puts a positive obligation on the state to enact legislation safeguarding individuals' privacy.

Specifically, the Supreme Court held that the ability to control one's personal information is part of what constitutes personal liberty, which was previously only defined under the Constitution. This case marked a significant shift from viewing privacy as a regulatory consideration to a constitutional obligation. Following the Supreme Court's directive to fortify privacy through legislation, the legislature brought the DPDPA and subsequently the DPDP Rules, 2025. The banking sector, in particular, should now take active steps in order to comply with these requirements because they store a considerable amount of private financial information.

Pre-2023, the framework remained patchwork: the IT Act, SPDI Rules focused on security, not data subject rights; RBI guidelines were supervisory; no unified fiduciary roles, access/deletion mechanisms, or oversight body existed. This led to inconsistent compliance amid rising digital banking and services. As Capco's analysis underscores this fragmentation, noting that prior regimes allowed for operational ambiguities, leading to risks like data aggregation via fintech APIs without adequate safeguards, which the DPDPA aims to address through stricter accountability[18]. While the earlier fragmented regime enhances flexibility for innovation, it poses great inconsistency risks, which is essential to address for the enhancement of consumer trust and retention. For example, consumers using apps like PhonePe faced unauthorized data sharing with affiliates, eroding trust, while banks risked regulatory scrutiny and lost business opportunities due to inconsistent privacy standards across institutions.

The enactment of the DPDPA and notification of DPDP Rules, 2025 have a strong potential to allay these concerns. By transitioning from a decentralized, security-focused regulatory approach to a comprehensive rights-based regulatory framework that defines and regulates all types of personal data in the various industries, including banking, it has the potential to redefine the manner in which individuals have access to the personal information of others as well as their own rights relating to their personal information. As Deloitte points out, the phased rollout (up to 18 months for full enforcement) provides banks time to adapt, but requires proactive integration of

[18] Capco, Navigating India's Digital Personal Data Protection Act: a transition framework for financial services (July 1, 2025), https://www.capco.com/intelligence/capco-intelligence/india-dpdpa.

privacy into business models to align with global standards like GDPR.[19] While phased rollout is practical and sustainable, delays in the rollout might lead to expose risks. From my perspective, proactive integration can be the best strategy, as delays can be mitigated by voluntary adoption, undermining phased supporters by noting early movers gain advantages, and critics by highlighting how it minimizes transitional chaos. This transition could foster innovation through trust, though smaller institutions may face disproportionate challenges. For instance, large banks like SBI can absorb upgrade costs to offer secure digital services, gaining consumer loyalty, but regional rural banks might struggle with implementation, potentially limiting access for underserved consumers. India's laws have been influenced by the European Union (EU), which has one of the strictest data protection rules in the world. The EU started with the Data Protection Directive 95/46/EC, but in 2018, it replaced it with the General Data Protection Regulation (GDPR)[20] . GDPR ensures that companies take privacy seriously by enforcing strict rules, such as allowing people to request the deletion of their data and imposing heavy fines for violations. In comparison, the DPDPA's consent-heavy model differs from GDPR's legitimate interests' basis, potentially making compliance more burdensome for Indian banks in cross-border operations, as highlighted in Hogan Lovells' discussion[21]. This consent-heavy regime empowers individuals, undermining flexibility by arguing it risks abuse, and burden by showing global alignment boosts credibility. For example, multinational banks like HSBC handling EU-Indian transactions may need dual compliance systems, increasing costs for banks while ensuring stronger privacy for consumers involved in international transfers.

III. THE DPDP ACT, 2023 AND THE OBLIGATIONS OF BANKS AS DATA FIDUCIARIES

The Digital Personal Data Protection Act, 2023 (DPDPA), imposes specific obligations on banks as Data Fiduciaries under its rights-based model. Meaning thereby, banks are required to obtain clear, specific, informed consent before collecting or processing customer personal data, except in cases of deemed consent. The Act's provisions fundamentally alter banking data practices to prioritize privacy and accountability.

A. Consent requirements

[19] Deloitte, India's DPDP Rules 2025: Leading digital privacy compliance (2025), https://www.deloitte.com/in/en/services/consulting/about/indias-dpdp-rules-2025-leading-digital-privacy-compliance.html.

[20] Regulation (EU) 2016/679 (General Data Protection Regulation) [2016] OJ L119/1.

[21] Hogan Lovells, The Data Chronicles: India's DPDPA brought into force (Dec. 4, 2025), https://www.hoganlovells.com/en/publications/the-data-chronicles-indias-dpdpa-brought-into-force.

Banks are mandatorily required to provide a notice under Section 5(1)[22] as Data fiduciaries to data principles detailing the personal data and processing purpose and rights of data principles accruing before seeking consent under Section of the Act. Further, Section 6(1)[23] mandates that consent must be free, specific, informed, unconditional, and unambiguous via affirmative action, and is limited to the stated purpose, and in cases for new uses, consent needs to be renewed. As per Section 6(7)[24] Data principles may give, manage, review or withdraw consent to the Data Fiduciary through a Consent Manager.

This requirement makes it essential for banks to overhaul onboarding and service delivery, as KPMG emphasizes, by implementing unbundled consents for activities like credit scoring or marketing, potentially reducing "shadow processing" but risking customer fatigue if not designed intuitively. Protiviti further warns that improper consent collection remains a top risk, with banks needing verifiable mechanisms for vulnerable groups, integrating with existing RBI digital consent frameworks to avoid duplication. From the consumer's perspective, it might be praiseworthy as possessing granularity for protection, but for banks it can cause fatigue and drop-offs, while for regulators it can be a balanced oversight. From my perspective, I advocate for consumer interest, as protection prevents exploitation, undermining bank arguments by noting user-friendly designs minimize fatigue, and regulators by emphasizing that enforcement ensures balance. For example, consumers applying for loans at Axis Bank could withdraw consent for marketing easily, preventing spam emails and enhancing satisfaction, but banks might see higher drop-off rates during sign-up due to multiple consent prompts, impacting customer acquisition.

B. Data minimisation principle

Under Section 5(2)[25], banks must collect and process only personal data necessary and proportionate for the specified purpose. This puts a limitation on extensive datasets for creditworthiness assessments, forcing banks to justify collections and reduce unnecessary data gathering. Obligations and violation consequences have been mentioned under fiduciary duties under Chapter II.

In practice, this principle challenges traditional data-heavy analytics, as Capco notes, requiring banks to rationalize data fields and delete obsolete records, which could enhance efficiency but limit innovation in fraud detection if alternative data sources are curtailed. EY's decoding suggests phased implementation allows time for data mapping, but failure to comply could expose banks to penalties, underscoring the need for privacy-by-design in new tech deployments. Risk reduction

[22] Digital Personal Data Protection Act, No. 22 of 2023, §5(1) (hereinafter "DPDPA").
[23] DPDPA, §6(1).
[24] DPDPA, §6(7).
[25] DPDPA, §5(2).

builds trust, undermining efficiency by showing streamlined data lowers breach costs, and innovation by arguing ethical limits spur creative alternatives. For example, banks like ICICI may limit credit assessments to essential transaction data, excluding location history, which protects consumers from over-surveillance but could lead to less accurate risk profiling, potentially raising interest rates for borrowers.[26]

C. Data principal rights

Data Principles generally, customers have rights mainly under S11 to S 14[27]. As under Section 11 - having the right to access information about personal data, right to correction and erasure of personal data under Section 12, Right to grievance redressal under Section 13, Right to nomination of representatives under Section 14. Banks must implement systems for timely responses, extending beyond standard customer service to data governance.

Fulfilling these rights demands robust infrastructure, with Protiviti estimating that 40% of banks have siloed data, complicating erasure requests. This 'right to be forgotten' could clash with retention mandates, but as IAPP's operational impacts series argues, it empowers consumers, potentially boosting trust in digital banking amid rising data concerns. From one perspective, it is proper control, while from another it can be tech burdens. Largely, as it fosters accountability, undermining operational burdens by noting tech investments yield efficiency, and regulatory compliance by showing exceptions handle clashes. For example, a consumer at Kotak Bank can request erasure of old transaction data post-loan closure, preventing long-term profiling and safeguarding privacy, but banks face technical hurdles in deleting from backups, increasing IT costs.

D. Deemed consent provisions

Section 7[28] allows for deemed consent for legitimate uses like KYC/AML compliance without explicit consent, but only for specified purposes such as bank account opening or emergencies as medical emergency involving a threat to the life or immediate threat to the health of the Data Principal or any other individual, or providing medica treatment or health services during an epidemic, during any disaster or breakdown of public order. Banks cannot extend this to unrelated activities, thereby balancing regulatory needs with privacy.

This provision provides flexibility, but DPDP Rules 2025 highlight reconciliation challenges with RBI's KYC norms, where deemed consent must be narrowly interpreted to avoid purpose creep. Capco adds that it aids financial integrity but requires clear documentation to defend against DPB

[26] EY, Decoding the Digital Personal Data Protection Act, 2023 (Nov. 20, 2025), https://www.ey.com/en_in/insights/cybersecurity/decoding-the-digital-personal-data-protection-act-2023 .
[27] DPDPA, §§ 11-14.
[28] DPDPA, §7.

scrutiny. In this regard, flexibility fosters value efficiency, while privacy purists fear loopholes here. I favor balanced views, as limits prevent abuse, undermining flexibility by noting unchecked use leads to creep, and purists by arguing necessities like KYC justify exceptions. For example, banks can process KYC for account opening without new consents, streamlining services for consumers, but if extended to marketing, it risks violations, leading to fines for banks and eroded consumer trust in data handling.

E. Additional obligations of significant data fiduciary

Banks, handling high-volume sensitive data, are likely notified as Significant Data Fiduciaries (SDFs)by the Central Government under Section 10(1), based on volume, sensitivity, and risk factors as risk to rights of the Data Principal, risk to electoral democracy, security of state, potential impact on the sovereignty and integrity of India. SDFs must appoint a Data Protection Officer reporting to senior management (Section 10(2)(a))[29], conduct periodic Data Protection Impact Assessments (Section 10(c)(i)), and audits (Section 10(c)(ii)).As probable SDFs, banks face elevated duties, with Protiviti noting costs of INR 50-100 crore for DPIAs and audits, disproportionately affecting mid-tier banks. KPMG recommends integrating these into enterprise risk management to turn compliance into a strategic advantage. For example, large SDFs like SBI must conduct annual DPIAs for AI tools, identifying biases that protect consumers from unfair lending, but the high costs could strain smaller banks, limiting their ability to compete and potentially reducing options for consumers.

F. Data breach notification

Under Section 8(6)[30], banks must notify the Data Protection Board and affected data principals of breaches promptly, alongside reasonable security safeguards under Section 8(6). This promotes transparency but risks reputational harm, necessitating robust detection and response plans.

Tsaaro's breach response guide emphasizes 72-hour reporting, aligning with RBI but adding principal notifications, which could amplify damage if not managed well[31]. Protiviti advises real-time monitoring and vendor accountability to mitigate risks. For example, in a breach like the 2023 Yes Bank incident, prompt notifications allow consumers to freeze accounts quickly, minimizing fraud losses, but banks suffer stock dips and customer churn due to lost confidence

G. Penalties for non-compliance

[29] DPDPA, §10(2)(a).
[30] DPDPA, §8(6).
[31] Tsaaro, Responding to Data Breaches: Key Obligations Under the DPDPA, 2023 and DPDP Rules, 2025 (Nov. 14, 2025), https://tsaaro.com/blogs/responding-to-data-breaches-key-obligations-under-the-dpdpa-2023-and-dpdp-rules-2025.

The Board may impose penalties up to those in the Schedule for significant breaches under Section 33(1)[32], considering factors as provided under Section 33(2) as (a) the nature, gravity and duration of the breach; (b) the type and nature of the personal data affected by the breach; (c) repetitive nature of the breach; (d) whether the person, as a result of the breach, has realised a gain or avoided any loss; (e) whether the person took any action to mitigate the effects and consequences of the breach, and the timeliness and effectiveness of such action; (f) proportionality; and (g) the likely impact of the imposition of the monetary penalty on the person.

Also, banks are responsible for notifying the Data Protection Authority of India and the affected individuals if there is a data breach that involves any personal information[33]. This requirement for Data Protection is to promote both transparency as well as accountability, and it can also have negative impacts on reputation, as the mere mention of the data breach may diminish consumer confidence in a financial institution. Therefore, all organizations should have effective detection and response mechanisms for data breaches and response plans in place.

Finally, the Act lays out a schedule for penalties to be levied against an entity for non-compliance with the requirements of the Act[34]. Organizations that fail to provide sufficient security controls or to notify consumers of a data breach, or to fully comply with all obligations regarding children's[35] Data can be subject to severe financial penalties and face significant regulatory scrutiny. Thus, the existence of potential financial responsibility and regulatory scrutiny provides an additional strong incentive for financial institutions to develop, implement and integrate privacy compliance into their overall governance processes. Capco warns that fines up to INR 250 crore could erode trust, but proactive strategies like regular audits can mitigate this. For example, a repeat breach at a bank like Punjab National Bank could trigger maximum penalties, forcing operational cutbacks and higher fees for consumers, while encouraging better security to prevent future incidents.

By combining these requirements, the role of financial institutions will change from passive custodians of their customers' information to a fiduciary who is legally obligated to their clients to protect that information. Developing and maintaining a comprehensive data governance framework through integrating data governance and risk management, and corporate accountability will allow banks to maintain a high level of trust from their clients. As IAPP notes[36], this fiduciary shift aligns with global trends but requires phased adaptation to avoid overwhelming

[32] DPDPA, §33(1).
[33] DPDPA, §5(2).
[34] DPDPA, §§ 33-34.
[35] Digital Personal Data Protection Rules, 2025 (notified Nov. 14, 2025) (hereinafter "DPDPA Rules"), Rule 10.
[36] IAPP, with rules finalized, India's DPDPA takes force (Nov. 14, 2025), https://iapp.org/news/a/with-rules-finalized-india-s-dpdpa-takes-force.

smaller players. For example, it empowers consumers with control over their data, like nominating heirs for digital assets, but banks must invest in training, raising expenses that could be passed to consumers via fees.

IV. THE DPDP RULES, 2025 AND THE OPERATIONALISATION OF PRIVACY IN BANKING

The Digital Personal Data Protection Act, 2023, creates the legal foundation for personal data, while the DPDP Rules, 2025, specify how this legal foundation must be implemented in daily functions. For Banks, these Rules are critical because they fundamentally reshape how Banks do their business, including Business Process Operations, Systems Interfaces/Architectures, Customer Interfaces, and Compliance Structures. The Rules enable Financial Institutions to move from complying with Data Protection laws to establishing formal Data Protection Practices within their organisation.

Consent Management Reforms- One of the Significant Operational Change is that, as per Rule 3 of the DPDP Rules 2025[37] Banks must disclose the form of consent when obtaining consent from Data Principals and provide notices to this effect to the Data Principals. Consent notices must be written in a clear and simple manner; Banks will no longer be able to rely on the language in very long Terms and Conditions to provide Data Principal notice of the purpose of collecting Data. As per Rule 3(c) Consent management needs to be as easy to withdraw as it is to give[38].

The Rules as *Rule 4 provides for Registration and Obligation of Consent Manager read with FIRST SCHEDULE PART A- Conditions for registration of Consent Manager and PART B- Obligations of Consent Manager*[39]- introduce an official role for Consent Managers, which provide interoperable platforms as some apps or portals for user-friendly management enabling users to give, review, and withdraw their consent to share data without cumbersome Terms and Conditions and responsibilities of the consent managers. dpdpa.com's industry analysis sees synergies with RBI's Account Aggregator, but warns of harmonization needs to avoid complexity in financial data sharing. For example, consumers can manage consents across banks via a single app, simplifying control and reducing errors, but banks must integrate systems, incurring costs that could delay fintech collaborations.

1. **Data Breach Protocols**: Another key requirement as per Rule 7[40] of the DPDP Rules,2025 for banks is to establish procedures for notifying customers of a data breach.

[37] DPDPA Rules, Rule 3.
[38] DPDPA Rules, Rule 3(c).
[39] DPDPA Rules, Rule 4, Sch. I, Part A & B.
[40] DPDPA Rules, Rule 7.

When a bank learns of a customer's personal data being lost or stolen, the bank must notify the customer promptly. The notice must include a description of the breach, possible effects of the breach on the individual and steps the bank has taken to remedy the situation. This demands enhanced monitoring and communication investments to balance trust-building with reputational risks. Tsaaro highlights that financial sector's alignment with RBI's controls (e.g., PCI DSS) strengthen response, but principal notifications add layers, potentially increasing costs. For example, in a hypothetical breach at Canara Bank, detailed notifications help consumers change passwords swiftly, averting theft, but banks face media backlash and legal claims, affecting stock prices.

2. **Transparency and Accountability**: Rule 9 also increases the mechanism for transparency and accountability. Banks are required to post information on how to contact them with questions about data or complaints about data in a public way, usually by having a person designated as Data Protection Officer as per Rule 9[41]. Also, as per Rule 13(1)[42]- Significant Data Fiduciaries, e.g., banks, must conduct regular, i.e. once in every period of twelve months, independent audits and Data Protection Impact assessments regarding new technologies or sensitive categories of data handled using computers. Privacy oversight becomes part of a bank's governance model. Protiviti recommends AI for automating DPIAs, noting that this institutionalizes privacy but requires board-level oversight. For example, audits at Union Bank could reveal vulnerabilities in app data handling, protecting consumers from leaks, but the annual requirement burdens banks with ongoing expenses, diverting funds from customer services.
3. **Data Principal Rights Fulfilment**: As mentioned in Rule 14[43], a key procedure for Data Principals is a bank's obligation to respond to requests for access to, correction of, updating of, or erasing of a person's data, i.e., Data Principal, within 90 days. Banks would need to develop internal processes for locating and modifying/deleting information that exists in multiple databases through multiple platforms as Transactions, Customer Relationship Management (CRM), and Compliance Archive Systems. It is a significant operational challenge for banks because their systems often retain their transactional data within three different system types. Capco stresses self-service portals to meet timelines, but legacy silos could delay compliance, risking fines. For example, a consumer requesting data access at IDBI Bank gains insight into usage, enabling better financial decisions, while

[41] DPDPA Rules, Rule 9.
[42] DPDPA Rules, Rule 13(1).
[43] DPDPA Rules, Rule 14.

banks must upgrade CRM systems, increase IT budgets and possibly leading to slight fee hikes for services.3

4. **Digital Board Engagement**: Additionally, the Rule 20[44] of DPDP Rules,2025, establish a digital-first framework to govern the functioning of the Data Protection Board. Banks will be able to submit complaints and initiate proceedings through an online process. Thus, banks will increasingly engage in direct regulatory compliance via digital compliance portals. Banks should establish policies and procedures for documenting and retaining their data practices in order to demonstrate compliance with the Data Protection Board if it conducts an inquiry into a bank's data practices.

In essence, the DPDP Rules shift privacy compliance from being a one-time requirement to being an ongoing practical obligation of business operations. This means that banks need to take into account privacy when designing both their systems and customer-facing technology as well as their internal Governance Structures. These Rules are intended to add to what the DPDP calls for; they outline how banks need to operate in order to comply with the Act. EY notes the three-phase rollout (full by May 2027) eases transition, but sectors like banking must prioritize data security to avoid scrutiny. For example, phased audits help banks like Bank of Baroda gradually build compliance, benefiting consumers with improved protections over time, but initial phases may confuse users if banks communicate changes poorly.

V. SECTOR-SPECIFIC IMPACTS OF THE DPDP FRAMEWORK ON INDIAN BANKS

The consequences of the DPDP Act, 2023, and DPDP Rules, 2025, are greater than meeting statutory obligations. As they will also dictate how Banking Institutions complete many of their daily operational activities. Consequently, these legislative measures will influence the way *banks perform four key functions: risk assessment, technology usage, regulatory coordination and customer trust*, to name a few. While there may be procedural implications, the magnitude of impact will be largely structural in nature, which has been discussed below.

A. Impact on risk assessment and credit assessment

As a result of the reliance on Data Analytics, the banking industry has become heavily dependent upon the use of Data Analytics to determine the creditworthiness of customers, as well as identify potential fraud and pricing of Financial Products. While the use of Data Analytics has been established as a relatively new methodology in Banking, the DPDP Framework establishes limits on how much data banks may use to perform their evaluative functions by introducing both the

[44] DPDPA Rules, Rule 20.

requirement for consent and the principle of Data Minimisation[45]. Prior to the establishment of the DPDP Framework, banks relied on both Traditional Bankers' practices and large datasets, e.g. Transaction History, Spending Patterns, and Alternative Sources of Data to perform their evaluations. However, after the enactment of the DPDP Act and notification of DPDP Rules,2025, banks will only be able to use that data to the extent that it is required to complete the specific purpose for which it was collected, i.e. Link Between Purpose and Collection and justification for the use of that data must be provided by the bank[46]. Thus, Banks will likely move away from the use of broad-based profiling techniques in favour of providing a more robust internal justification for each piece of data or data set that is used to inform the development of Decision-Making Models for Risk Management and Credit Assessment.

This shift could reduce bias in AI models, as Protiviti suggests, but may constrain alternative data use in underserved markets, per RBI reports. KPMG warns of stricter governance in analytics, prohibiting silent processing, which might slow innovation but promote ethical practices. For example, banks assessing loans for rural farmers might limit data to basic income records, excluding utility payments, leading to fairer but potentially higher-risk lending for banks, while consumers benefit from unbiased approvals and lower chances of discriminatory denials.

B. Impact on its systems and cybersecurity infrastructure

The DPDP framework emphasizes secure system design. Banks must ensure that strong encryption, strict access controls, detailed audit trails, and efficient breach detection are in place within their organization. While cybersecurity was regulated via the guidelines issued by the RBI[47], the DPDP framework adds a legal aspect to failure to implement or maintain these data protection safeguards.

In addition to ensuring compliance with DPDP legislation, banks will now have to implement data architecture that meets the demands of customer rights. As a result, banks will need to implement systems capable of identifying all the data connected with an individual; therefore, they should be able to respond to requests for correction or deletion of the information related to that individual. The implementation of the DPDP framework will cause banks to re-evaluate their data storage methods, as many legacy banking systems continue to store data in a fragmented manner. Compliance will therefore be more complex due to technical limitations.

Also, compliance with DPDP regulations will be applicable to third-party service providers, e.g., cloud-service providers, and IT outsourcing partners. As a result, Banks will remain responsible

[45] DPDPA, § 5.
[46] DPDPA, § 5.
[47] Reserve Bank of India, *Cyber Security Framework in Banks*, RBI/2015-16/418 DBS.CO/CSITE/BC.11/33.01.001/2015-16, at 2 (June 2, 2016).

for ensuring that all third-party processors comply with the provisions of DPDP regulations so entrusted with third-party responsibility. Consequently, vendor management will form part of the broader framework of privacy governance, as opposed to merely being an operational issue. Protiviti identifies legacy architectures as a key hurdle, recommending PETs (privacy-enhancing technologies) and automation for efficiency. Capco stresses vendor due diligence, noting costs for upgrades could hinder startups. For example, banks partnering with AWS for cloud storage must audit vendors annually, ensuring consumer data security but raising operational costs for banks, which might delay tech adoptions and limit innovative services for consumers.

C. Regulatory convergence and legal tensions

The interaction between the DPDP Act, read with DPDP Rules,2025, and other financial regulations presents a significant sectoral challenge. For example, both KYC requirements and AML laws require banks to retain customer information for an extended period. Conversely, the DPDP Framework provides for limits on storage and deletion when it is no longer necessary for legal compliance. Therefore, in order to meet their obligations, banks must be able to show the legal basis for retaining such information. Banks may also experience a regulatory overlap between the Data Protection Board and the responsibility of the Reserve Bank of India (RBI) to supervise banks, resulting in the banks having dual compliance obligations to meet. Banks must therefore work together to develop co-ordinated approaches to address the intersecting regulatory obligations that exist.

The dpdpa.com highlights the need for harmonization with RBI/SEBI/IRDAI, especially for KYC and cross-border flows. Protiviti suggests memoranda of understanding to resolve overlaps, warning of potential litigation if not addressed. For example, banks retaining AML data for 10 years under PMLA might conflict with DPDPA deletion requests, exposing banks to lawsuits while consumers gain stronger rights to challenge retentions, potentially speeding up data purges post-compliance.

D. Impact on consumer trust and competitive positioning

Privacy is an increasingly important factor in how consumers perceive the safety of their financial information. As a result, the level of trust consumers have in banking systems to protect their personal and financial information directly influences their adoption of digital banking services. By implementing transparent consent procedures, providing clearly defined ways to lodge complaints against financial institutions, and promptly notifying consumers in the event of data breaches, banks can build consumer trust in their ability to safeguard sensitive information. Additionally, privacy governance gives banks a competitive advantage in the marketplace. On the other hand, a major data breach that has been made public through mandatory disclosure

requirements will often cause more reputational damage to institutions today than it would have previously.

The recognition of customers as Data Principals with established rights creates a substantial change in the customer-bank relationship. Data is no longer merely regarded as an asset to be used by the institution itself; rather, data now falls under the individual control of the Data Principal. This shift has the potential to foster more responsible data use by both banks and their customers. KPMG positions compliance as a differentiator, enhancing resilience and empowerment. Capco agrees, noting proactive privacy can yield competitive edges in trust-driven markets. For example, banks like IndusInd adopting strong privacy policies could attract privacy-conscious millennials, boosting market share, while consumers feel safer using UPI, increasing digital adoption rates.

E. Compliance costs and institutional restructuring

The DPDP framework will impose considerable costs on finance companies. Banking organisations will need to invest significant resources in developing new technology systems, creating compliance review processes, developing staff training programs, establishing governance structures such as Data Protection Officers and creating internal auditing systems. These costs will be disproportionately borne by smaller banks/finance companies since they are likely to have limited resources to invest. Still, these investments have the potential to mitigate the financial repercussions of regulatory fines and reputational damage.

Privacy compliance is being increasingly integrated into enterprise risk management programs. Data protection risk is now subject to oversight at the Board of Directors level. This represents the institutionalisation of privacy governance, which has transitioned from "recommended best practices" to "required regulatory expectations". Protiviti's survey reveals gaps, with 37% lacking privacy budgets, urging scalable tech investments. Deloitte's guidance on the 18-month timeline recommends metrics and training for effective restructuring. For example, appointing DPOs at Federal Bank elevates privacy oversight, reducing breach risks for consumers, but the restructuring costs could lead banks to consolidate branches, affecting accessibility for rural consumers.

F. Overall sectoral transformation

The combination of these factors indicates that the DPDP regime affects both regulatory processes and business models in the Banking Sector. Financial Institutions and Banking Organisations must develop a strategy to balance the benefits of data-driven innovation with the legal responsibilities that accompany such innovation. In summary, the DPDP framework expects to encourage the disciplined use of data, to implement more robust internal controls on how data is used and to require greater transparency in how data is processed. The DPDP framework will impose operational challenges on the banking and finance sector, but it will promote the

establishment of a more sustainable and trustworthy digital finance ecosystem. As IAPP observes, phased enforcement aids globalized sectors like banking, but demands alignment with GDPR for international operations. For example, Indian banks expanding abroad must comply with dual regimes, strengthening global consumer protections but raising entry barriers for banks, limiting competition.

VI. CONCLUSION

The DPDP Act, 2023, and DPDP Rules, 2025, fundamentally transform India's banking sector from a cybersecurity-centric model to a rights-based data governance regime, even including customer rights as right to be forgotten, imposing structured obligations on banks as Data Fiduciaries. While introducing operational challenges as consent management, data minimisation in credit assessments, legacy system upgrades, and regulatory coordination with RBI, the framework ultimately fosters consumer trust through transparency, accountability, and enforceable Data Principal rights. Though compliance costs and tensions with KYC/AML retention requirements persist, these reforms promise a potential and resilient digital banking ecosystem, *balancing innovation with privacy*. Banks succeeding in this "privacy reckoning" will not only mitigate penalties under Section 33 and Section 34 but also gain a competitive edge via increasing customer confidence and robust governance integration. Ultimately, as Capco concludes, viewing challenges as opportunities for transparency could position Indian banks as privacy leaders in Asia. For example, by embracing these rules, banks like State Bank of India can lead in ethical AI, attracting international partnerships while consumers enjoy safer, more transparent financial services.